Installation and User Guide for

EDconnect 8.3

Version 1.2

U.S. Department of Education

FSA
FEDERAL
STUDENT AID

DOCUMENT CONTROL

DOCUMENT INFORMATION

Title:	EDconnect 8.3 Installation and User Guide
Revision:	1.2
Issue Date:	11/16/2012

DOCUMENT HISTORY

Version Number	Date	Summary of Change
1.0	03/05/2012	Created for EDconnect 8.1 release
1.1	09/11/2012	Updated for 8.2 release
1.2	10/30/2012	Updated for 8.3 release

Table of Contents

1 STUDENT AID INTERNET GATEWAY (SAIG) OVERVIEW 1

1.1 SYSTEMS OVERVIEW 1
1.2 STORE AND FORWARD DATA TRANSMISSIONS 3
1.3 DESTINATION POINT ADMINISTRATION 4
1.3.1 Destination Point Administrator 4
1.3.2 SAIG User Statement 5

2 INSTALLING EDCONNECT 6

2.1 HARDWARE AND SOFTWARE REQUIREMENTS 6
2.1.1 Estimating Hard Disk Space Needs 7
2.1.2 Supported Operating Systems 8
2.2 IMPORTANT INSTALLATION NOTES 9
2.3 DOWNLOADING SOFTWARE/PAPER DOCUMENTATION 10
2.3.1 Downloading the Software 12
2.4 INSTALLING EDCONNECT 13
2.5 SETTING UP EDCONNECT 16
2.5.1 Setting Up EDconnect With Imported Security Settings 16
2.5.2 Setting up EDconnect without Imported Security Settings 23
2.5.3 Setting up a Test Security Group 27
2.5.4 Selecting a Connection 28

3 USING EDCONNECT 34

3.1 DESTINATION POINT ADMINISTRATION 34
3.2 SECURITY AUTHENTICATION FOR USER LOGONS 35
3.3 SECURITY VIEW 37
3.4 SECURITY GROUPS 40
3.4.1 To add a "Production" Security Group 40
3.4.2 To add a "Test" Security Group 44
3.4.3 To delete a Security Group 45
3.4.4 To Modify a Security Group 46
3.5 USERS 48
3.5.1 To add an FSA User ID 48
3.5.2 To delete an FSA User ID 50
3.5.3 To Modify an FSA User ID 51
3.6 SAIG CONNECTIONS 53
3.6.1 Selecting a Connection 53
3.6.2 Firewalls 58
3.7 WIZARDS 59

4 PASSWORDS 60

4.1 TYPES OF PASSWORDS 60
FSA User Password 60
SAIG Password 61
4.2 FSA USER PASSWORD 62
4.2.1 Changing Your FSA User Password 63
4.3 SAIG PASSWORD 64

4.3.1 Changing Your SAIG Password ... 66
4.3.2 Performing a "Local Only" SAIG Password Change ... 67
4.3.3 Performing a "Network and Local" SAIG Password ... 69
4.3.4 Changing your SAIG Password After Help Desk Resets It ... 71
4.3.5 Changing Your SAIG Password After It Has Expired ... 73

5 DATA TRANSMISSION ... 75

5.1 SENDING AND RECEIVING DATA ... 75
5.1.1 Sending Data ... 75
5.1.2 Receiving Data ... 76
5.1.3 Data Transmission Menu ... 77
5.1.4 Transmission Queue (TQ) ... 78
5.1.5 TQ Templates ... 80
5.1.6 Activity Log ... 81
5.1.7 Mailbox Query ... 83
5.1.8 Received File View ... 84
5.1.9 Message Class Manager View ... 85
5.1.10 Views ... 86
5.1.11 Import (.imp) files ... 87
5.1.12 Unattended Transfer User ID and .imp files ... 91

6 EDCONNECT ERROR CODES ... 98

6.1 NUMERICAL ERRORS ... 100
6.1.1 Error -1 ... 100
6.1.2 Special Requirements for Specific Firewalls ... 102
6.1.3 Error 2 ... 102
6.1.4 Error 4.xx ... 103
6.1.5 Error 5.xx ... 104
6.1.6 Error 10 ... 106
6.1.7 Error 13 ... 106
6.1.8 Error 31 ... 106
6.1.9 Error 48 ... 107
6.1.10 Error 70 ... 107
6.1.11 Error 103 ... 107
6.1.12 Error 107 ... 107
6.1.13 Error 118 ... 107
6.1.14 Error 203 ... 107
6.2 NON-NUMERICAL ERRORS ... 108

7 SECURITY AUTHENTICATION ERRORS ... 110

8 MISCELLANEOUS ... 112

8.1 SORTING RECORDS ... 112
8.1.1 Filtering Records ... 112
8.1.2 Changing File Paths ... 113
8.2 GETTING HELP ... 115
8.2.1 Online Help ... 115
8.2.2 The SAIG Help Desk ... 117

9 FREQUENTLY ASKED QUESTIONS ... 118

9.1 HOW DO I IMPORT FILES? ... 118
9.2 HOW DO I PRINT PMESSAGES? ... 119

9.3 WHAT FILES DO I NEED TO MOVE WHEN CHANGING PCS? 120
9.4 WHY AM I GETTING AN "INVALID VALUE" ERROR MESSAGE? 121
9.5 HOW DO I COMBINE FILES? 122
9.6 WHY AM I GETTING AN ERROR NOTIFICATION THAT CANNOT SEND A FILE? 123
9.7 WHAT IS THE DIFFERENCE BETWEEN A SECURITY AUTHENTICATION ERROR AND A NUMERICAL ERROR? 124
9.8 I CHANGED MY SAIG PASSWORD AND NOW I CAN'T TRANSMIT..... 125

APPENDIX A – SAIG USER STATEMENT 1

APPENDIX B – INSTALLING EDCONNECT 8.3 ON COMPUTERS THAT HAVE FDCC SECURITY SETTINGS 2

1 Student Aid Internet Gateway (SAIG) Overview

1.1 Systems Overview

Welcome to the U.S. Department of Education's (ED's) Student Aid Internet Gateway (SAIG).

Through the SAIG, you can send, receive, and manage Federal student aid information electronically. By linking your computer to the resources of various Title IV Application System databases and processing services, the SAIG helps you manage Title IV Federal Student Aid (FSA) information efficiently.

- ***TDNgine (TDN)* —** TDN is a bTrade Commercial-off-the-shelf (COTS) product that is the "engine" of the SAIG application. This application is used as the mailbox application for sending, storing, retrieving, and archiving data. TDN resides on FSA's servers located at the Virtual Data Center (VDC).
- ***TDClient* —** TDClient is a client-side bTrade COTS product used to send and receive FTP data transmissions securely over the Internet. This software is command-line based and ***does not have*** a user interface. TDClient resides on the ***end user's*** computer or server.
- ***TDCommunity Manager (TDCM)* —** TDCM, also known as SAIG Portal, is a web-based bTrade COTS product that allows users to manage their mailboxes and to view data transmissions history to and from mailboxes. This product does not send or receive data.
- ***EDconnect* —** EDconnect is a custom client-side software product used to send and receive data transmissions securely over the Internet. This software presents a user interface for users to send and receive data. The EDconnect is coded in the C++ language and utilizes the TDClient Windows API. The software is installed on the client's standalone PC or in a workstation/network server environment.

Using software provided for the SAIG, you collect data on your personal computer (PC) or computer system and transmit the collected data in batches over the SAIG. The appropriate Title IV Application System receives the data, processes the data, performs any required database cross-referencing, and returns the processed data to your mailbox. In addition to providing a summary of the services available through the SAIG, this guide gives detailed instructions on the installation of EDconnect.

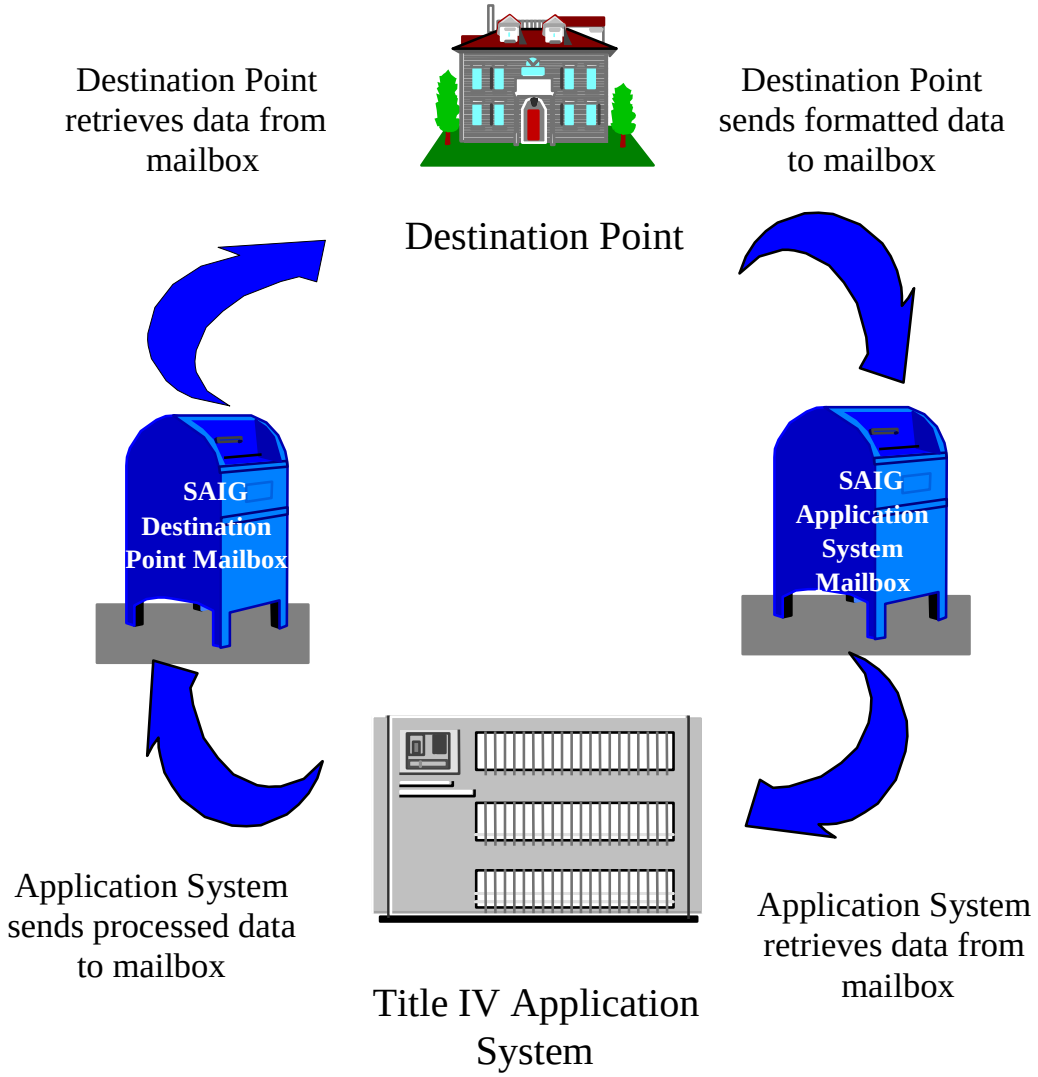
A Help component is available within the EDconnect software. To see a list of available topics, select Help Topics from EDconnect's Help menu. Both the installation guide and EDconnect's online Help are designed to address the needs of non-technical users, although a working knowledge of Windows and the ability to perform basic PC operations are assumed.

By enrolling in the SAIG, you have become a "destination point." FSA provides the EDconnect software to make it possible for you to send and receive data through the

SAIG. In addition, FSA makes other programs and documentation available for additional Title IV Application Systems in which you may have enrolled.

1.2 Store and Forward Data Transmissions

As a destination point, you have been assigned a SAIG electronic mailbox. Using EDconnect or TDClient software, you can retrieve information, sent to you by the Title IV Application Systems, from your mailbox. Using the same software, you can send information to the mailboxes of the Title IV Application Systems. EDconnect, or your mainframe software, will send data to the correct mailbox according to the type of data you are sending. The figure below illustrates the flow of data between a destination point and a Title IV Application System using electronic SAIG mailboxes:



1.3 Destination Point Administration

1.3.1 Destination Point Administrator

The Destination Point Administrator is the term applied to the “owner” of the destination point. The administrator is responsible for the security of data obtained through the SAIG. The administrator controls access to the SAIG through a particular destination point by setting the levels of access to EDconnect and the SAIG for each user. The administrator also maintains SAIG User Statements (see Appendix) for all users of the SAIG at a particular destination point.

1.3.1.1 For Security Groups

Security Groups share a common TG number, a common Connection Type (“Production” or “Test”), a common SAIG password, common access to EDconnect features, and common access to the SAIG. Security Groups can be especially useful for institutions that have separate TG numbers for services such as COD (Pell and/or Direct Loan), CPS, and NSLDS. You can also create more than one Security Group for the same TG number. Changing the password for one Security Group changes the password for all other Security Groups accessing the same TG number and using the same Connection Type.

When a user within a Security Group connects to the SAIG, the user connects with the TG number and SAIG password for that group. The individual user’s name will appear in the Activity Log for each Send or Receive record.

The Destination Point Administrator is responsible for controlling the varying levels of access among the Security Groups set up in EDconnect by managing SAIG passwords, SAIG access, and SAIG connections at the group level.

1.3.1.2 For Users

Users represent individuals within Security Groups sharing common access to EDconnect and the SAIG. The Destination Point Administrator is responsible for controlling each user’s level of access to EDconnect and the SAIG at the group level. User IDs are issued by FSA.

When a user connects to the SAIG and sends or receives data, the user’s name will appear in any Send or Receive record in the User Name column of the Activity Log.

Startup options, color preferences, and file folder locations are established at the user level. User passwords are issued by FSA.

1.3.2 SAIG User Statement

A copy of the SAIG User Statement is shown in Appendix A. This statement may be copied. The Destination Point Administrator should have signed copies of this statement on file for each EDconnect user.

2 Installing EDconnect

This section contains detailed instructions for downloading and installing EDconnect. Instructions are provided for both stand-alone and network installations.

2.1 Hardware and Software Requirements

EDconnect 8.3 requires a connection to the Internet. You must have either a direct connection to the Internet or a dial-up connection through an Internet Service Provider (ISP). Direct connections include local area networks (LANs), digital subscriber line (DSL), T1, and cable modems. If you use a standard modem to connect to the Internet, you have a dial-up connection. This connection must be active (i.e., you must be connected to the Internet) in order to use EDconnect.

To comply with ED requirements, your personal computer must meet or exceed the following minimum configuration:

- IBM or fully IBM-compatible PC with a 1.2 GHz processor.
- 512 MB RAM memory.
- 60 GB hard drive.
- 48X CD-ROM drive (CD-RW recommended).
- Windows compatible keyboard and mouse.
- SVGA graphics adapter capable of 800 X 600 screen resolution or higher.
- 56 kbps analog modem using V.90 and an Internet Service Provider (ISP) *or* a direct connection to the Internet.
- Laser printer capable of printing on standard paper.
- Windows XP Home or Professional, Windows Vista or Windows 7.

2.1.1 Estimating Hard Disk Space Needs

The software takes up the following space on your hard disk:

Product	Size
EDconnect	15 MB
EDExpress	16 MB
SSCR with 300 records	6 MB

Each set of 5,000 records requires the following space:

Record	Size
Direct Loan	49 MB
ISIR	16 MB
NSLDS	7 MB
Packaging	3 MB

2.1.2 Supported Operating Systems

EDconnect can be used as stand-alone or as multi-user software and can be installed on the following Operating Systems:

- Windows XP
- Windows Vista
- Windows 7

In multi-user mode, the EDconnect database (edconn.mdb) can also reside on the following supported network operating systems:

- Windows Server 2003

Users should not run the software on peer-to-peer networks, such as Artisoft LANtastic or Novell's Personal NetWare.

According to the Microsoft Knowledge Base, some anomalies have been known to occur when using Microsoft Access with the following networks: DEC Pathworks, IBM LAN Server, Lantastic, Novell's Personal Netware and Sun PC-NFS. Since EDconnect makes extensive use of Microsoft Access as a database engine, do not use these network operating systems with EDconnect.

2.2 Important Installation Notes

Before you start the installation, be sure to close all Windows applications, including screensavers, e-mail notification programs, and antivirus software.

Installing EDconnect creates default folders and subfolders to manage the transfer of files between different Title IV financial aid software packages and to simplify file management. ED recommends that you use these default folders. If you change the default folders in one software package, you must remember to change the file paths in all the other software packages. Otherwise, EDconnect will not be able to locate the files because the file paths will not match. It is not recommended to change the default folders with installation.

You must be an Administrator on your workstation in order to install EDconnect 8.3. If you are not an Administrator, you will receive a warning when you try to install EDconnect. Once an Administrator has installed EDconnect, you can run it as a member of the Power Users group (Windows XP only). If your EDconnect database is on a network server, you must be a Power User or higher on the network (or “domain”) as well as on your workstation. There are no workarounds for these Windows rights issues. Please consult with your organization’s technical department if you receive a warning that an Administrator must install the EDconnect software.

Note: Department of Education users with Federal Desktop Core Configuration (FDCC) security settings applied to their computers will need to follow an additional step after installing EDconnect 8.3 in order to enable transmissions to the SAIG mailbox server. For step-by-step instructions please see Appendix B at the end of this guide.

2.3 Downloading Software/Paper Documentation

You can download both software and paper documentation from the FSA Download website (www.fsadownload.ed.gov). The amount of time it takes to download a file depends on the file size and the speed of your Internet connection. If you do not have a direct connection to the Internet, we recommend a 56 kbps modem.

The table below shows the minimum possible download time for various file sizes and modem speeds. The actual times will vary, depending on the quality of the telephone line and Internet traffic.

