Software & Security Considerations

Chapter 3

In Chapter 2 we described the enrollment process for the FSA systems that are used to confirm student eligibility and disburse FSA funds. In this chapter we'll give an overview of the software and security issues that must be considered when planning how your school will process FSA data and reports. The security of personal and organizational data has become increasingly important in recent years, and federal law requires that your school have an information security plan. This chapter may assist you in developing your school's plan.

SOFTWARE PROVIDERS

While your school is required to have at least one SAIG Mailbox and to enroll in FSA systems such as the CPS, COD, and NSLDS, the Department doesn't specify what software must be used at your school to open, create, or correct FSA records and reports.

As a service to participating schools, FSA provides free PC-based software to transmit and receive data over the Internet (EDconnect) and to work with student application and award/disbursment records (EDExpress). FSA also provides software to electronically certify student enrollment and address information with the NSLDS (SSCR), and to assist schools participating in the Direct Loan (Direct Loan Tools) and Perkins Loan (Perkins DataPrep) programs.

However, schools may choose to use software developed by third-party vendors, or develop their own PC or mainframe-based software programs to work with FSA records and reports. Some of the more sophisticated software products have the advantage of being able to share information with other offices at your school—for instance, enrollment data with your bursar's office and payment information with your business office.

If you choose a third-party software product, you are responsible for ensuring that it can perform the necessary functions to open, edit, and create FSA student records and reports. (In particular, your software must be able to send and receive COD records in XML format.) Ultimately, the responsibility for ensuring the timeliness and accuracy of electronic data rests with your school.

CHAPTER 3 HIGHLIGHTS

- Software Providers
  - → Communications software: EDconnect
  - → Data processing: EDExpress, mainframe, & 3rd party software
- Security issues
  - → SAIG Mailbox & Destination Point Administrator
  - → FSA Web site access
  - → Software permissions
- Options for controlling data flow & user access
  - → Creating SAIG Mailboxes
  - → Setting user permissions in the software
  - → Setting file paths
- Examples
  - → Single mailbox & multiple mailboxes
  - → Password protection policies

ED Software downloads

FSA software, as well as related manuals and technical references, can be downloaded from the Web at: fsadownload.ed.gov

For help installing the software, call CPS/SAIG Technical Support at 1-800-330-5947 or email : CPSSAIG@ed.gov

SECURITY ISSUES

Security precautions

- Exit EDconnect and EDExpress completely when leaving a workstation for long periods of time.
- Have a unique user ID and password.
- Choose passwords that cannot be guessed easily.
- Don't leave login information in public view.
- Don't allow students to enter or edit any information in your software
- Keep all personal information printed from software or ED Web sites in a secure place.
- Have the appropriate level of access.
- Close student records when updates are completed.
- Delete access for staff who are no longer employed or responsible for FSA program administration.

Because student aid records contain personally-identifiable information that is quite sensitive, your school must take special care to ensure that only appropriate members of the administrative staff have are able to view and edit those records. The person who configures the security settings in EDExpress is usually referred to as the "Systems Administrator."

The Systems Administrator can be one of the Destination Point Administrators identified in the SAIG enrollment process, as discussed in Chapter 2. Or it may be someone at your school who has general responsibility for the installation of new software and the security of the network. In either case, the person configuring the software should give careful consideration to how it will be used and the types of access required for each user.

Managing permissions for school staff requires a little planning, because access to FSA data is controlled at three different levels:

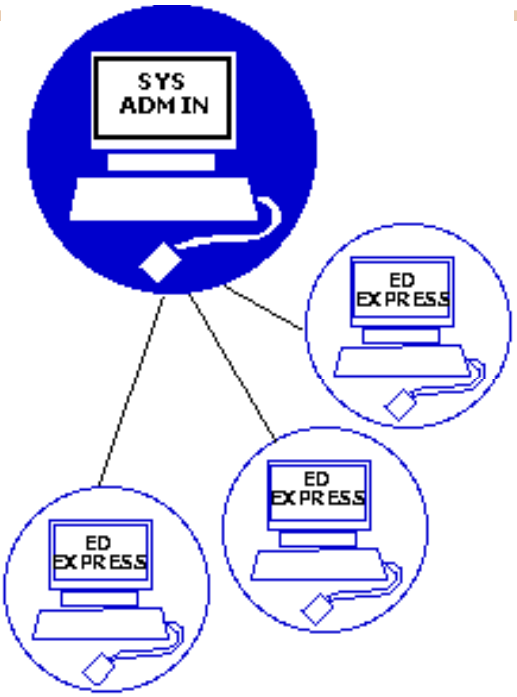
- *SAIG Mailbox.* The Destination Point Administrator (DPA) specifies what kinds of data are sent to a particular mailbox when the mailbox is created. The DPA also creates and updates the SAIG Password for that mailbox, which is shared by all members of the Security Group that will be using that mailbox.

