Encrypting Destiny Data Files

System administrators can provide extra protection of application data on the Destiny server by encrypting external Destiny data files.

Certain Destiny data files are stored from standard drive folders on the Destiny application server. This data includes text documents – such as patron import files and report output – as well as image files, such as patron pictures. These files are external to the SQL database and as such are to be protected from unauthorized access with normal Windows access controls: login authentication and file permissions.

Protect Destiny with encryption

You might want to use file encryption to protect Destiny files against physical (stolen hard drive) or remote access. With file encryption, data is stored as unintelligible characters, protecting it from any account that has not been granted encryption rights.

Encrypted file system

Follett recommends using the Encrypted File System (EFS) technology built into Windows Server®. EFS lets the system administrator designate files to be encrypted when they are saved. The encryption process is automatic and transparent to authorized user accounts.

EFS encryption strength

EFS uses industry-standard public-private key technology to provide strong encryption. Windows Server uses the Advanced Encryption Standard (AES) algorithm by default, which uses a 256-bit key for encryption and decryption. The encrypting/decrypting process is performed in kernel mode, eliminating the risk of keys being left in an external paging file.

Encrypt Destiny data

EFS encryption can be set at the folder level so all files created in that folder are automatically encrypted. In Destiny, the FSC-Destiny folder is the parent folder under which non-SQL data files are stored. Assigning EFS encryption to this folder will encrypt external Destiny files.

You can use an existing user account, or create a new one, to encrypt the Destiny folder.

Important: Be sure to stop the Destiny service before performing these steps.

To create a new user account on the server for the Destiny service:

1. Select **Start > Control Panel > Administrative Tools > Computer Management**. The Microsoft Management Console opens.
2. On the left-side, expand **Local Users and Groups** , and then select the **Users** folder.
3. In the Actions pane, click **More Actions,** and then select **New User**.
4. Enter a user name and password, and set the options for the new account.
   Select the following options:
   - Password never expires
   - User cannot change password

   Important: Do **not** select the *User must change password at next logon* and *Account is disabled* options.
5. Click **Create**.
6. Select **Start > Control Panel > Administrative Tools > Local Security Policy**.

7. On the left side, expand **Local Policies**, and then select **User Rights Assignment**.
8. On the right side, double-click **Log on as a service**.
9. Click **Add User** or **Group**.
10. Select the Destiny account.
11. Click **OK**.

To modify the Destiny service to run under the new account:

1. Unregister the Destiny Service, as follows:
   - Open a command prompt, and navigate to the `\FSC-Destiny\jboss\bin` directory.
   - Run the following command: `destiny unregister`
2. In the `\FSC-Destiny\fsc\bin` directory, create a plain text file named password.conf, and add the following lines:

   ```
   wrapper.ntservice.account=<domain name>\<user name>
   wrapper.ntservice.password=<password>
   ```

   Note If the server is not part of a domain, use the machine name instead of a domain name.
3. Log in to Windows Server using the Destiny account.
4. Register the Destiny Service, as follows:
   a. Open a command prompt, and navigate to the \FSC-Destiny\jboss\bin directory.
   b. Run the following command: `destiny register`
   c. Close the command prompt.

To update the folder properties on `\FSC-Destiny`:

1. Log in to the Windows server using an Administrator account.
2. Open Windows Explorer ,and navigate to the `\FSC-Destiny` folder.
3. Right-click the `\FSC-Destiny` folder, and select **Properties**.
4. On the **Security** tab, add the Destiny user account and grant it Full Control.
5. On the **General** tab, click **Advanced**.
6. Select **Encrypt contents to secure data**.
7. Click **OK**.
8. On the **General** tab, click **Apply**. The Confirm Attribute Changes pop-up opens.
9. Select **Apply changes to this folder, subfolders and files.**
10. Click **OK**.
11. Restart the Destiny service.

At this point, there should be no unencrypted data in your Destiny installation. Check for any Destiny-related data (such as patron upload files) that may have been stored elsewhere on the server and move it to the FSC-Destiny folder.

Note: If you prefer to keep these files outside the FSC-Destiny folder, you can encrypt the folder where they are stored using the same Destiny account.

When running command-line utilities (such as patron or class uploads) from an encrypted folder, first log in to the Windows server using the Destiny account.

When running command-line utilities from an encrypted folder as a scheduled task, configure the scheduled task to run as the Destiny account.

Backup notes

This process only encrypts the contents of the folder where Destiny is installed. If you copy the contents of the Destiny directory to another location, the files may not be encrypted in the new location.

When making backups of Destiny, you may want to encrypt your backup location as well, using the steps above. In case of server malfunction, you may also want to export the certificate that you used to encrypt the folder.

For more information on this process, contact Microsoft technical support.

Technical support

For technical product issues, including how-to procedures and error reporting:

Destiny email techsupport@follettlearning.com

Destiny International email internationalsupport@follettlearning.com

Phone support 888.511.5114 + Option 2

Customer service

For ordering and billing/payment issues:

Email softwarecs@follettlearning.com

Phone support 888.511.5114 + Option 1