Modem Speed	1 Megabyte	5 Megabytes	10 Megabytes
56 kbps (53 kbps)	3 min.	16 min.	32 min.
768 kbps or higher (typical for cable modems and DSL)	15 sec. or less	1 min., 15 sec. or less	2 min., 30 sec. or less
1.5 mbps or higher (typical for T1 lines)	7.5 sec. or less	37 sec. or less	1 min., 15 sec. or less

Some organizations block their employees from downloading programs from Internet sites. If you have problems downloading from the FSA Download website, try again later. If you continue to experience problems, contact your technical support staff to ensure that you have full download rights.

Paper documentation is available to download from the Internet in Adobe PDF format. The following types of paper documentation are available for you to download:

- Installation and User Guides
- Cover letters
- Other instructions

Each link to the above paper documents is accompanied by a description that includes the date the document was posted, the size of the file, and the approximate download time.

1. Type the FSA Download Web address, “fsadownload.ed.gov”, into the address box at the top of your browser window.

2. Click the “Software and Associated Documents” link to access the page containing descriptions of available Student Aid Internet Gateway Software and Documentation.
3. Click the EDconnect link for the “SAIG Mailbox Software & Manuals: EDconnect, TDClient,TDCM”. This will take you to the download page for EDconnect, TDClient and TDCM.
4. Right-click on the document or Software you want to download under the section “Full Version EDconnect 8.3.0”.
5. Select “Save As”… from the File menu, choose a location on your hard drive, then click the “Save” button to save the file.
6. Once you have downloaded the file, go to the location on your hard drive where you saved it. Double-click the file to open the document.

2.3.1 Downloading the Software

The installation package for EDconnect 8.3 is available on the FSA Download website (www.fsadownload.ed.gov). Follow the steps below to download the EDconnect 8.3 software

1. Type the FSA Download web address, “fsadownload.ed.gov”, into the address box at the top of your browser window.
2. Click the **Full Download** link to download EDconnect 8.3. A **Save As…** dialog box will appear.

   Note: If clicking the **Full Download** link takes you to a new Web page rather than starting the download process, click the **Back** button on your browser and right-click the **Full Download** link. Choose **Save Target As…** from the pop-up menu in order to start the download process.
3. Select a location on your hard drive in which to save the file, or accept the default location. The Windows Desktop is a convenient place to save the file and locate it later. Click the **Save** button. The length of time it will take the file to download depends on the speed of your Internet connection. See the table of download times in this section.

Note: We recommend that you download the installation file to a folder other than the one in which you will install EDconnect. You may want to create a folder called “FSA Download,” for example, specifically for the installation files you download from the FSA Download website.

Once you have downloaded the installation file to your hard drive, go to the folder containing the **EDconn830.exe** file and double-click it to start the installation. Go to the *Installing EDconnect* section of this guide for further instructions.

Note:

- Downloading the software does **not** install it.
- You should have no other programs running while you are installing EDconnect.

2.4 Installing EDconnect

Follow the steps below to install EDconnect 8.3.

1. Close any programs that are running, including antivirus software.
2. Locate the **EDconn830.exe** file you downloaded and double-click it to start the installation.

   Note: The installation process begins and a **Welcome** screen appears.
3. Select the Next button and the Installation Type dialog box will open.
4. You will be prompted to select the type of installation: Local Install, Local Install - Custom, Network Install, or Workstation Install. During installation, you can click once on an option to highlight it, and view its description at the bottom of the dialog box. Please read the explanation of each installation option below:

   - Select **Local Install** if you are installing EDconnect, including the database, on a single PC for the first time. By selecting **Local Install**, you will install all EDconnect components, including the database, to your local hard drive.
   - Select **Local Install - Custom** if you already have an EDconnect 8.3 database to your local hard drive. By selecting **Local Install - Custom**, you will install all EDconnect components except the database to your local hard drive

   Note: The EDconnect software defaults to **Local Install – Custom** when prompted to select a install option

   - Select **Network Install** if you do not have an existing EDconnect 8.3 database in a network location and want a number of PCs to have common access to a single EDconnect database. Performing a **Network Install** places the EDconnect database (**EDconn8.mdb**) on your Local Area Network (LAN). The EDconnect database contains the information users will share, such as the Activity Log and Security View information. A **Network Install** does not install the program itself. After a **Network Install**, you must perform a **Workstation Install** on each PC to install the program files.

   Note: Record the location of the EDconnect database when performing a **Network Install**. You will need this information when performing the **Workstation Install.**

   - Select **Workstation Install** if you already have an EDconnect 8.3 database on your network. Perform a **Workstation Install** on each PC that you want to access the EDconnect database. **Note:** You must perform a **Network Install** before performing a **Workstation Install** if you do not already have an EDconnect 8.3 database on your network. The **Workstation Install**

checks for a valid EDconnect database in the selected network location before proceeding.

5. Select the type of installation by clicking once on the option and then on the **Next** button. The **Destination Folder** dialog box will appear on your screen. Depending on your operating system, the default destination folder is **C:\Program Files\EDconnect8** for a local installation. Make note of where the destination folder is.

   Note: For a network installation, you will need to select the appropriate LAN drive as the database location. You can accept the default folder or change the destination folder by using the Browse button.

6. Select **Next** and the **Select Program Folder** dialog box will appear on your screen. This dialog box enables you to enter a new folder name, select an existing folder, or accept the default folder name of EDconnect8.

7. Select Next and the **System Information** dialog box will appear on your screen. This dialog box provides information about your computer system. You can ignore this information or verify it against the minimum system requirements in the Hardware and Software Requirements section of this guide.

8. Select **Next** and the **Install Settings** dialog box will appear, confirming that setup has enough information to begin copying files to your PC. If you want to review or change any of the settings, click on the Back button to return to the appropriate dialog box.

9. Select **Next**. A progress bar appears, showing you the progress of files being copied to your hard drive. When the installation is finished, EDconnect will open a window containing icons for the program and for Transmission Queue templates.

   Note: If you want to create a shortcut to EDconnect on your Desktop, right-click on the EDconnect icon and select **Send To** from the menu, then select **Desktop (create shortcut)**.

10. Click **Finish**. The installation program will ask you to restart your computer.

Note: Department of Education FSA users with FDCC security settings on their computer will need to follow an additional step after installing EDconnect 8.3 in order to enable transmissions to the SAIG mailbox server. For step-by-step instructions please see Appendix B at the end of this guide.

Helpful Hints

- The EDconnect database contains a record of data transfers but does **not** physically contain any of the files you have sent or received. All files you have sent or received are stored in a separate location and are unaffected by the EDconnect database. Other databases you may have on your

computer, such as the EDExpress, or SSCR databases, are also unaffected by the EDconnect database.

- During the installation, EDconnect creates several Transmission Queue (TQ) template icons in the EDconnect Program Group. These icons enable quick access to commonly used default TQ template files. If you select one of these icons, EDconnect will start and will automatically fill in the Transmission Queue with the appropriate data requests. For example, selecting the **all.tqt** icon starts EDconnect and places a request in the Transmission Queue for all data and all messages currently in your mailbox.
- You can drag or copy these TQ icons, along with the EDconnect icon, to your desktop from the icon window that appears at the end of the installation.

2.5 Setting Up EDconnect

The following instructions will lead you through the steps necessary to setup EDconnect 8.3. These instructions assume that you have installed EDconnect 8.3 for the first time. Remember this version is *not* an upgrade from EDconnect 7.X.

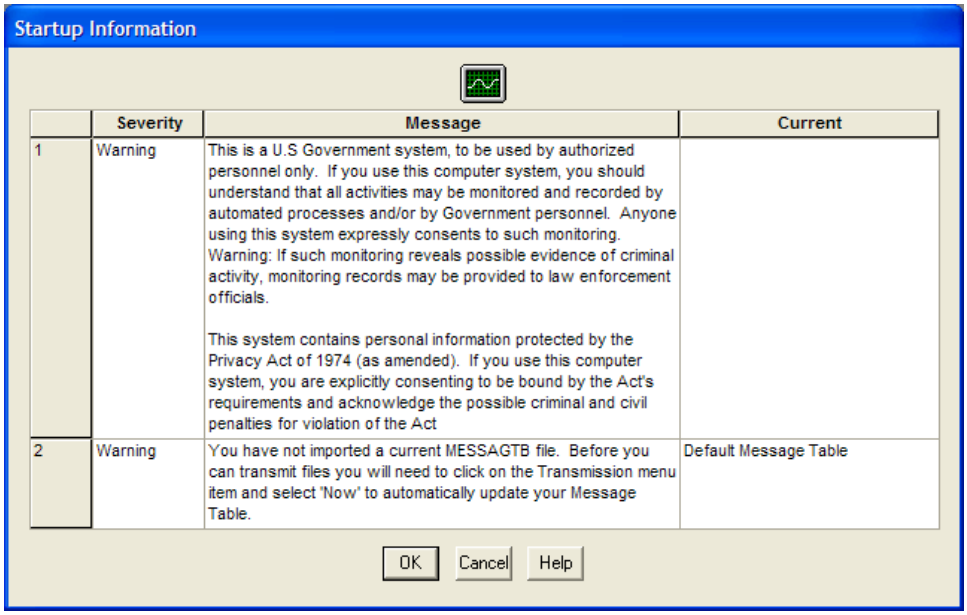
EDconnect users will also need to obtain an **FSA User ID, FSA User Password** and **Security Token** from FSA prior to beginning set up. The **Security Token** is a physical token that you will use to generate a **One-Time Password** to enter into the **Security Code** field.

Note! You must be connected to the Internet before you start EDconnect.

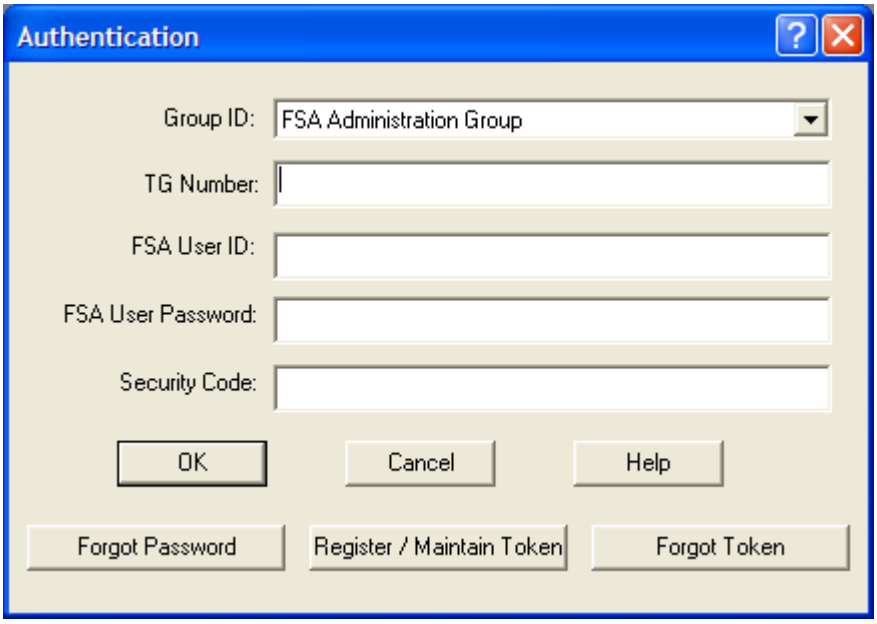
Security Settings can be imported from EDconnect 7.X; however, any imported users must be updated to FSA User IDs.

2.5.1 Setting Up EDconnect With Imported Security Settings

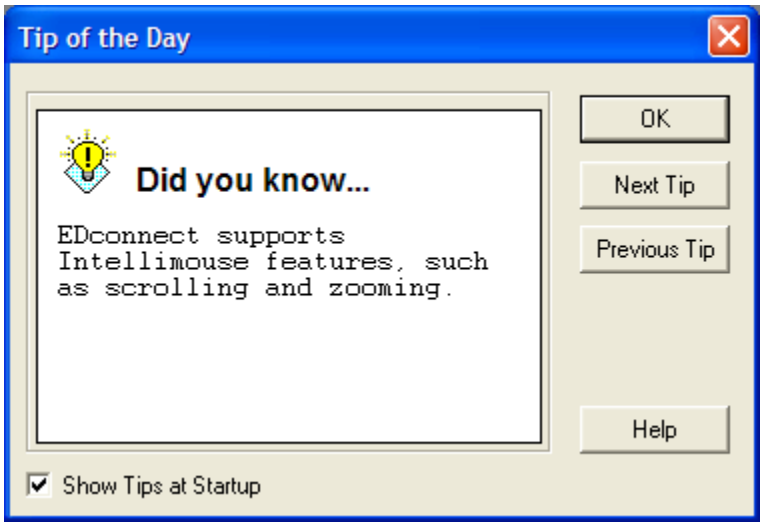
1. **Start EDconnect.** When you run EDconnect for the first time, a startup information dialog box will appear. This contains warnings about using EDconnect and both critical and non-critical issues.



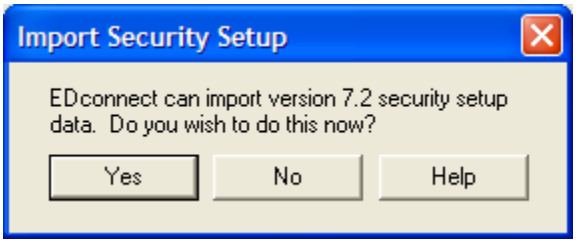
2. **Log in to EDconnect.** After you accept the warnings, a Security Authentication dialog box will appear with the default group name of **"FSA Administration Group"** already selected. Enter your **TG Number**, **FSA User ID**, **FSA User Password** and **One-Time Password**, if applicable, and click OK.



- You will immediately see the “Tip of the Day” dialog box.

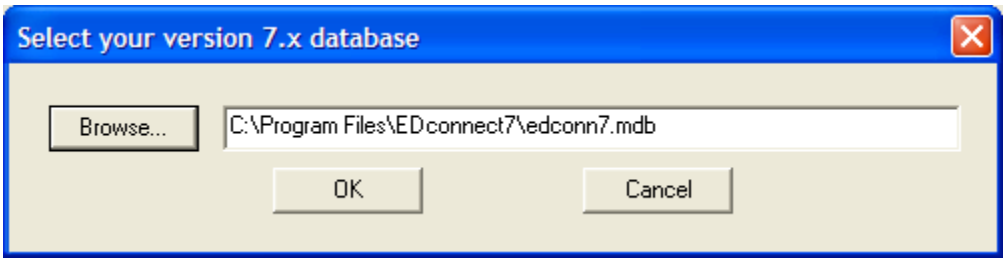


3. **Import Security Settings.** Next, EDconnect will prompt you to import your security settings (Security Groups and Security Users) from the EDconnect 7.X database.

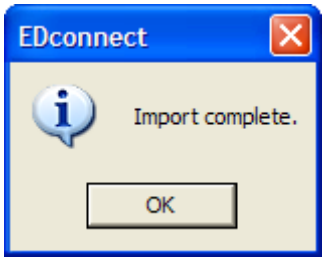


- If you do not have EDconnect 7.X installed or choose “No”, skip to section 2.5.2 “Setting up EDconnect without Imported Security Settings”. If you have EDconnect 7.X installed and set up on your system and would like to import your security settings, click “Yes”. You will receive a prompt with the default location of the EDconnect 7.X database – if it is installed in that location.

Note – If the EDconnect 7.X database was installed in a non-default area, you will need to use the browse feature to locate it.

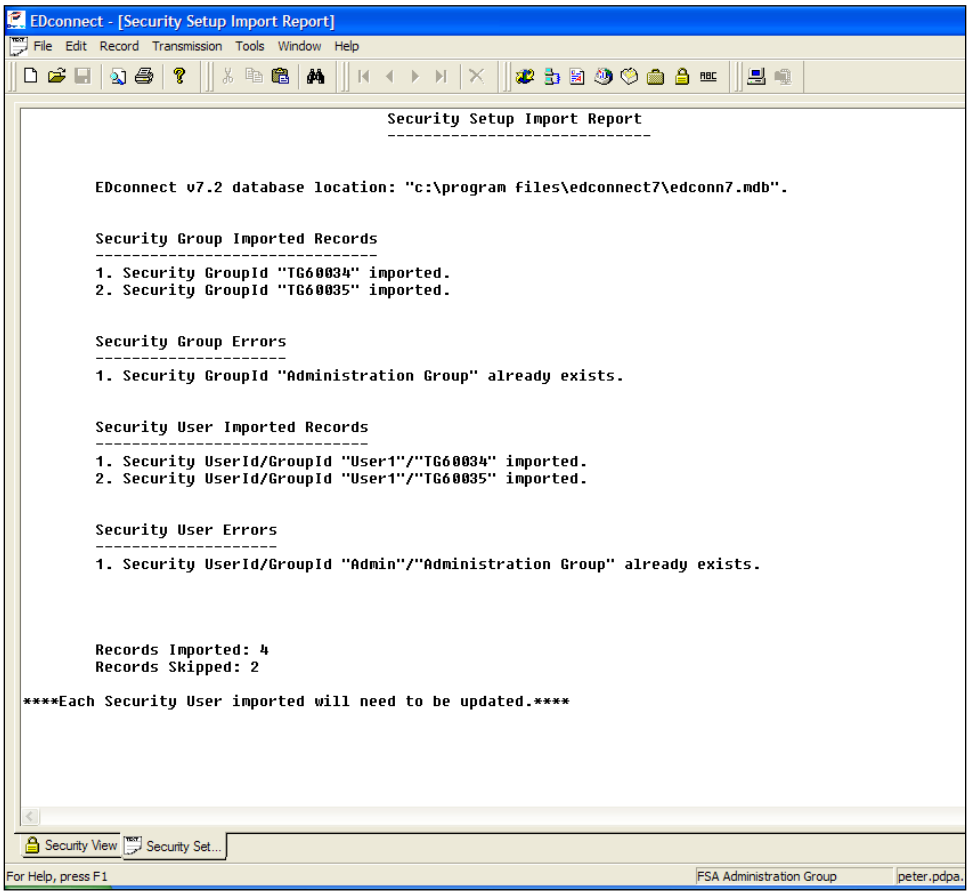


- If you choose OK, you will receive the confirmation dialog box.