- *FSA Web sites.* The Destination Point Administrator for a primary mailbox can enroll users for the CPS and NSLDS Web sites. (NSLDS Web access requires the creation of

Local Security

Since software programs such as EDconnect and EDExpress are used to access student records and build a database of student information, the school must be careful to restrict access to the software to those staff members who are authorized to view and/or change student records.

When software is installed on a server and will be used by multiple users, the Systems Administrator will assign access rights to each of the individual users.



a separate mailbox for each user.) The COD Security Administrator performs a similar function for the COD Web site.

- *EDconnect & EDExpress (or equivalent).* User permissions for software that is run on school computers are set locally, and the information about the school staff who are using the software is not transmitted to any of the FSA systems.

Because access is configured separately for Web users and software users, it is possible for a Web user to have access to some data that he or she cannot open in local software (or vice versa). In general, we recommend that you configure the access rights in EDconnect and EDExpress so that they are consistent with the permissions that you have established through the SAIG Enrollment Form, the SAIG Web site, and with COD School Relations. (See Chapter 2.) For instance, if you have given a user access to CPS data in EDconnect and EDExpress, then you would probably want to give that user the capability to view and edit ISIR data on the *FAA Access to CPS* Web site.

Information security requirements

Schools that participate in the FSA programs are required to follow Federal Trade Commission regulations, which require all financial institutions to develop, implement, and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives:

- Insure the security and confidentiality of customer information,
- Protect against any anticipated threats or hazards to the security or integrity of such information, and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

For more information on these requirements, see Volume 2 of the *FSA Handbook*.

OPTIONS FOR CONTROLLING DATA FLOW & USER ACCESS

Destination Points & TG numbers

An SAIG Mailbox or "Destination Point" is identified by its "TG Number."

Creating separate SAIG Mailboxes

One way to organize the exchange of FSA data is to create separate SAIG Mailboxes for different kinds of data. For instance, you could establish one mailbox solely for ISIR data, and another mailbox solely for COD data.

As we discussed in Chapter 2, the SAIG enrollment process gives you the choice of the following types of data for a mailbox:

- Central Processing System (FAFSA/ISIR data for students)
- Grants Processing (Pell, ACG/SMART, TEACH)
- Direct Loans Processing
- Direct Loan Services Information
- Campus-Based (the FISAP application and report)
- Direct Loan Borrower Delinquency Reports
- NLSDS Batches (Enrollment & Transfer Monitoring)
- Cohort Default Rates (eCDR)

In theory, you could have a different mailbox for each of these types of data, but at most schools, it would make more sense to combine some of these categories into one mailbox. For instance, staff members working with default prevention could be served by a single mailbox that collected NSLDS batches, eCDR information, and Direct Loan Borrower Delinquency Reports. Or a school might have an SAIG Mailbox for Direct Loan data coming from both the COD system and the DL Service Center, but a different one for getting Grant data from COD.

Also note that you will need to establish separate SAIG Mailboxes for additional locations of your school if they have different Federal School Codes for purposes of FAFSA/ISIR data. Similarly, a school can obtain separate Direct Loan codes for approved additional locations, if it wants to set up a mailbox to receive DL data for just that location.

Setting user permissions in the software

If you are acting as the Systems Administrator and are setting up EDconnect or EDExpress software on a PC, you can set the access rights for each Security Group that you create. All of the users in a Security Group have the same access rights.

Your EDExpress Security Groups do not have to mirror your EDconnect Security Groups, because the access rights that are being assigned are quite different. EDconnect controls the ability to send or receive files to SAIG Mailboxes, and we recommend that you only establish one Security Group for each of your school's mailboxes. EDExpress controls the functions for working with the individual records (viewing, updating, printing, etc.).

- *EDconnect—Security View>Properties.* Since you will only create one EDconnect Security Group for each of your SAIG Mailboxes, all of the users in that Group have the same access to the mailbox. In other words, you cannot limit their access so that they can send/receive only certain types of files.

- *EDExpress—Tools>Global>Security Groups.* Because you can create multiple Security Groups in EDExpress, you can set very specific levels of access to different types of data (Global, App Express, Pell, DL, COD, and Packaging). For instance, you could create a Security Group just for your counselors, with permission to view (but not edit) ISIR records, while another Security Group of more senior staff would have the ability to edit ISIRs, as well as access rights for COD data.