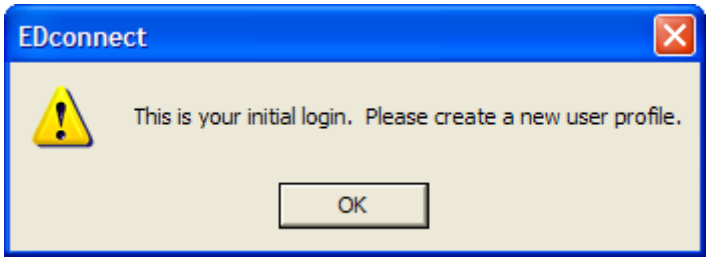


Note: You cannot import security settings from EDconnect 6.X.

- After you click OK, you will see the Security Settings Import Report displayed behind it.



4. **Create an FSA User ID.** After you import the security settings, EDconnect will prompt you to create the profile of the **FSA User ID** you logged in with. The User Wizard will guide you through this. It is important to make sure that imported users are updated from their former ID to an **FSA User ID** before they attempt to login. If they are not updated, they will not be allowed access to EDconnect.



- After you create your profile, you will see the Security Setup Import Report displayed.

5. **Create a Security Group.** Only an **FSA User ID** belonging to the **FSA Administration Group** can create other security groups. To create a security group, right click on the EDconnect folder in the **Security View** and choose

Insert. The **Group Wizard** will lead you through the tabs of the **Group Properties** dialog box. The **Group Properties** settings control your access to the SAIG, as well as each user's access within a group. The **FSA Administration Group** cannot conduct transmissions and therefore does not have a password field in the Network tab. Once your **FSA Administration Group** is created, you will need to create the required security groups for your institution in order to transmit.

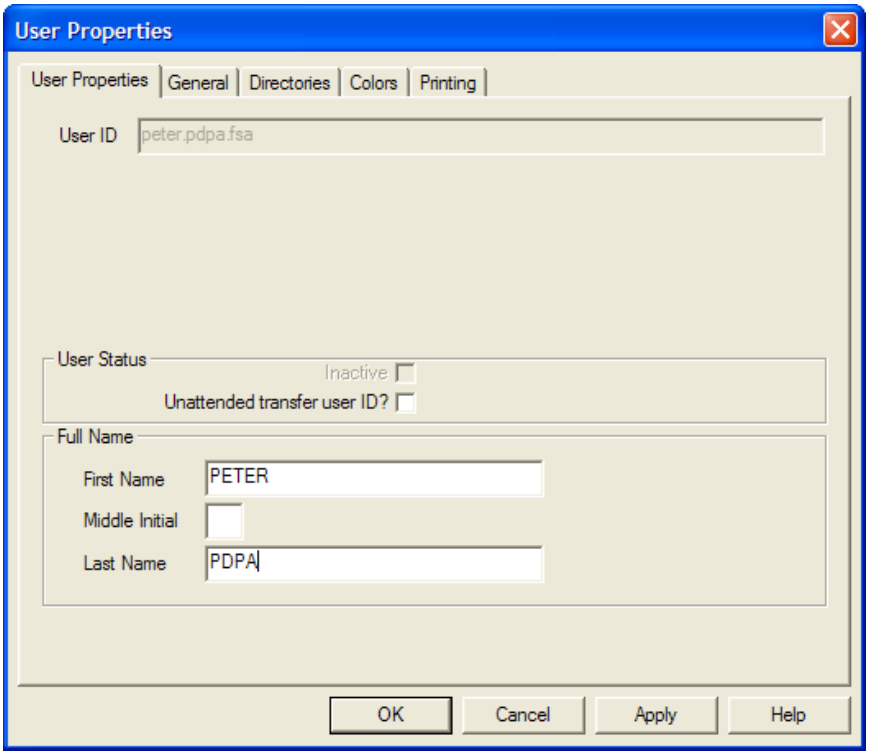
6. **Perform a Local Only password change.** During the initial setup of your non-Administration security group, EDconnect will prompt you for a new SAIG password. The first step in establishing your SAIG password is to perform a **Local Only** password change.
   - If you are installing EDconnect to access a *new* SAIG mailbox, the initial password is set as follows: "ccyynnnn" where "ccyy" is your birth year and "nnnn" represents the last four digits of your social security number. Enter your initial password as the **Local Only** password. Go to **Step 7**.
   - If you are installing EDconnect in order to access an *existing* SAIG mailbox you have been accessing with an earlier version of EDconnect, enter the SAIG password you used in the previous version as the **Local Only** password. Under these circumstances, you do not need to perform a **Network and Local** password change. Skip to **Step 8**.
   - If you have already performed a **Local Install** of EDconnect on another computer in your office and have transmitted a SAIG password from that computer, enter *that* SAIG password as a **Local Only** password change. Under these circumstances, you do not need to perform a **Network and Local** password change. Skip to **Step 8**.
7. **Change your SAIG password.** After you perform a **Local Only** password change, you must perform a **Network and Local** password change to establish your password on the SAIG. When you change your SAIG password, be sure to select **Network and Local**. This adds a password change record to the **Transmission Queue**. EDconnect will transmit the password change the next time you connect to the SAIG.
8. **Set up a personal FSA User ID.** After you set up your **FSA Administration Group** profile, you will need to set up your **FSA User ID**. To create a new user, select the group name, right click and select Insert. The **User Wizard** will lead you through the tabs of the **User Properties** dialog box.

Note - While an FSA Administration Group member cannot transmit, the **FSA User ID** is associated with a **TG Number**, which is why a **TG Number** is required for authentication with the **FSA Administration Group.** All users in this group must belong to the same **TG Number**.

After you have accessed EDconnect, you will have to set up your user profile. When you have finished, you will be allowed access into EDconnect. At this point, you can create other group IDs and **FSA User IDs** for each person who will be using EDconnect at your institution. All user IDs and passwords are issued by FSA.

When you set up a FSA User ID, you will notice a small box on the User Profile box labeled “Unattended Transfer User ID?” If you will be sending .imp files with this user ID, you will need to check this box to allow the user this permission.

Note: Unattended users will not display in the dropdown list of the Security Authentication screen and will not be able to log in. It is not recommended that you make an FSA User ID into an unattended user. See *Section 5.1.12 Unattended Transfer User ID and .imp Files* for more detailed information about setting up unattended users.



9. **Download the message class table.** Message class tables “teach” EDconnect what kinds of files it can send and receive. These tables are placed periodically into your SAIG mailbox. Your mailbox will contain the latest message class table. When you connect to the SAIG, it will automatically download to your PC and import into EDconnect.

10. **Coordinate global file paths for sending and receiving files.** EDconnect does not automatically create paths for sending and receiving data. If you do not specify **Send** and **Receive** paths, EDconnect will use the paths listed in the **Filename** field of the **Message Class Manager**.

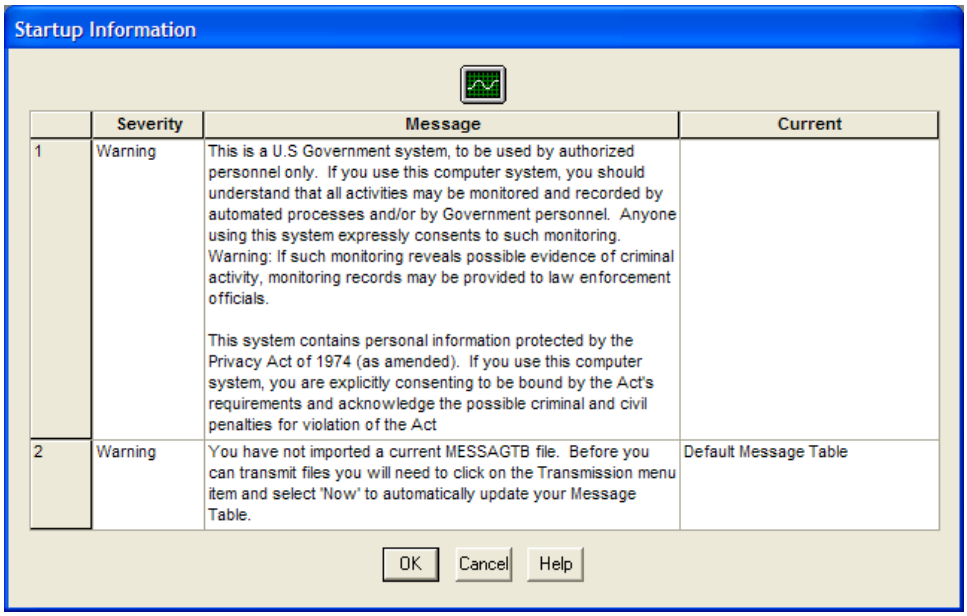
    - Once you have gained access to EDconnect, you can change the paths on the **Directories** tab of the **User Properties** dialog box. Right-click the **FSA User ID** you wish to edit and select **Properties** from the pop-up menu. Click

the **Directories** tab. At the top of the tab, a drop-down list will enable you to select **Database**, **Send**, or **Receive**.

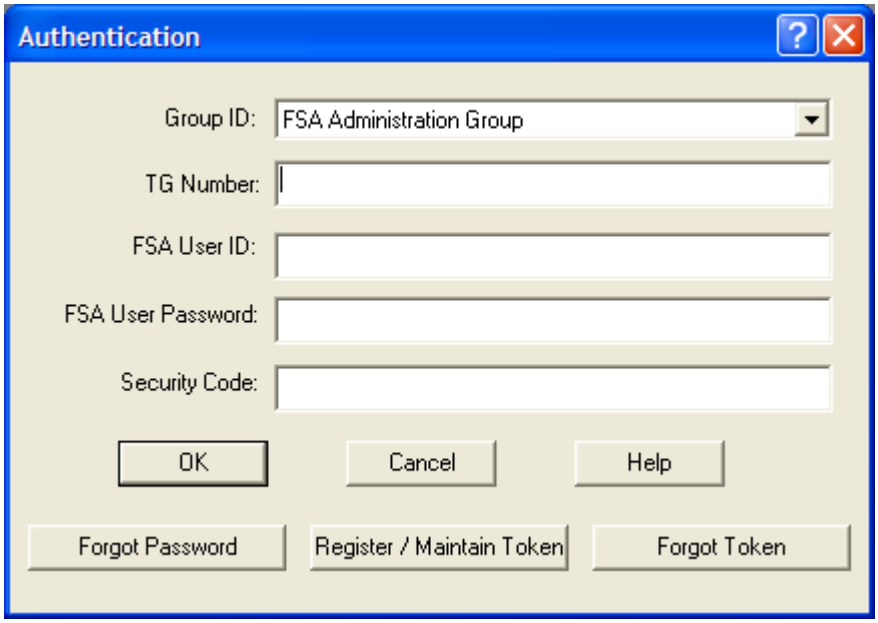
- The **Database** path will reflect the current location of the EDconnect database, but the **Send** and **Receive** paths will be blank. Select **Send** or **Receive**, then type in the full path, including drive letter, or use the **Browse** button to find the correct folder.
- Be sure to enter a location for both the **Send** and **Receive** folders. If you would like to use the same setting for all existing users in a specific group, place a check in the box marked “Set all users of this group to the specified directories.”

2.5.2 Setting up EDconnect without Imported Security Settings

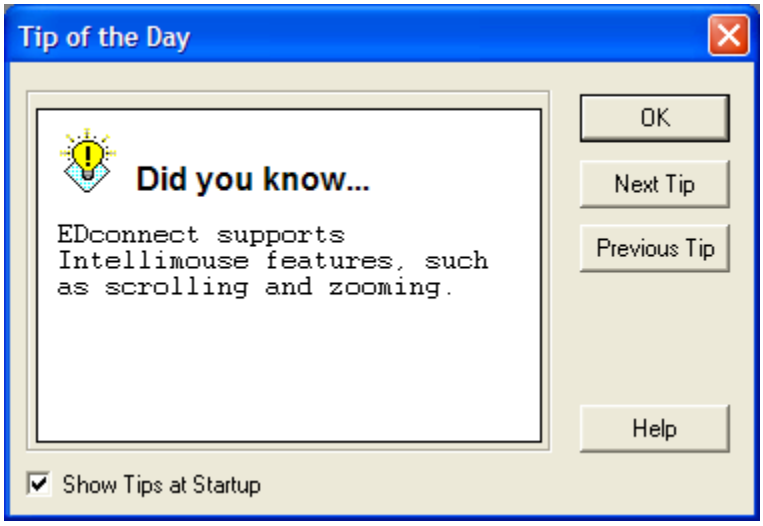
1. **Start EDconnect.** When you run EDconnect for the first time, a startup information dialog box will appear. This contains warnings about using EDconnect and both critical and non-critical issues.



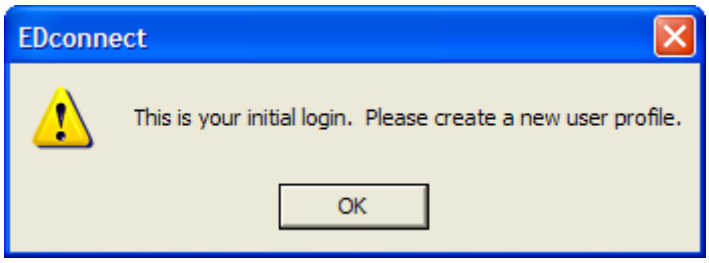
2. **Log in to EDconnect.** After you accept the warnings, a Security Authentication dialog box will appear with the default group name of **"FSA Administration Group"** already selected. Enter your **TG Number**, **FSA User ID**, **FSA User Password** and **One-Time Password**, if applicable, and click OK.



- You will immediately see the “Tip of the Day” dialog box.

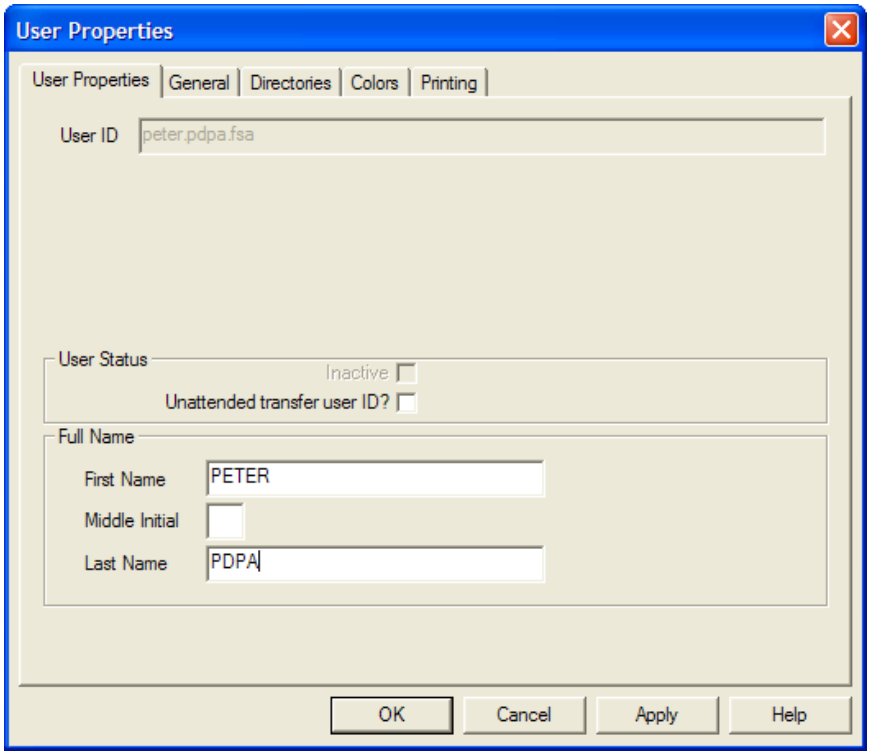


3. **Import Security Settings.** Next, EDconnect will prompt you to import your security settings (Security Groups and Security Users) from the EDconnect 7.X database. If you do not have EDconnect 7.X installed or do not want to import those setting, choose **No**. If you choose **Yes**, go back to section *2.5.1 Setting Up EDconnect with Imported Security Settings*.
4. **Create an FSA Administration Group Profile.** After you decline to import the security settings, EDconnect will prompt you to create the profile of the **FSA User ID** you logged in with. The User Wizard will guide you through this.



5. **Create a Security Group.** Only an **FSA User ID** in the **FSA Administration Group** can create other security groups. To create a security group, right click on the EDconnect folder in the **Security View** and choose **Insert**. The **Group Wizard** will lead you through the tabs of the **Group Properties** dialog box. The **Group Properties** settings control your access to the SAIG, as well as each user’s access within a group. The **FSA Administration Group** cannot conduct transmissions and therefore does not have a password field in the Network tab. Once your **FSA Administration Group** is created, you will need to create the required security groups for your institution in order to transmit.

6. **Perform a Local Only password change.** During the initial setup of your non-Administration security group, EDconnect will prompt you for a new SAIG password. The first step in establishing your SAIG password is to perform a **Local Only** password change.
   - If you are installing EDconnect to access a new SAIG mailbox, the initial password is set as follows: “ccyynnnn” where “ccyy” is your birth year and “nnnn” represents the last four digits of your social security number. Enter your initial password as the Local Only password. Go to **Step 7**.
   - If you are installing EDconnect in order to access an existing SAIG mailbox you have been accessing with an earlier version of EDconnect, enter the SAIG password you used in the previous version as the Local Only password. Under these circumstances, you do not need to perform a Network and Local password change. Skip to **Step 8**.
   - If you have already performed a Local Install of EDconnect on another computer in your office and have transmitted a SAIG password from that computer, enter that SAIG password as a Local Only password change. Under these circumstances, you do not need to perform a Network and Local password change. Skip to **Step 8**.
7. **Change your SAIG password.** After you perform a **Local Only** password change, you must perform a **Network and Local** password change to establish your password on the SAIG. When you change your SAIG password, be sure to select **Network and Local**. This adds a password change record to the **Transmission Queue**. EDconnect will transmit the password change the next time you connect to the SAIG.
8. **Set up a personal FSA User ID.** After you set up your **FSA Administration Group** profile, you will need to set up your **FSA User ID**. To create a new user, select the group name, right click and select Insert. The **User Wizard** will lead you through the tabs of the **User Properties** dialog box.
   - When you set up a FSA User ID, you will notice a small box on the User Profile box labeled “Unattended Transfer User ID?”. If you will be sending .imp files with this user ID, you will need to check this box to allow the user this permission.
   - **Note**: Unattended users will not display in the dropdown list of the Security Authentication screen and will not be able to log in. It is not recommended that you make an FSA User ID into an unattended user. See *Section 5.1.12 Unattended Transfer User ID and .imp Files* for more detailed information about setting up unattended users.



8. **Download the message class table.** Message class tables "teach" EDconnect what kinds of files it can send and receive. These tables are placed periodically into your SAIG mailbox. Your mailbox will contain the latest message class table. When you connect to the SAIG, it will automatically download to your PC and import into EDconnect.

9. **Coordinate global file paths for sending and receiving files.** EDconnect does not automatically create paths for sending and receiving data. If you do not specify **Send** and **Receive** paths, EDconnect will use the paths listed in the **Filename** field of the **Message Class Manager**.

   - You can change the paths on the **Directories** tab of the **User Properties** dialog box. Right-click the **FSA User ID** you wish to edit and select **Properties** from the pop-up menu. Click the **Directories** tab. At the top of the tab, a drop-down list will enable you to select **Database**, **Send**, or **Receive**.
   - The **Database** path will reflect the current location of the EDconnect database, but the **Send** and **Receive** paths will be blank. Select **Send** or **Receive**, then type in the full path, including drive letter, or use the **Browse** button to find the correct folder.
   - Be sure to enter a location for both the **Send** and **Receive** folders. If you would like to use the same setting for all existing users in a specific group, place a check in the box marked "Set all users of this group to the specified directories."

2.5.3 Setting up a Test Security Group

If you have been advised to do so, EDconnect 8.3 enables you to set up a test Security Group to send and receive files from the SAIG test system without interfering with your production Security Group(s). See *Section 3.4 Security Groups* for further information about setting up a test Security Group.

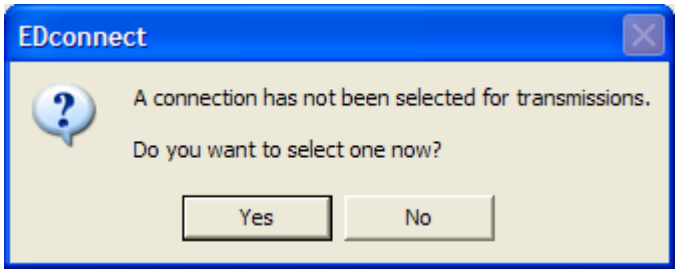
2.5.4 Selecting a Connection

EDconnect 8.3 uses the Internet to access the SAIG. You will need to be connected to the Internet before you can login to EDconnect. Your Internet connection to the SAIG has no relationship to the dial-up connection used by earlier versions of EDconnect.

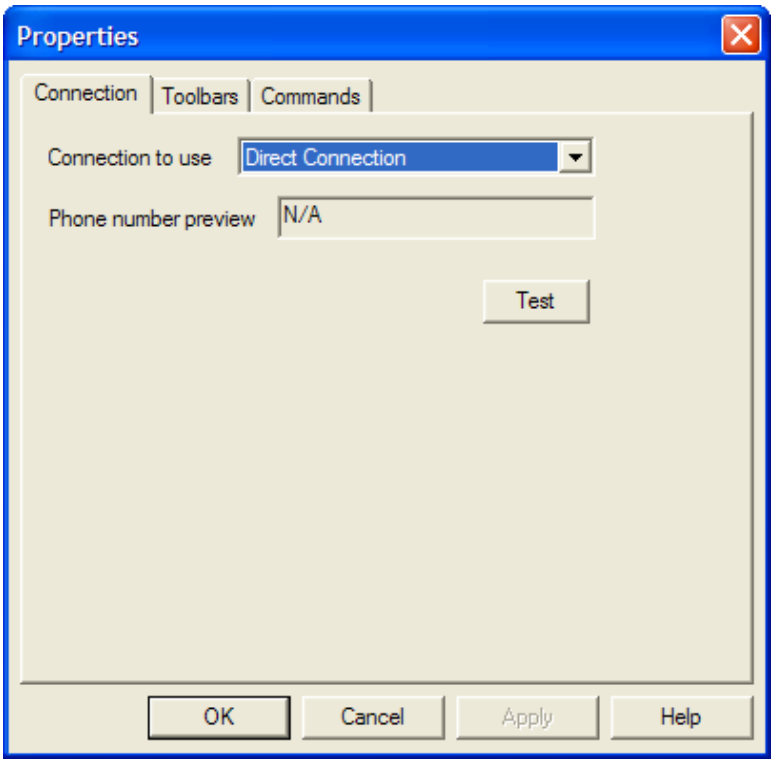
The first **FSA User ID** to login *after setup* that is not in the **FSA Administration Group** will be prompted to set a connection. This only needs to be done once.

2.5.4.1 Setting up the Connection When Prompted

1. Start EDconnect and login via the **Security Authentication** screen as a new first time **FSA User**. You will then receive the set-up connection prompt.

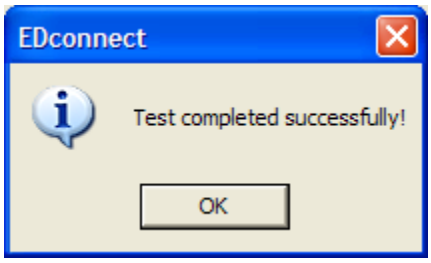


2. If you select **No**, skip to *3.6.1 Selecting a Connection* for details on how to setup the connection later. Note that you cannot transmit until this connection is set up. If you choose yes, you will get the Connection Properties dialog box.

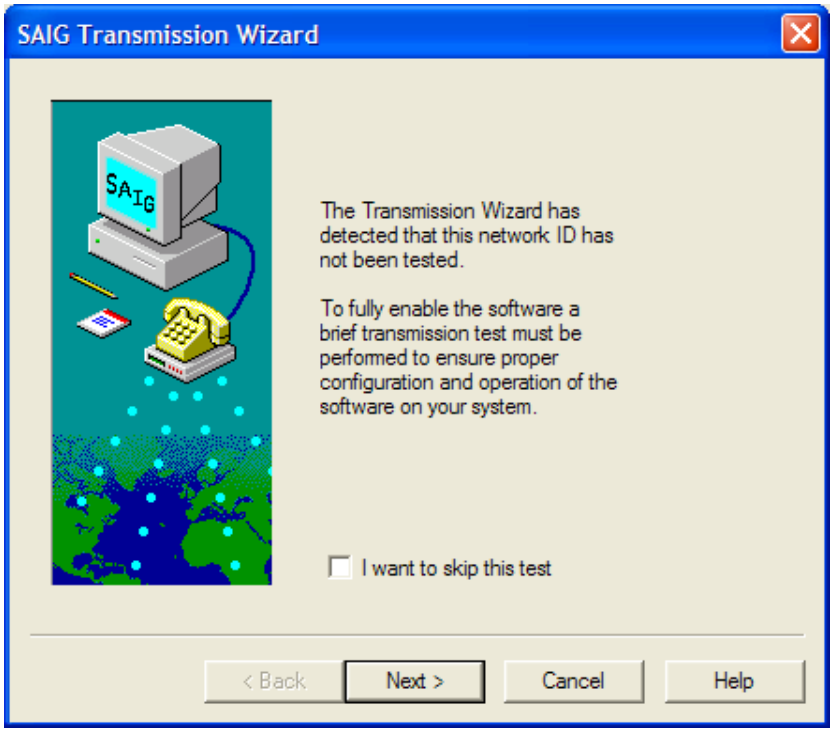


- The drop-down list in the Connection to use selection box displays a list of Internet connections available on your computer. If you have a direct connection to the Internet, such as DSL, T1, or cable, "Direct Connection" may be the only option listed. If you connect to the Internet using a modem and an Internet Service Provider (ISP), in most cases your ISP's dial-up connection will appear on the list.

3. After selecting your connection, click the **Test** button. You will receive a confirmation message.



4. This will be followed by the Transmission Wizard.

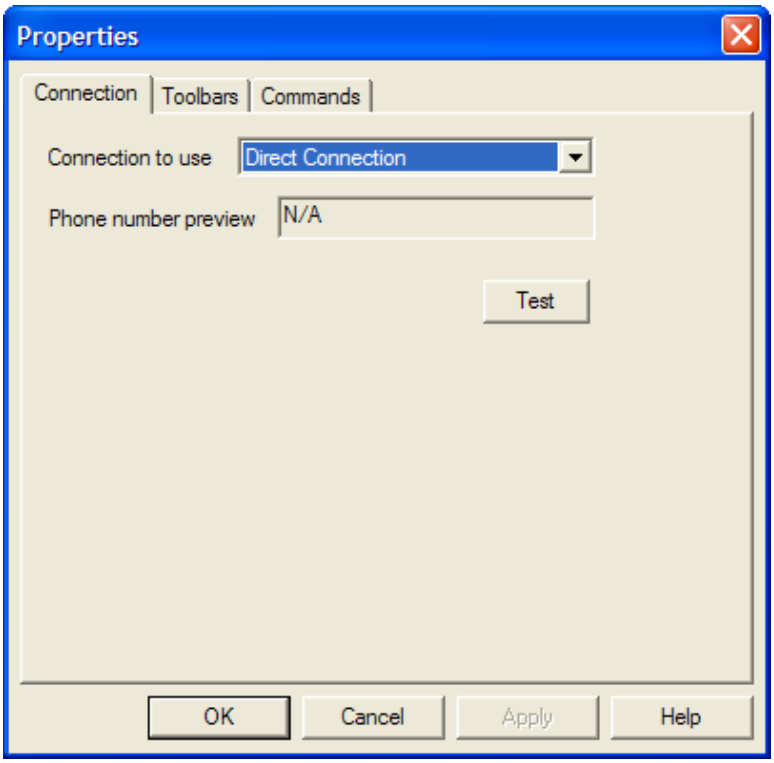


- It is a good idea to run the transmission test to verify that your connection is good and you have the ability to transmit successfully.

2.5.4.2 Setting up the Connection Without Prompts

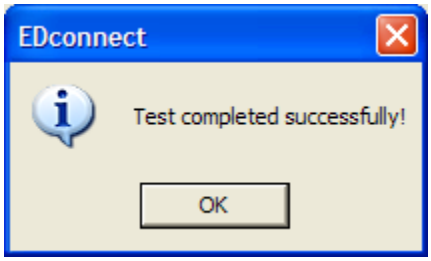
If you opted No at the prompt, or want to set the connection later, follow these steps. Remember that if you do this while logged in under FSA Administration Group, you will not be able to access the Transmission Wizard or run a transmission test.

1. Select Tools from the EDconnect main bar menu, then Customize. You should see the Connection Properties dialog box.



- The drop-down list in the **Connection to use** selection box displays a list of Internet connections available on your computer. If you have a direct connection to the Internet, such as DSL, T1, or cable, “Direct Connection” may be the only option listed. If you connect to the Internet using a modem and an Internet Service Provider (ISP), in most cases your ISP’s dial-up connection will appear on the list.

2. After selecting your connection, click the **Test** button. You will receive a confirmation message.



3. You will not receive the Transmisson Wizard at this point. You can however, test the transmission connection at any time by choosing **Test** under the Transmission menu in the main EDconnect menu bar.

Helpful Hints

- Some ISPs use proprietary connections that are created when you install their communications software. Although EDconnect *may* be able to dial your ISP and connect to the Internet through a proprietary dial-up connection, the connection may use protocols that will prevent EDconnect from sending and receiving data over the SAIG. Some ISP-provided communications programs do not create standard dial-up connections at all, so your Internet connection may not appear on the **Connection to use** drop-down list.
- You can select "Direct Connection" even if you connect to the Internet using a modem and an ISP. Once you connect to the Internet through your ISP, the open Internet connection becomes a "Direct Connection" that will enable EDconnect to communicate with the SAIG. You must be connected to the Internet before using EDconnect.
- If you select "Direct Connection," you will need to connect to the Internet through your ISP the way you normally connect *before* using EDconnect.
- If you select your ISP's dial-up connection and are unable to send and receive data using EDconnect, select **Customize** from the **Tools** menu and choose "Direct Connection" from the **Connection to use** drop-down list. You will need to connect to the Internet through your ISP the way you normally connect *before* using EDconnect if you select "Direct Connection."
- Do *not* select any dial-up connections associated with previous versions of EDconnect, such as "SAIG-0" or "T4WAN-0." EDconnect 8.3 cannot use these connections.

2.5.4.3 Firewalls

A firewall is a barrier between your computer or your Local Area Network (LAN) and an external source, such as the Internet. The barrier can be software, hardware, or a combination of the two. A firewall examines each packet of information coming into and

going out of your computer and prevents unauthorized packets from being sent or received.

A port is a pre-defined “channel,” numbered from 0 to 65535, used by your computer to send and receive specific kinds of data. Your computer usually sends and receives e-mail through port number 25 and makes standard Internet connections through port number 80.

A firewall can prevent EDconnect from communicating with the SAIG by blocking the packets of information your computer is trying to send to and receive from the SAIG. If you have trouble connecting to the SAIG after installing EDconnect 8.3, contact your technical support staff to see if you are behind a firewall. “Error -1” usually means that the port used by EDconnect to send and receive data is blocked. Your technical support staff will need to open port number 26581 for inbound and outbound TCP/IP traffic and give your computer access to **saigmailbox.ed.gov** (**saigmailboxdev.ed.gov** for the test system) to enable EDconnect to communicate through the firewall.

In order to use the **Transaction Delivery Community Manager** (**TDCM**), you need to be able to connect to **saigportal.ed.gov** and will need standard internet port number 80 (HTTP) and port number 443 (SSL) open. Information about using the TDCM is available in the SAIG Mailbox Software & Manuals: EDconnect, TDClient and TDCM section on the FSA Download website (www.fsadownload.ed.gov).

2.5.4.4 Getting Help

For help installing or using EDconnect, contact the SAIG Help Desk at 800-330-5947 or by e-mail at **CPSSAIG@ed.gov**.

3 Using EDconnect

3.1 Destination Point Administration

The Destination Point Administrator (DPA) is the “owner” of the Student Aid Internet Gateway (SAIG) mailbox and is responsible for security within EDconnect. The DPA creates and controls **Security Groups** and the users within those groups through the **Security View**.

Security Groups share a common **TG number**, a common **Connection Type** (“Production” or “Test”), a common **SAIG Password**, and common access to the SAIG. The main purpose of separating users into groups is to regulate user access within EDconnect. Groups can also be useful for dividing functions among users. Folder icons represent **Security Groups** in the **Security View**.

Users are individuals within **Security Groups** who share a common access to EDconnect and the SAIG.

- Each **FSA User ID** has its own **FSA User Password**. The DPA should have a signed **SAIG User Statement** on file for each user.
- When you enroll through the SAIG Enrollment Site (**fsawebenroll.ed.gov)**, you are required to print the **SAIG User Statement** as part of the online enrollment process.
- You should retain the statements at your institution for auditing purposes.

Helpful Hints

- You control **SAIG Passwords** at the *group* level.
- FSA controls and issues access to EDconnect.
- You control startup options, color preferences, and file directory locations at the *user* level.
- **FSA User IDs** can belong to multiple groups in the **Security View**.

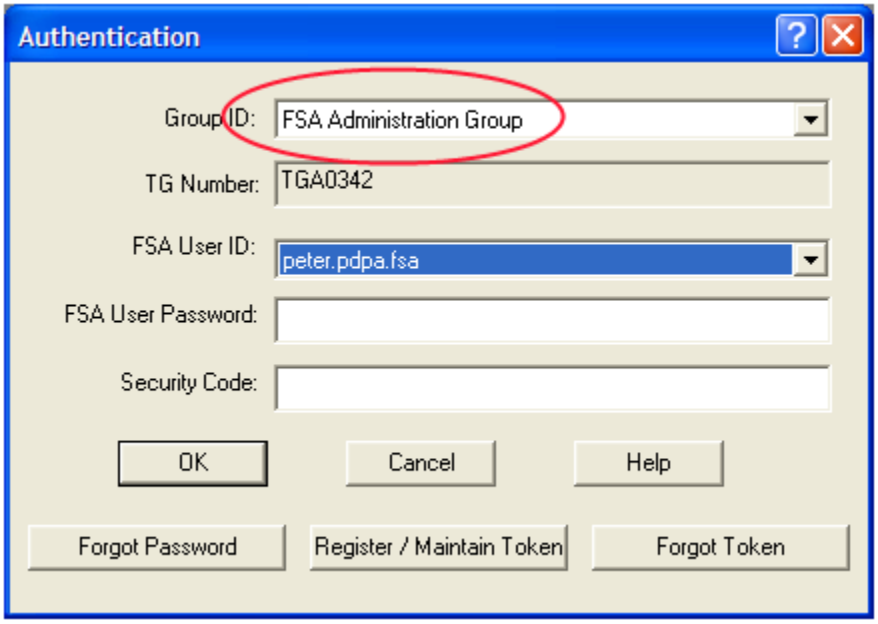
3.2 Security Authentication for User Logons

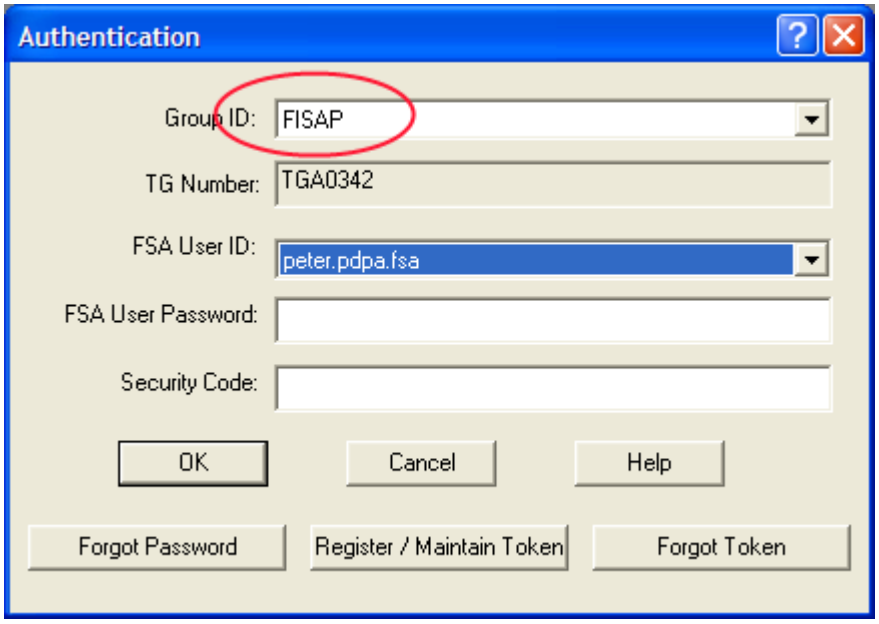
An **FSA User ID** can belong to several different **Security Groups** within EDconnect. This method enables a single user to send and receive data using different **TG numbers** and **Connection Types** ("Production" or "Test").