You can organize your Security Groups to control workflow. For instance, you might give your COD workgroup the capability to create and update Common Records, but not give them the permission to transmit files in EDconnect. A member of the EDconnect Security Group for the SAIG Mailbox would be responsible for sending and receiving files on a predetermined or *ad hoc* schedule. This would be one way to stage your work in larger batches.

Access to shared database files

For network setups, the executable files for EDExpress are loaded onto individual PC's, but the database file (****.mdb) is loaded onto a network drive. A student record in the database file can only be opened by one user at a time. Each time that record is accessed, EDExpress records in that .mdb file who accessed it and when.

Changing default file paths in EDconnect & other software

When you change the default paths for files, you MUST make sure that you change them identically in EDconnect and your financial aid software (e.g., EDExpress) so the two software programs both know where to store and where to find student records. To change file paths in EDconnect, go to: *Tools/Setup/File*.

Setting file paths

You may find it convenient to have different types of data sent to different folders on a single-user PC or a network. This can be done by setting file paths in EDconnect. There are two ways to do this:

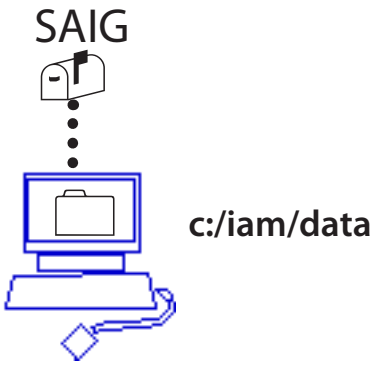
- *EDconnect.* Different file paths for each type of message can be set in the "Message Class Manager" in EDconnect. For instance, you could specify that all 09-10 processed ISIRs be placed in a network folder on the "F" drive. To ensure the security of this data, use of the F drive would be restricted to counselors and other aid staff working with student aid applications and verification.

- *EDconnect.* User-specific file paths can be set in EDconnect so that when a user logs in, any files that he or she downloads will go to that user's designated folder. Note that this method can create problems if a user automatically downloads all files to his or her folder, including files that other users need.

Your systems administrator can provide an additional layer of security by controlling which users have access to the data kept in folders on a shared drive.

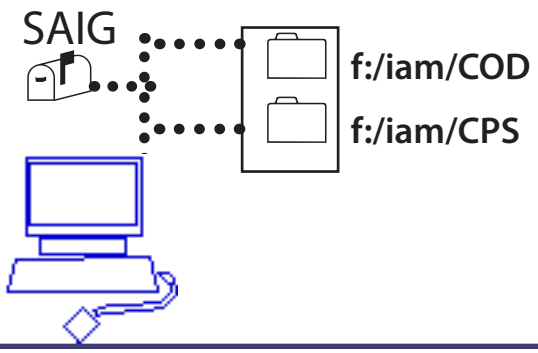
File Paths—Examples

Single-user file path



Selecting a file path for a single user is relatively simple. Unless you specify otherwise, EDconnect will create a new folder on your PC's hard drive, using the file path c:/iam/data. EDconnect will download new data from your SAIG Mailbox to this folder. EDExpress will automatically look for this folder when preparing to open new files.

Network file path



In a network environment with multiple users, you will probably want to set a file path that leads to a folder on a commonly-shared network drive. You also may want to create separate folders for different kinds of files. But you must be careful to specify these new folders when configuring EDExpress, so that it knows where to find new files.

Security Group Setup—Examples

SAIG Mailboxes at Career Tech: Single Security Group

	EDconnect	EDExpress Software
 TG 99991	**DP-1** **SAIG PW: 123abc** DPA: Bill Frisell Steve Lacy	**Admin Group:** Bill Frisell Steve Lacy
 TG 99992	**NSLDS User 1** **SAIG PW: def123** DPA: Steve Lacy	

Career Tech has set up two SAIG mailboxes for the 2 members of its small financial aid office. Bill Frisell and Steve Lacy use the first mailbox to exchange CPS, COD, and NSLDS batch files. Because only the DPA of a mailbox can have on-line access to NSLDS, Steve Lacy has a separate mailbox for that purpose.