EDconnect utilizes Two-Factor Authentication (TFA) to authenticate a user. User IDs and passwords are issued by FSA. Access to EDconnect requires a **Group ID**, **TG Number**, **FSA User ID**, **FSA User Password**, and a **One-Time Password** (when applicable). After the initial rollout of TFA tokens, all **FSA Users IDs** will be required to enter a **One-Time Password**.

- FSA will issue your institution a Security Token. This is a physical token that will generate a One-Time Password that is required to log into EDconnect.
- Each group can be associated with a different TG number.
- If a user belongs to more than one group, the EDconnect Security Authentication dialog box enables the user to select the group to log in under for that session.

In the illustrations below, the FSA User ID "peter.pdpa.fsa" belongs to both the "FSA Administration Group" and the "FISAP" group. He can login to the software under either group.





The **Security Code** field is where a user will enter the **One-Time Password** generated by a physical token that is issued by FSA. This token must be registered through FSA. To register a token select the **Register/Maintain Token** button on the Security Authentication screen. Users will then be routed to the **Login - AIMS TFA Portal**.

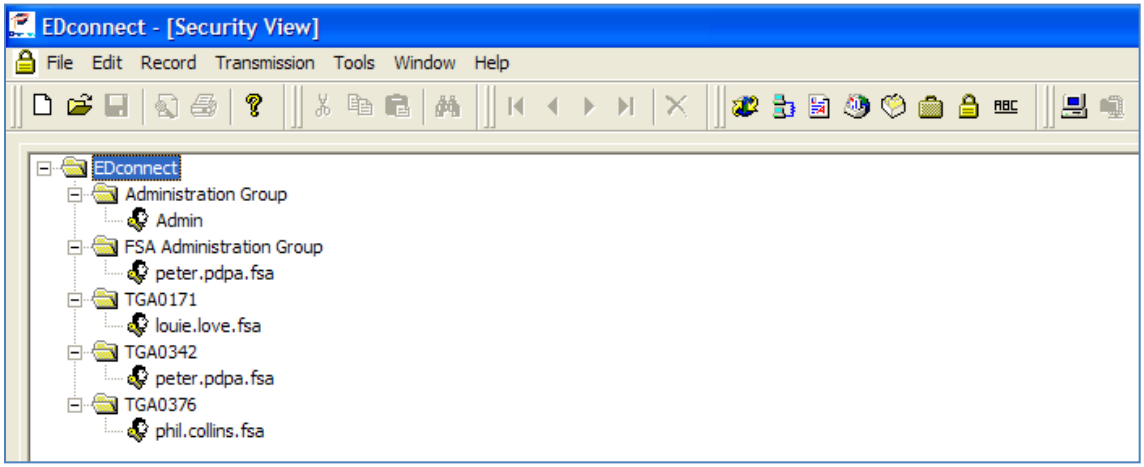
If you have forgotten your token and cannot generate the **One-Time Password**, you can reset it by selecting the **Forgot Token** button on the Security Authentication screen. Users will then be routed to the **Login - AIMS TFA Portal**.

If you have forgotten your password, you can reset it by selecting the **Forgot Password** button on the Security Authentication screen. Users will then be routed to the **Change Password** website.

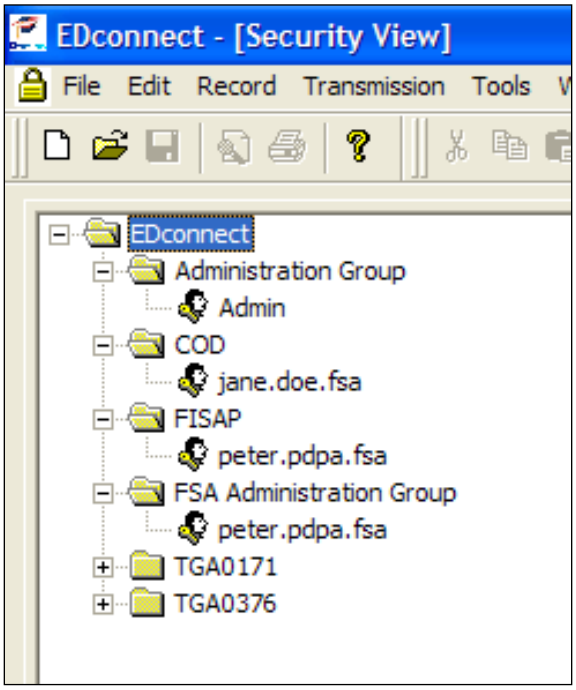
3.3 Security View

The **Security View** controls user access to EDconnect. This view enables you to set up **Security Groups** as well as to create individual users within those groups.

- You control **SAIG Passwords** at the *group* level.
- FSA controls and issues access to EDconnect.
- You control startup options, color preferences, and file directory locations at the *user* level.
- **FSA User IDs** can belong to different groups in the **Security View**.
- An illustration of an EDconnect Security View is shown below:



In the example below, “FSA Administration Group”, “FISAP” and “COD” represent **Security Groups**, while the individual names below the group names signify users within those groups.



There are three methods to move a user to another group.

Only a user belonging to the **FSA Administration Group** can move a user to another group by dragging and dropping the **FSA User ID**.

To drag and drop a FSA User ID

1. Select the **FSA User ID** by pressing your left mouse button to highlight it.
2. Move your cursor over the group into which you want to drop the **FSA User ID**.
3. Release the mouse button.

Any FSA Administrator or Group user has the functionality to copy one user from one group to another group.

To copy a FSA User ID

1. Click on the **FSA User ID** you want to copy.
2. Select **Copy** from the **Edit** menu.
3. Click on the group to which you want to copy the **FSA User ID**.
4. Select Paste from the Edit menu.

Any FSA user can delete another user and re-insert that user into another group, unless the deleted and re-inserted user is a member of the FSA Administration Group.

Delete and Re-Insert

1. Click on the **FSA User ID** you want to copy. The **FSA User ID** will appear highlighted.
2. Click with the right mouse button and select **Delete** from the pop-up menu and click yes to the “Delete User?” message.
3. Click with the right mouse button on the Group you want to add the **FSA User ID** to and select Insert from the pop-up menu
4. Use the User Wizard to recreate the deleted **FSA User ID**.

3.4 Security Groups

Within EDconnect, a **Security Group** represents a collection of users who connect to the SAIG using the same **TG number**, the same **Connection Type** ("Production" or "Test"), and the same **SAIG Password.**

An institution can have one or more **Security Groups** with varying levels of access to EDconnect functions.

Security Group *names* often correlate to the group's function, i.e. FISAP, COD, CPS, etc.

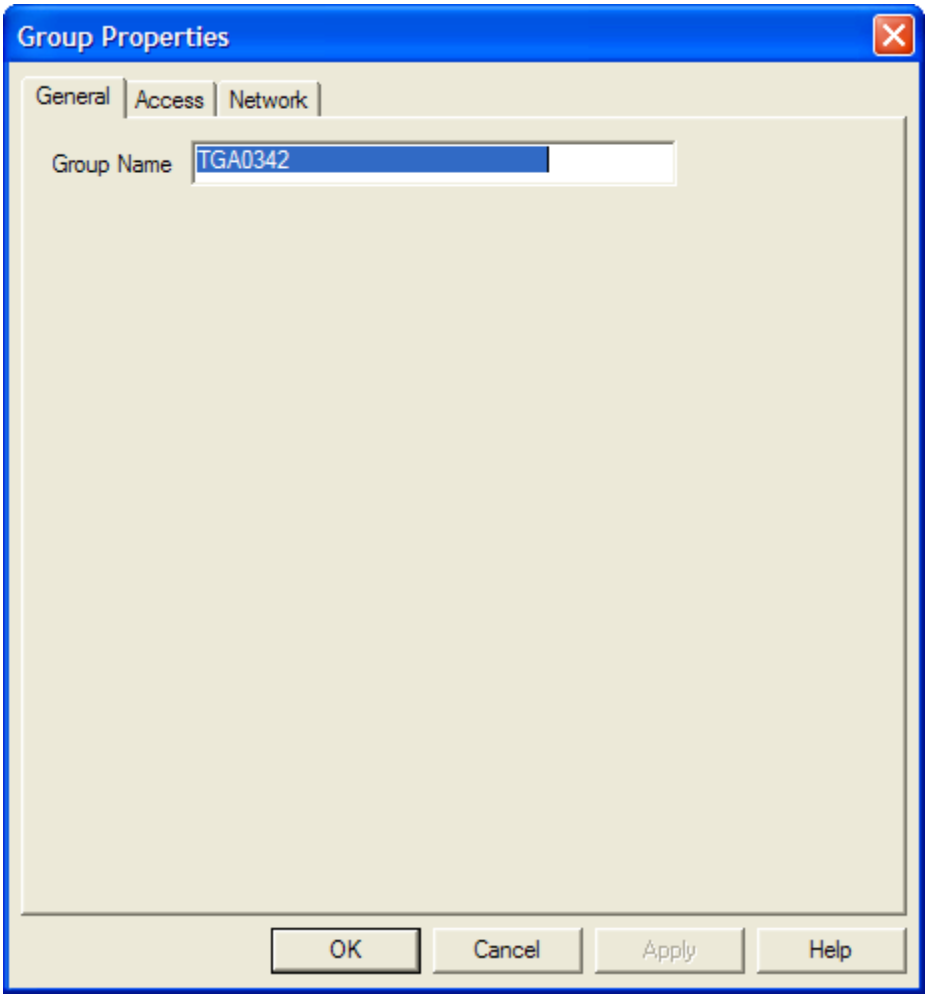
Connection type can be set either by the current user or will be prompted to the first non-Administration user to login. See section *3.6.1 Selecting a Connection* for more detail.

Only an **FSA Administration Group** user can create or delete groups, as well as modify group TG Numbers. The **FSA Administration Group** is a permanent group and cannot be deleted.

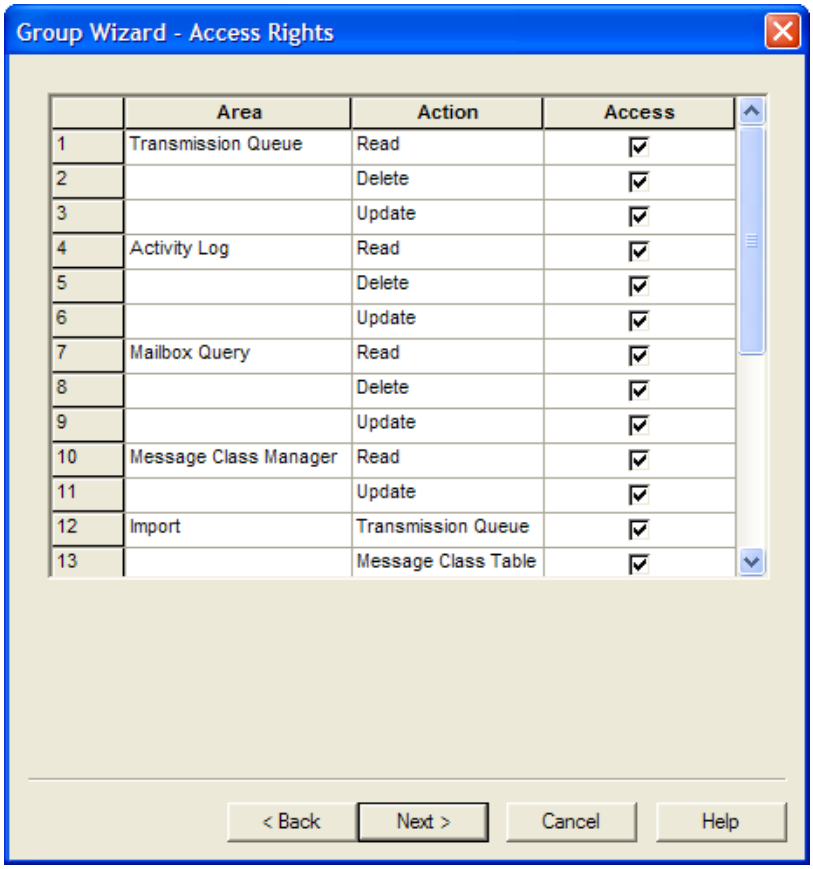
3.4.1 To add a "Production" Security Group

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the **EDconnect** folder.
3. Select **Insert** from the pop-up menu. The **Group Wizard** will appear on your screen.

4. Complete the **General Information** screen by providing a group name. Click **Next**.

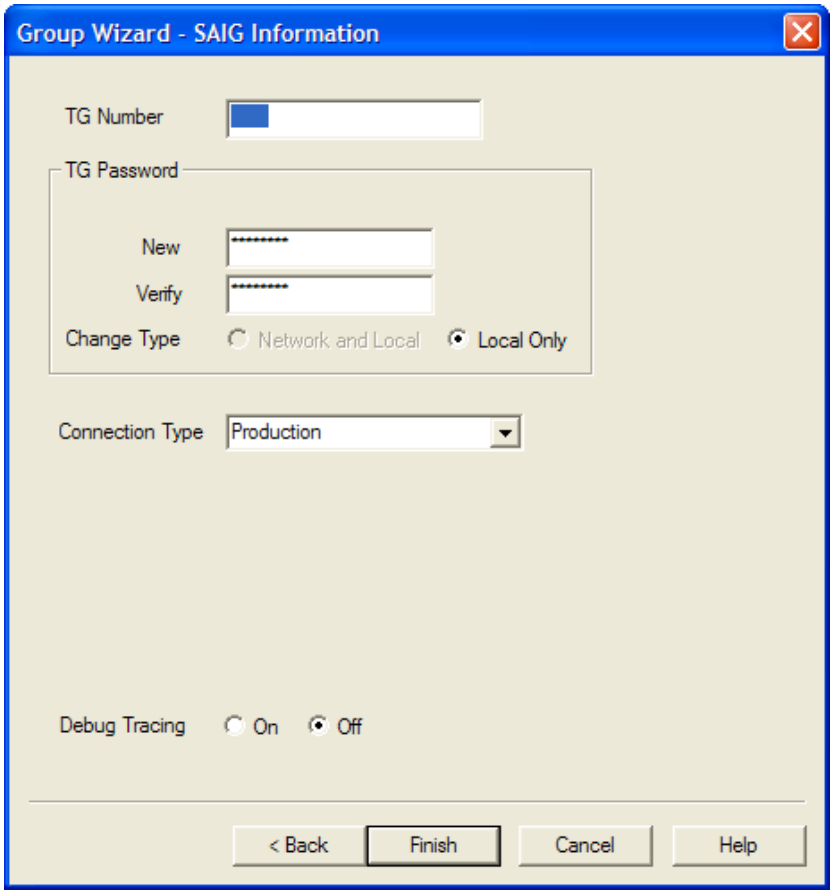


5. Set up access rights for all the users in the group by completing the **Access Rights** screen. Click **Next**.



	Area	Action	Access
1	Transmission Queue	Read	☑
2		Delete	☑
3		Update	☑
4	Activity Log	Read	☑
5		Delete	☑
6		Update	☑
7	Mailbox Query	Read	☑
8		Delete	☑
9		Update	☑
10	Message Class Manager	Read	☑
11		Update	☑
12	Import	Transmission Queue	☑
13		Message Class Table	☑

6. Set up **SAIG Password** information for the group by completing the **SAIG Information** screen. Leave the **Connection Type** set to the default value "Production."



7. Click **Finish**.

3.4.2 To add a "Test" Security Group

If you have been advised to set up a test Security Group to access the SAIG test system, follow the steps above but in step 6 select "Test" as the **Connection Type** on the **SAIG Information** tab.

Helpful Hints

- You can also access the **Group Wizard** by highlighting **EDconnect** in the **Security View** and selecting **Insert Record** from the **Record** menu.
- Multiple groups can have access to the same TG number, but they cannot have the same group name. For example, groups 'FISAP' and 'COD' can both have access to TGA0376 but you cannot have two groups named 'FISAP'.

3.4.3 To delete a Security Group

You must be logged in as a user of the **FSA Administration Group** to delete a Security group.

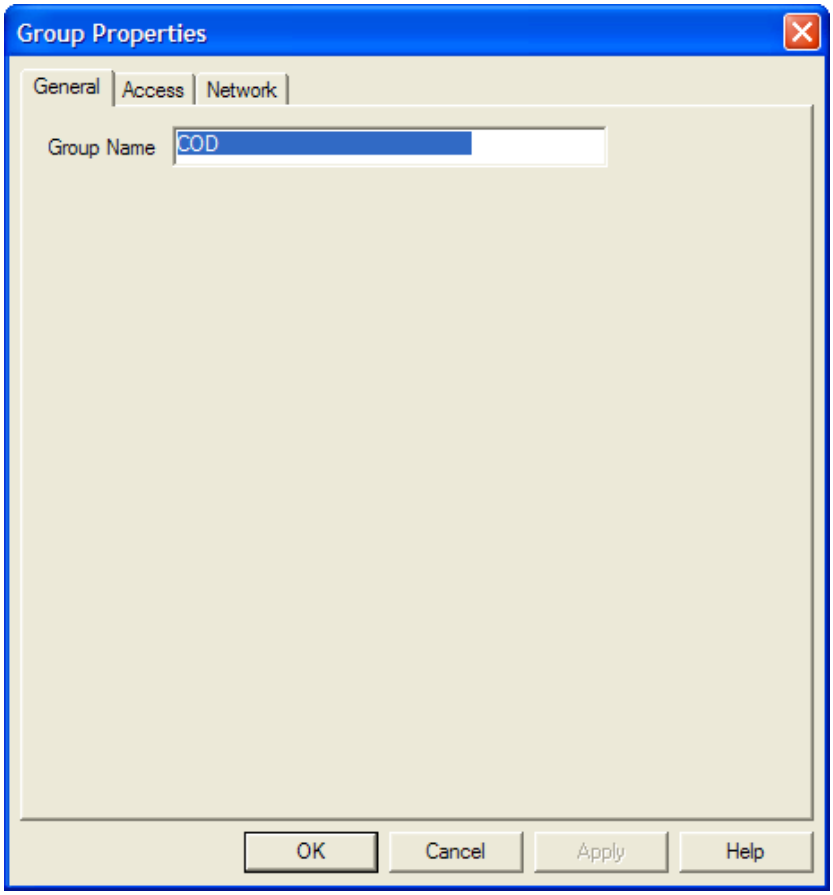
1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the **EDconnect** folder.
3. Select **Delete** from the pop-up menu.
4. Verify confirmation message, "Delete the group COD and all users within this group?" and select yes.

3.4.4 To Modify a Security Group

You must be logged in as a user of the **FSA Administration Group** to modify a Security group.

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the **EDconnect** folder.
3. Select **Properties** from the pop-up menu.

4. Verify the **Group Properties** dialog box open, displaying the **Group Properties** screen with the group name visible.



5. From this screen, you can select which tab you need to make your modifications. Click **Apply** and then **OK** when you are finished.

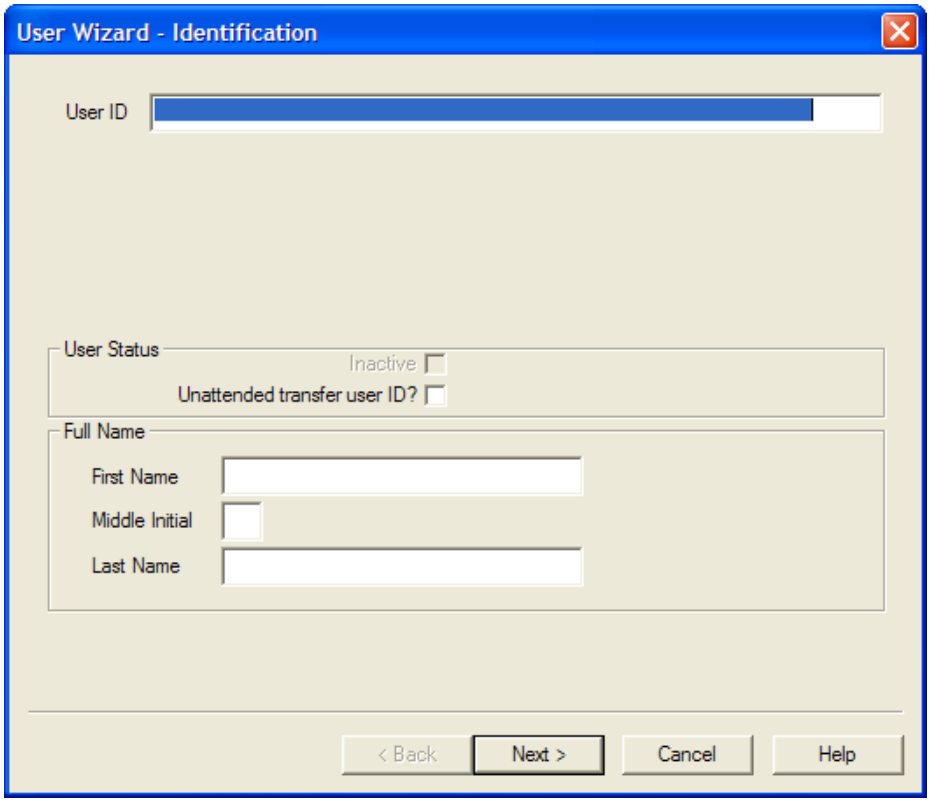
3.5 Users

Within EDconnect, users represent the individuals within **Security Groups** who access the SAIG through that group's **TG number**. You add users to **Security Groups** in the **Security View**. Users must be added using an FSA User ID. **FSA User IDs** and **FSA User Passwords** are issued by FSA.

By default, any **FSA User ID** can create and delete other users, except those in the **FSA Administration Group**.

3.5.1 To add an FSA User ID

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the **Security Group** to which you want to add a user.
3. Select **Insert** from the pop-up menu. The **User Wizard** will appear on your screen.



4. Complete the information on the **Identification** tab. Click **Next**. Remember that all user IDs must be **FSA User IDs** or they will not be allowed access to **EDconnect**. For more on the 'Unattended Transfer User ID' box, see *Helpful Hints* below.
5. Change the defaults, if desired, on the **General Information** tab. Click **Next**.

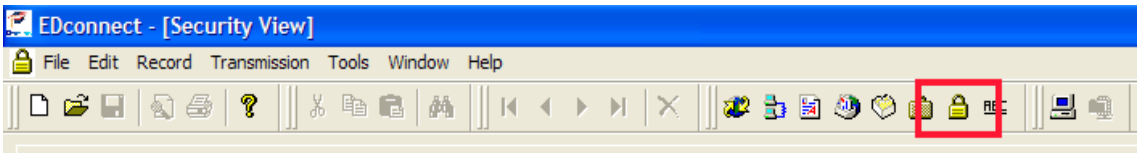
6. Change the default directory settings, if desired, on the **Directory Settings** tab. The drop-down menu (above the **Browse** button) enables you to set the path for the EDconnect database, the **Send** path, and the **Receive** path. Click **Next**.
7. Choose your color preferences. Click **Next**.
8. Choose your printing preferences.
9. Click **Finish**.

Helpful Hints

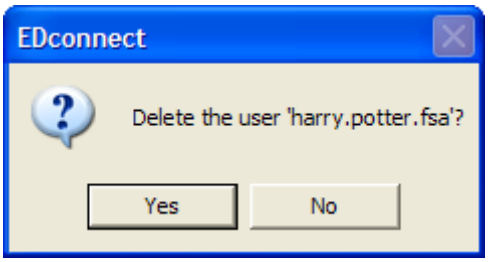
- The password you establish through the **Group Wizard** is associated with your **TG number** and enables your destination point to connect to the SAIG.
- All user IDs must be FSA User IDs, otherwise they will not be allowed access to EDconnect.
- The 'Unattended Transfer User ID' box is to be checked only when the **FSA User ID** will be sending .imp files. When this box is checked, the **FSA User ID** will not show up in the drop down of the **Security Authentication** dialog box. For more on .imp files, see section *5.1.1 Import (.imp) Files.*

3.5.2 To delete an FSA User ID

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on **EDconnect's** main toolbar, highlighted here in red.



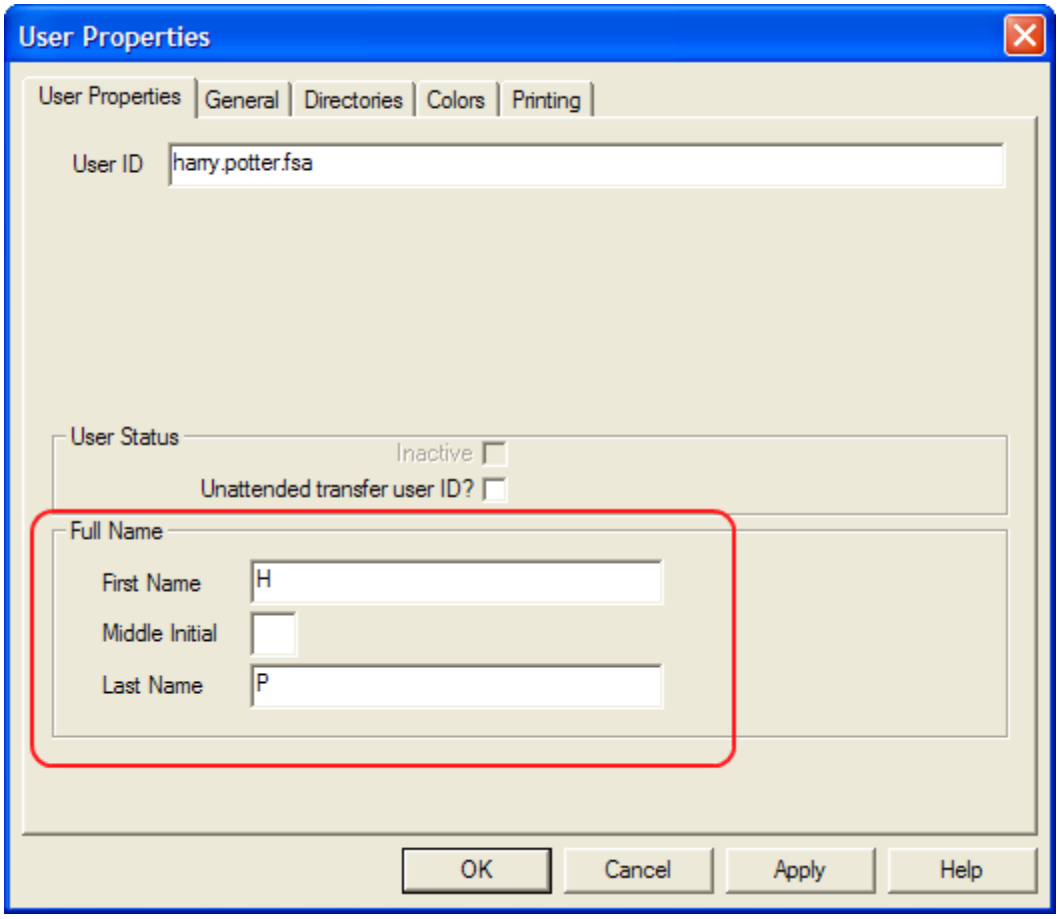
2. Right-click on the **Security Group** to which you want to delete a user.
3. Select **Delete** from the pop-up menu.
4. Verify confirmation message, "Delete the user harry.potter.fsa?"



5. Click **Yes**.

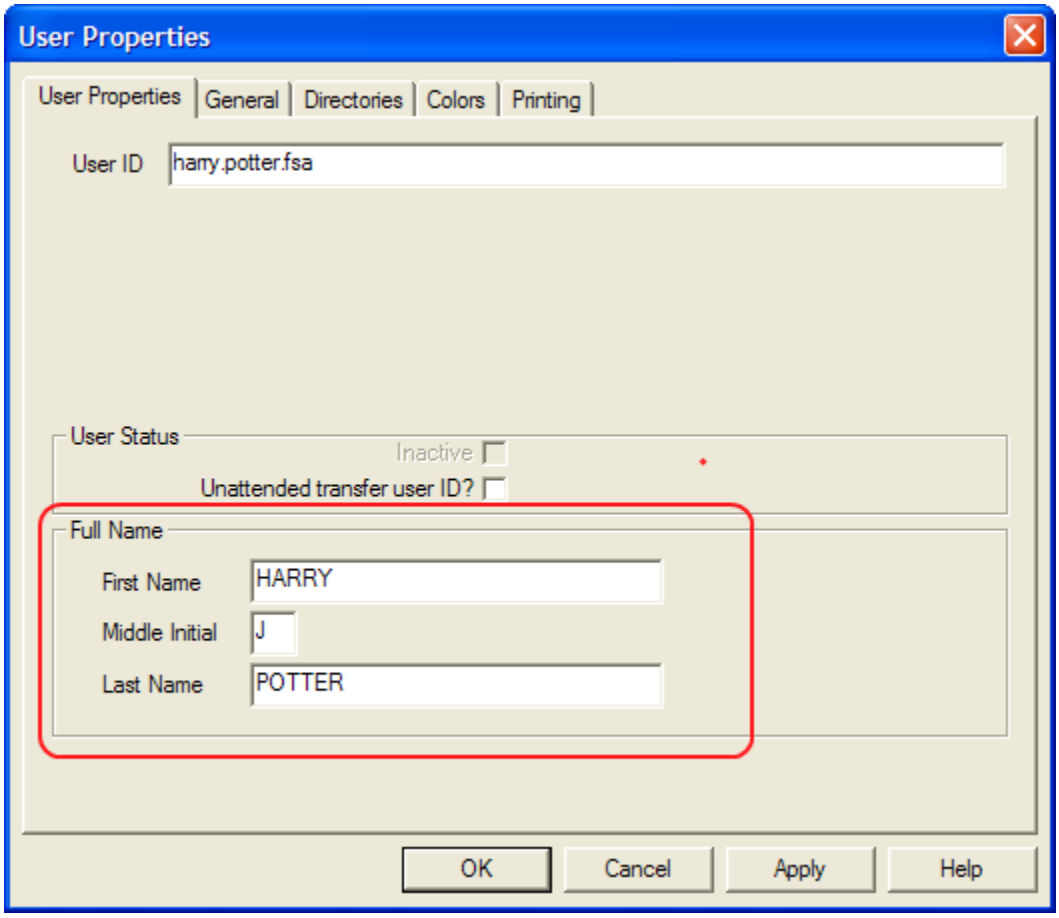
3.5.3 To Modify an FSA User ID

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on **EDconnect's** main toolbar.
2. Right-click on the **Security Group** to which you want to modify a user.
3. Select **Properties** from the pop-up menu.
4. Verify the **User Properties** dialog box appears.



5. Select the tab where you want to make the modification, (In this example, the Full Name field will modified.)

6. After your modification is made, click **Apply**, and **OK**.



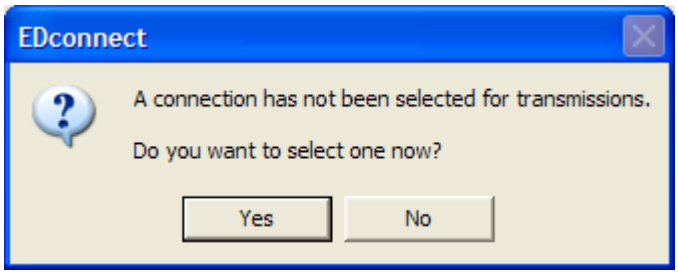
3.6 SAIG Connections

You must be connected to the Internet before starting EDconnect.

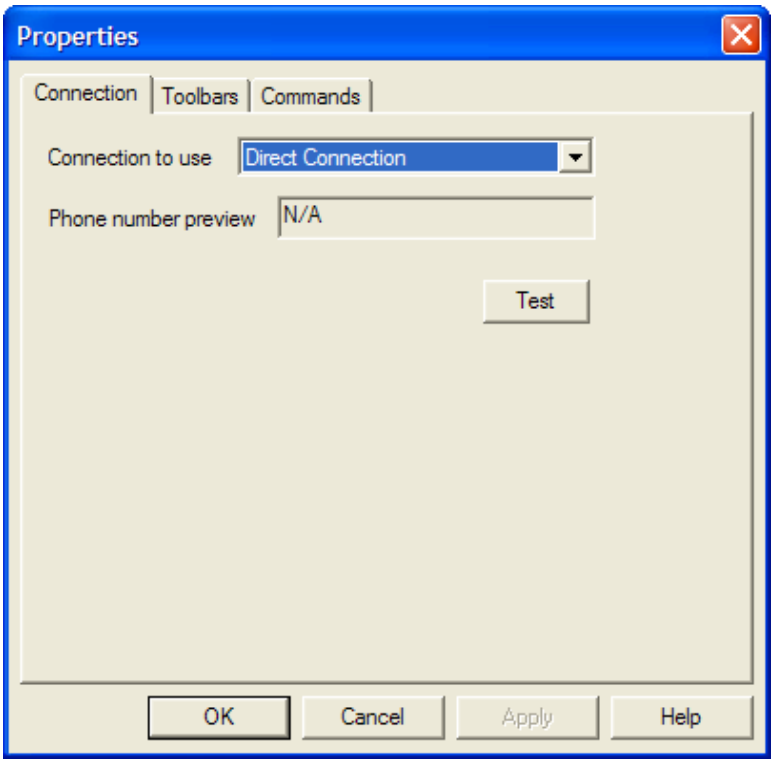
3.6.1 Selecting a Connection

There are two methods to select your connection.

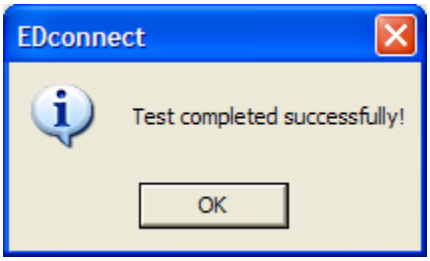
Method 1 - The first **FSA User ID** that is not part of the **FSA Administration Group** will be prompted to choose a connection upon initial login.