SAIG Mailboxes for AEC University: Multiple Security Groups

	EDconnect	FinAid Software
		Admin Group Lester Bowie Malachi Favors
 TG 00001	**COD Security Group** **SAIG PW: 456xyz** DPA: Lester Bowie Don Moye Joseph Jarman	**COD Users** Don Moye Joseph Jarman
 TG 00002	**Apps Security Group** **SAIG PW: 345tuv** DPA: Malachi Favors Roscoe Mitchell Joseph Jarman	**Apps Users** Roscoe Mitchell Joseph Jarman
 TG 00003	**NSLDS User1** **SAIG PW: 234qrs** Don Moye	**NSLDS Users** Don Moye Roscoe Mitchell
 TG 00004	**NSLDS User2** **SAIG PW: 678nop** Roscoe Mitchell	

AEC University has a larger aid office, and has set up separate mailboxes for staff who work with application data (ISIRs) and those who are responsible for Pell and Direct Loan awards (COD).

Each security group has its own TG number and SAIG password, which are used by all of the users in that group. Note that Joseph Jarman belongs to both the COD and Apps Groups.

In addition, several of the staff have individual mailboxes so that they can have access to the NSLDS Web site.

AEC University uses a product called Finaid Software to create and modify student records. Staff members are given access to different types of records, depending on their responsibilities.

Security Group Setup—Examples (continued)

SAIG Mailboxes at TriState College: Multiple Locations

	EDconnect	EDExpress Sofware	
		Admin Group: John Barth Willa Cather	TriState College has campuses in three different locations, so it has requested and received a different Federal School Code for each campus. Therefore, Tristate has three different mailboxes for ISIR data.
 TG 11110	**Apps - Maryland Security Group** **SAIG PW: abcd4321** DPA: John Barth Upton Sinclair	**Apps - Maryland Security Group** John Barth Upton Sinclair	(This example does not show TriState's other SAIG Mailboxes for COD, NSLDS, etc.)
 TG 11111	**Apps - Virginia Security Group** **SAIG PW: def8765** DPA: Willa Cather Mary Lee Settle	**Apps - Virginia Security Group** Willa Cather Mary Lee Settle	
 TG 11112	**Apps - DC Security Group** **SAIG PW: ghij1098** DPA: Jessie Fausett Ann Beattie	**Apps - DC Security Group** Jessie Fausett Ann Beattie	

SAIG Mailbox Rules and Security Groups.

For each SAIG Mailbox that it establishes, a school must designate at least one "Destination Point Administrator" who is responsible for the security of the data sent and received through that mailbox.

- Only the DPA of an SAIG Mailbox can have access to the NSLDS Web site.
- In EDconnect, there will be a "Security Group" of users at the school for each SAIG Mailbox; users will have the same SAIG password and common access to that Mailbox.
- In EDExpress, Security Groups have the capability to read and modify different types of files.

The EDExpress Security Groups are not necessarily associated with a particular Mailbox, and can have different users than the EDconnect Security Groups.

Sample Password Policies

Password Requirements

As a user, you may be responsible for any activity initiated by your user ID since you are the only person who should have your logon information. You must protect your user account(s), and not allow anyone else to use your account or use your computer while logged in under your account (except as required for system administration). In order to protect your user credentials, you must adhere to the following guidelines:

- Password must be at least eight (8) characters in length.
- Must contain a mixture of alpha and numeric characters, upper and lower case letters, well as special characters.
- The password must not match or resemble the word 'password' in any form (e.g., as-is, capitalized, or adding a number).
- The password cannot contain the same string as your userID or that contains your name.
- The password cannot be a dictionary word in any language.
- Do not lend or divulge the password to other persons, including individuals purporting to be system administrators.
- Never make the password visible on a screen, in written form (e.g., on sticky notes).
- When you leave your computer unattended, you must either log out or invoke protection of your system (e.g., a password-protected screensaver).
- Avoid using the "remember password" feature.

Password Construction Guidelines

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters (e.g., 0-9,!@#$%&*);
- Are at least eight (8) characters long; and
- Are not based on personal information, names of family, etc.

Poor, weak passwords have the following characteristics:

- The password contains less than eight (8) characters.
- The password is a common usage word such as names of family, pets, and friends, or birthdays and other personal information such as addresses and phone numbers.

System Development Standards

Each system should have its own password selection standard that adheres to the above guidelines while being commensurate with the level of security required by the level of sensitivity of the system.

As a system owner/manager, you must ensure your system(s) contain the following security precautions:

- Should support authentication of individual users.
- Should not store passwords in clear text or in any easily reversible form.
- Regular changing of passwords should be systemically enforced in accordance with procedures outlined in the system security plan.
- Users should be warned automatically prior to the expiration times and will be prompted to change their password automatically once expired.
- Should disable user accounts after three (3) consecutive invalid attempts are made to supply a password.
- Should require the reinstatement of a disabled user account by a Help Desk technician or a system administrator.