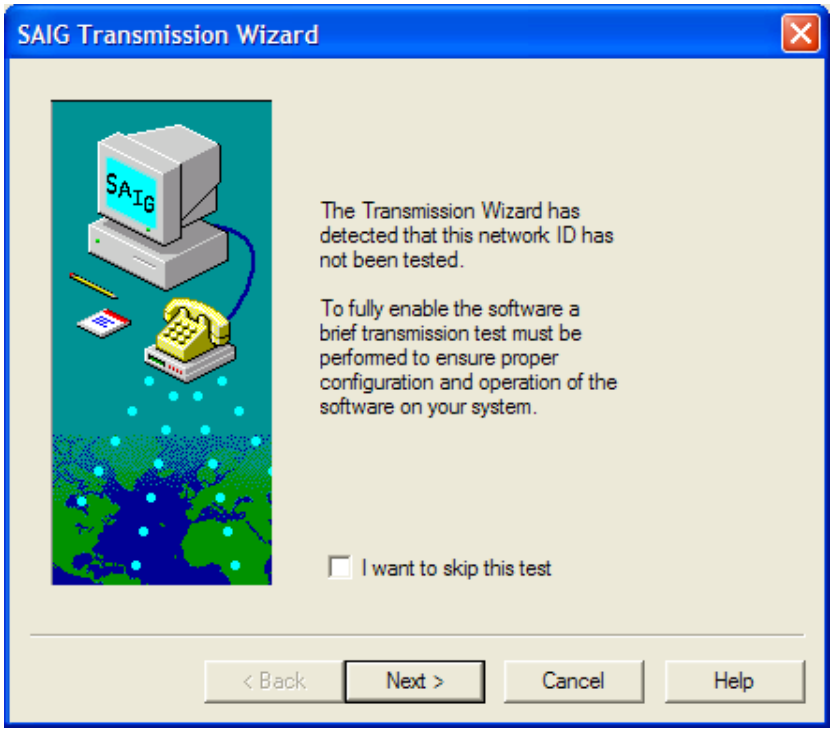
1. If you select **No**, you will still be allowed access to EDconnect but you cannot transmit until a connection has been set.
2. If you select **Yes**, you will be prompted to select one from the Connection Properties dialog box.



3. (Optional) Click **Test** to test the connection you have selected. You will receive a "Test completed successfully!" message.

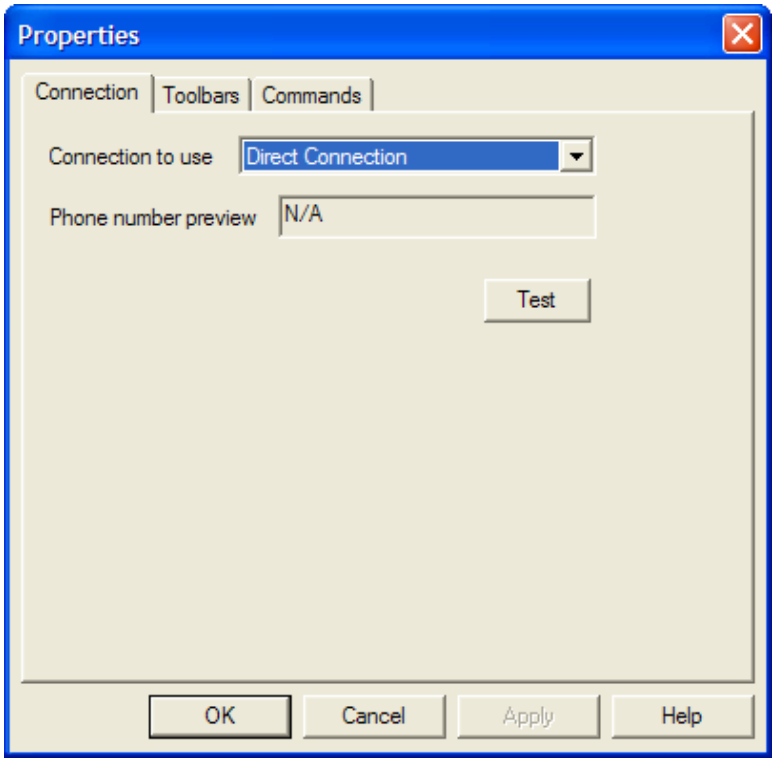


4. Click **OK**.
5. If this is your initial login or set-up, the **Transmission Wizard** will appear. You can run this test now, or choose to skip it by checking the **"I want to skip this test"** box. (Not recommended). You can also test your connection at any time by selecting '**TEST'** from the **Transmission** menu at the top of the screen.

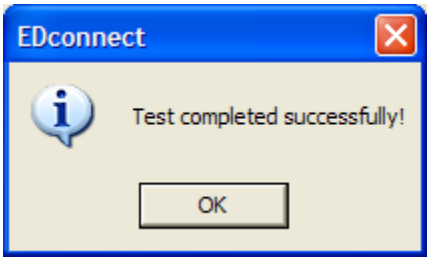


Method 2 - The second is a manual selection.

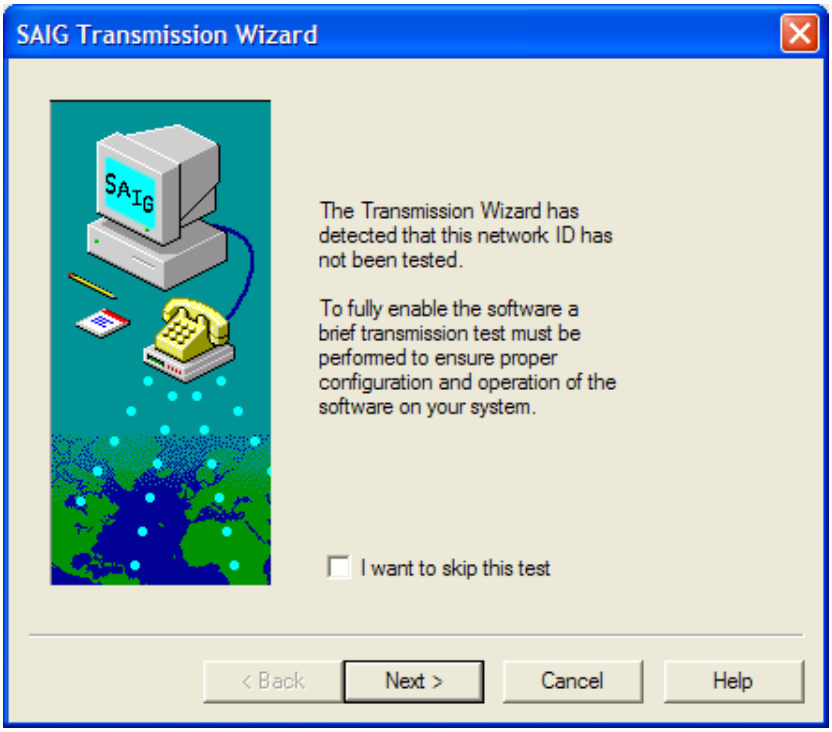
1. Select **Customize** from the **Tools** menu.
2. Select the **Connection** tab on the **Properties** dialog, if not already selected.
3. Select a connection from the drop-down list in the **Connection to use** selection box. See *Important Notes*, below, for information about selecting a connection.



4. (Optional) Click **Test** to test the connection you have selected. You will receive a "Test completed successfully!" message.



5. Click **OK**.
6. If this is your initial login or set-up, the **Transmission Wizard** will appear. You can run this test now, or choose to skip it by checking the **"I want to skip this test"** box. (Not recommended). You can also test your connection at any time by selecting '**TEST'** from the **Transmission** menu at the top of the screen.



Important Notes

- The drop-down list in the Connection to use selection box displays a list of Internet connections available on your computer.
- If you have a direct connection to the Internet, such as DSL, T1, or a cable modem, “Direct Connection” may be the only option listed.
- If you connect to the Internet using a modem and an ISP, in most cases your ISP’s dial-up connection will appear on the list.
- Some ISPs use proprietary dial-up connections that are created when you install their communications software.
- Although EDconnect *may* be able to dial your ISP and connect to the Internet through a proprietary dial-up connection, the connection may use protocols that will prevent EDconnect from sending and receiving data over the SAIG.
- Some ISP-provided communications programs do not create standard dial-up connections at all, so your Internet connection may not appear on the **Connection to use** drop-down list.
- **Note**: You can select “Direct Connection” even if you connect to the Internet using a modem and an ISP.
- Once you connect to the Internet through your ISP, the open Internet connection becomes a “Direct Connection” that will allow EDconnect to communicate with the SAIG.
- Selecting “Direct Connection” and connecting to the Internet *before* using EDconnect avoids potential problems associated with proprietary dial-up connections.

- If you select “Direct Connection,” you will need to connect to the Internet through your ISP the way you normally connect *before* sending and receiving data using EDconnect.
- If you select your ISP’s dial-up connection and are unable to send and receive data using EDconnect, select **Customize** from the **Tools** menu and choose “Direct Connection” from the **Connection to use** drop-down list. You will need to connect to the Internet through your ISP the way you normally connect *before* sending and receiving data using EDconnect if you select “Direct Connection.”

Warning

- Do *not* select any dial-up connections associated with older versions of EDconnect, such as “SAIG-0” or “T4WAN-0.”

3.6.2 Firewalls

A firewall is a barrier between your computer or your Local Area Network (LAN) and an external source, such as the Internet.

- The barrier can be software, hardware, or a combination of the two.
- A firewall examines each packet of information coming into and going out of your computer and prevents unauthorized packets from being sent or received.

A port is a pre-defined "channel," numbered from 0 to 65535, used by your computer to send and receive specific kinds of data. Your computer usually sends and receives e-mail through port number 23 and makes standard Internet connections through port number 80.

A firewall can prevent EDconnect from communicating with the SAIG by blocking the packets of information your computer is trying to send to and receive from the SAIG.

Determining If You Are Behind a Firewall

If you have trouble connecting to the SAIG after installing the new version of EDconnect, contact your technical support staff to see if you are behind a firewall. "Error -1" usually means that the port used by EDconnect to send and receive data is blocked.

Your technical support staff will need to open port number 26581 for inbound and outbound TCP/IP traffic and give your computer access to **saigmailbox.ed.gov** (for the test system use **saigmailboxdev.ed.gov**) to allow EDconnect to communicate through the firewall.

3.7 Wizards

EDconnect contains several wizards that assist you in your initial setup of the software. The following table describes each of the wizards:

Wizard Name	Function	Access
Group Wizard	Prompts you for all necessary information to set up a security group.	Select **Yes**, when prompted, to update a group. Choose to insert a group in the **Security View**.
User Wizard	Prompts you for all necessary information to set up a user.	Select **Yes**, when prompted, to update a user. Choose to insert a user in the **Security View**.
SAIG Connection Wizard	Prompts you to select a connection to use to send and receive data.	Select **Yes**, when prompted, to select a connection.
SAIG Transmission Wizard	Conducts a brief test to see if EDconnect is able to send and receive files.	If you have not completed the test, this wizard automatically appears on your screen after you log into EDconnect.

4 Passwords

4.1 Types of Passwords

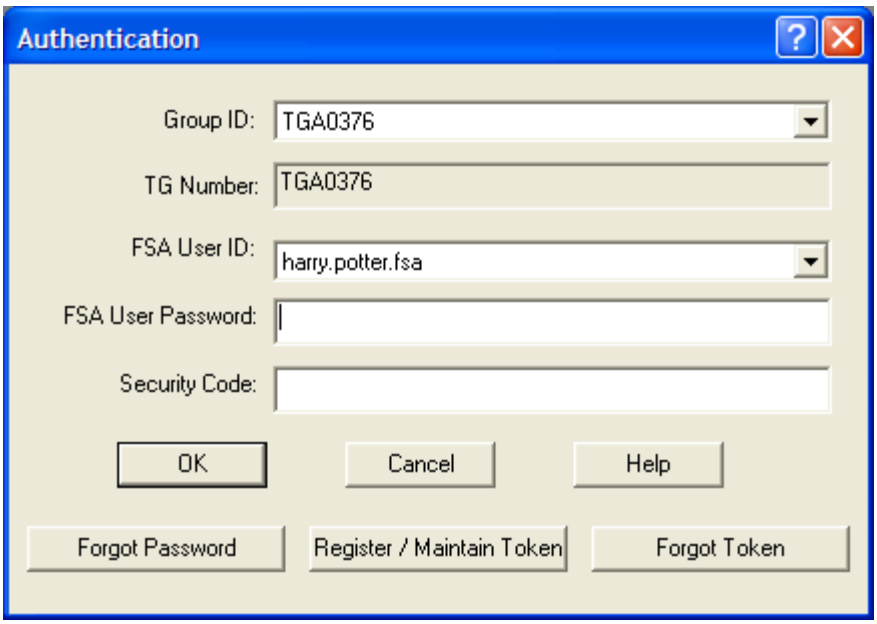
EDconnect requires two different types of passwords: **FSA User Passwords** and **SAIG Passwords**.

Each user must enter an **FSA User Password** to log into the software. EDconnect uses the **SAIG Password** (also known as your SAIG mailbox password) to connect to the SAIG.

After you have established your **SAIG Password**, you do not need to enter the **SAIG Password** in order to transmit. EDconnect stores the **SAIG Password** and sends it automatically each time you connect to the SAIG.

FSA User Password

- FSA User Passwords are issued by FSA.
- To change your password select the **Forgot Password** button on the Security Authentication screen. Users will then be routed to the **Change Password** website and guided through the process.



SAIG Password

The **SAIG Password** is independent of the EDconnect **FSA User ID Password**. The **SAIG Password** is controlled at the group level and is the password for your mailbox.

Users can set or change the **SAIG Password** on the Network tab of the **Group Properties** dialog box. See Section *4.3 SAIG Passwords* for detailed instructions on how to change your **SAIG Password**.

4.2 FSA User Password

Each user must enter a **FSA User Password** to log into the software. Each **FSA User ID** in the EDconnect **Security View** has its own personal password.

When you start EDconnect, the **Security Authentication** dialog box will appear. Enter or select your **Group ID**, **TG Number**, and **FSA User ID** from the drop-down list and enter the **FSA User Password** assigned by FSA and your **One-Time Password**, if applicable.

EDconnect has specific rules for **FSA User Passwords**:

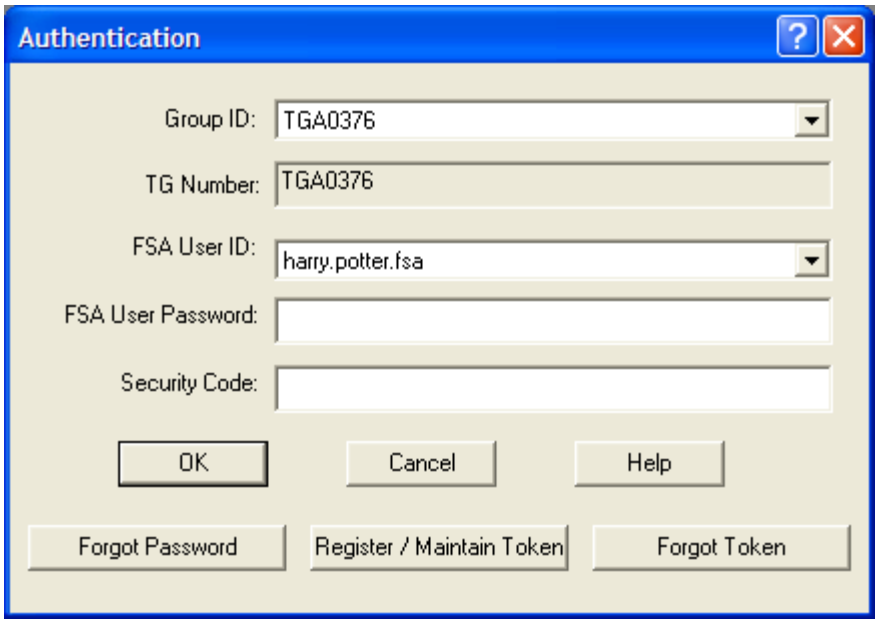
- Must be eight characters long
- Cannot be one of 5 previous passwords used
- Must contain 3 of the following:
  - An uppercase letter
  - A lowercase letter
  - A number (0-9)
  - A special character
    - User passwords can contain special keyboard characters, such as @, #, and $, but because some computer platforms use certain special characters as command characters, we recommend avoiding % (percent), ^ (caret), & (ampersand), \ (backslash), / (forward slash), < (less than), > (greater than), and | ("pipe" symbol).

Helpful Hints

- If you still are unable to log into EDconnect, please contact the SAIG Help Desk at 800-330-5947 or by e-mail at **CPSSAIG@ed.gov** for assistance.

4.2.1 Changing Your FSA User Password

FSA User Passwords are managed by FSA through the AIMs website. You can access this website by selecting the **Forgot Password** button on the Security Authentication screen where you will be guided through the process of changing your FSA User Password.



After you have successfully changed your password, return to the Security Authentication screen to login.

Helpful Hints

- All passwords in EDconnect are case-sensitive.
- Be sure to use the same capitalization each time you type your **FSA User Password**.

4.3 SAIG Password

EDconnect uses the **SAIG Password** (also called the **Group Password**, **TG Password**, or **Network Password**) to access your SAIG mailbox when you send or receive data.

The **SAIG Password** can be set or changed on the **Network** tab of the **Group Properties** dialog.

EDconnect has specific rules for SAIG passwords:

- Must be a minimum length of eight characters.
- Must begin with an alpha character
- Must contain at least two alpha characters of different cases (uppercase/lowercase) and at least one numeric character
- Cannot be the word “PASSWORD” (uppercase, lowercase, or mixed case)
- Cannot be the same as any of the previous five passwords
- Password will be locked out after three failures. (You must wait 30 minutes for your password to be unlocked. After 30 minutes, you can try again. If you have forgotten your password, you should use the Forgot Password button to retrieve it.)
- Can contain special characters
- SAIG passwords can contain special keyboard characters, such as @, #, and $, but because some computer platforms use certain special characters as command characters, we recommend avoiding % (percent), ^ (caret), & (ampersand), \ (backslash), / (forward slash), < (less than), > (greater than), and | ("pipe" symbol).

All passwords in EDconnect are case-sensitive. **SAIG Passwords** expire every 90 days.

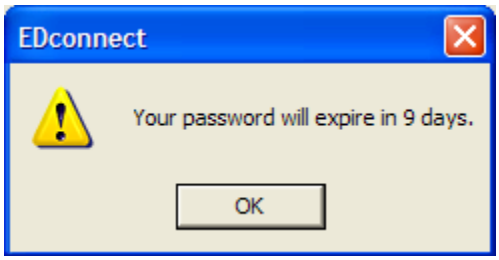
The **SAIG Password** is tied to a destination point’s **TG number** and **Connection Type** (“Production” or “Test”). While each user of EDconnect has his or her own **FSA User Password**, there is only one **SAIG Password** per **TG number** and **Connection Type**.

You can set up more than one **Security Group** with the same **TG number** and **Connection Type**. Since these groups connect to the SAIG with the same **TG number** and **Connection Type**, they must use the same **SAIG Password**. Once the groups are established, any future **SAIG Password** changes made to a security group will cause any other groups sharing the same **TG number** and **Connection Type** to change their passwords manually.

Helpful Hints

- Each TG number/Connection Type combination has its own **SAIG Password**.
- Each user of EDconnect has her or his own **FSA User Password**.
- Users do not need to know the **SAIG Password** to log into EDconnect or to transmit.

- As the expiration date for your **SAIG Password** approaches, you will receive a warning that the password is about to expire when you transmit with EDconnect.



4.3.1 Changing Your SAIG Password

You have two options for changing your **SAIG Password**: **Local Only** and **Network and Local**.

Your **SAIG Password** is associated with your **TG number** and **Connection Type** and is stored within EDconnect and on the SAIG. Your SAIG mailbox compares the password transmitted by EDconnect with the password stored on the SAIG to confirm your group identity during each transmission.

- A **Local Only** password change sets the password within EDconnect but does not transmit the password change to your SAIG mailbox.
- A **Network and Local** password change sets the password within EDconnect *and* transmits the change to your SAIG mailbox.

If you have had your **SAIG Password** reset by the SAIG Help Desk, you must:

1. Perform a **Local Only** password change, changing your **SAIG Password** to the password assigned to you (uppercase and without the quotation marks).
2. Perform a **Network and Local** password change to establish a new password on the SAIG.

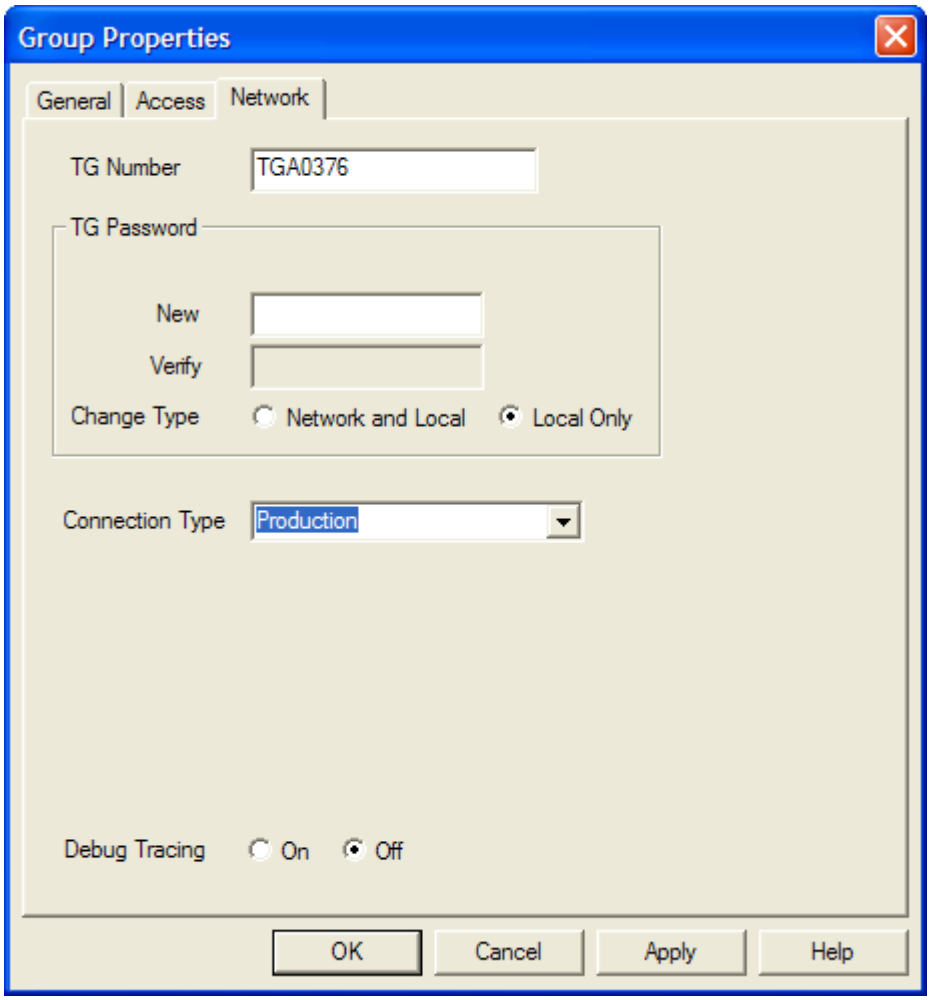
If you reinstall EDconnect but have already established a **SAIG Password**, a **Local Only** password change will synchronize the password within EDconnect to match the password stored by your SAIG mailbox.

Helpful Hints

- All passwords in EDconnect are case-sensitive.
- Be sure to use the same capitalization each time you type your **SAIG Password**.

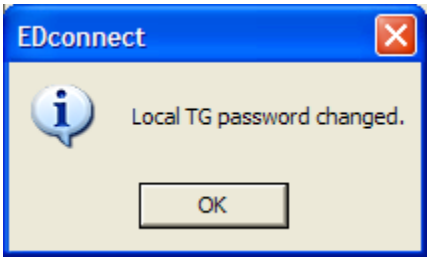
4.3.2 Performing a "Local Only" SAIG Password Change

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the desired group within the **Security View**.
3. Select **Properties** from the pop-up menu.
4. Select the **Network** tab from the **Group Properties** dialog.



5. Type your current **SAIG Password** in the **New** text box.
   Note: If you are accessing a new SAIG mailbox for the first time, the default password is an eight-digit number comprised of the year of the DPA's birth and the last four digits of his or her Social Security Number. If you have had your password reset by the SAIG Help Desk, the new password is "PASSWORD" (uppercase and without the quotation marks) or some other assigned password.
6. Type your password again in the **Verify** text box.

7. Select the **Local Only** option under **Change Type**, if not already selected.
8. Click **OK**. The message “Local TG password changed” appears.



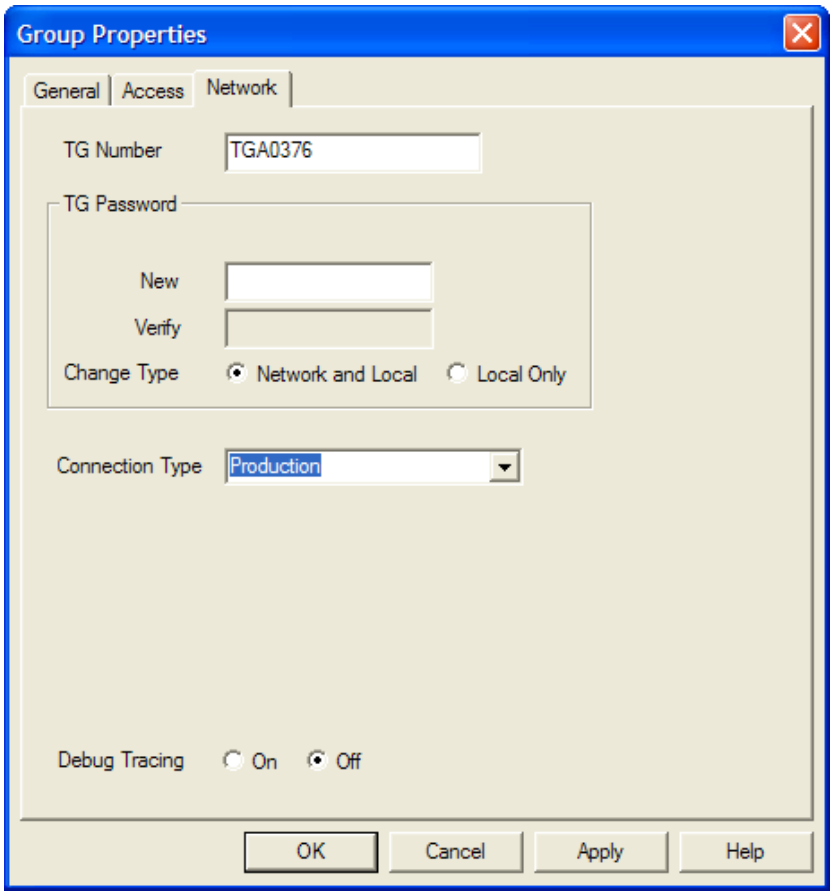
9. Click **OK** to return to the **Security View**.

Helpful Hints

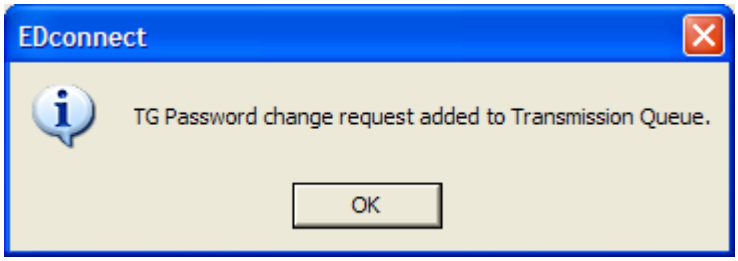
- A **Local Only** password change sets the **SAIG Password** within EDconnect without sending the password change to the SAIG.
- A **Local Only** password change is necessary after your password has been reset by the SAIG Help Desk, when you move EDconnect to a different PC, or when you install EDconnect on several PCs that share one **TG number** and **Connection Type** but have separate EDconnect databases.
- Your Local TG password must match the SAIG password in order to transmit successfully.

4.3.3 Performing a "Network and Local" SAIG Password

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on the desired group within the **Security View**.
3. Select **Properties** from the pop-up menu.
4. Select the **Network** tab from the **Group Properties** dialog.



5. Type your new **SAIG Password** in the **New** text box.
6. Type the password again in the **Verify** text box using the same capitalization.
7. Select **Network and Local** as the **Change Type**, if not already selected.
8. Click **OK**. The message "TG Password change request added to Transmission Queue" appears.



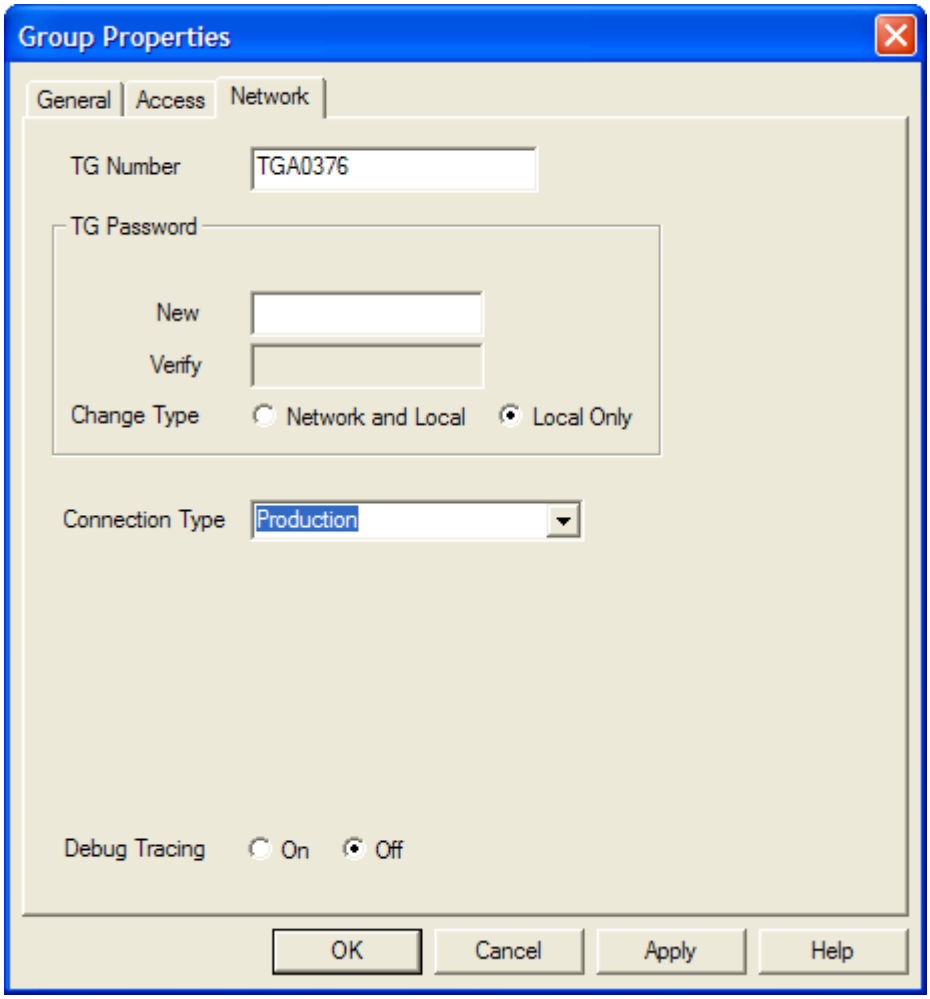
9. Click **OK** to return to the **Security View**.
10. Select **Now** from the **Transmission** menu or select the 'Transmit' icon to send your new password to the SAIG.

Helpful Hints

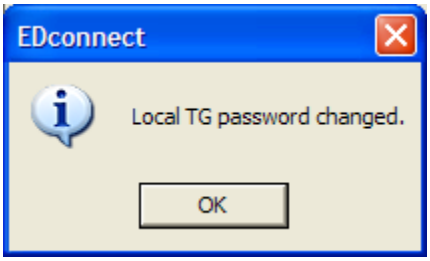
- Selecting a **Network and Local** change on the **Network** tab of the **Group Properties** dialog will create a password change request in the **Transmission Queue**. EDconnect will transmit the request the next time you send or receive data.
- You need to perform a **Network and Local** password change every 90 days or your **SAIG Password** will expire.

4.3.4 Changing your SAIG Password After Help Desk Resets It

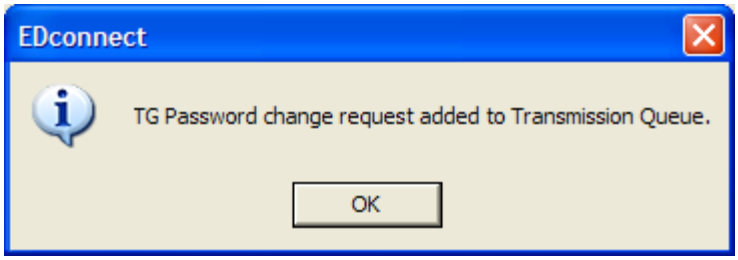
1. Right-click on the desired group in the **Security View**.
2. Select **Properties** from the pop-up menu.
3. Select the **Network** tab from the **Group Properties** dialog.
4. Type your assigned password in the **New** text box.
5. Type your assigned password again in the **Verify** text box.



6. Select **Local Only** as the **Change Type**, if not already selected.
7. Click **Apply**. The message “Local TG password changed” appears.



8. Click **OK** to respond to the message. The **Group Properties** dialog will stay on your screen.
9. Type your new password in the **New** text box.
10. Type the password again in the **Verify** text box using the same capitalization.
11. Select the **Network and Local** option, if not already selected.
12. Click **OK**. The message "TG Password change request added to Transmission Queue" appears.



13. Click **OK** to return to the **Security View**.
14. Select **Now** from the **Transmission** menu or the 'Transmit' icon to send your new password to the SAIG.

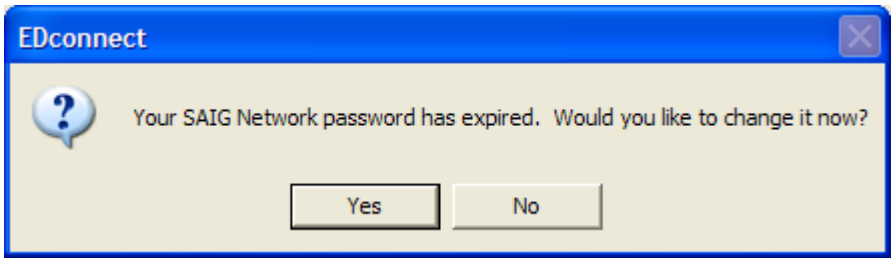
4.3.5 Changing Your SAIG Password After It Has Expired

Your **SAIG Password** expires every 90 days. You are warned that your **SAIG Password** is due to expire nine days before the expiration date. The expiration date and warning period are set by the SAIG network and cannot be modified.

To access the Group Properties dialog

1. Go to the **Security View**.
2. Right-click on the desired group name.
3. Select **Properties** from the pop-up menu.
4. Select the **Network** tab to check the expiration date.

If you attempt to connect to the SAIG after your password has expired, a message box appears, indicating that your password has expired.



You do *not* need to have the SAIG Help Desk reset your password if you receive this message. The SAIG will allow you to send and receive data as long as you transmit a password change.

To change your **SAIG Password**, click **Yes** to the message box and follow the steps on the previous page. After you enter your new **SAIG Password**, try another transmission. EDconnect will send your password change, along with any other items in the **Transmission Queue**.

Helpful Hints

- If you have had your password reset by the SAIG Help Desk, the password of your SAIG mailbox will be temporarily set to “PASSWORD” or some other assigned password to enable you to transmit a password change.
- You must perform a **Local Only** password change, changing your password to “PASSWORD” or to the assigned password.
- You must then perform a **Network and Local** password change to set your **SAIG Password** to a password of your own choice.

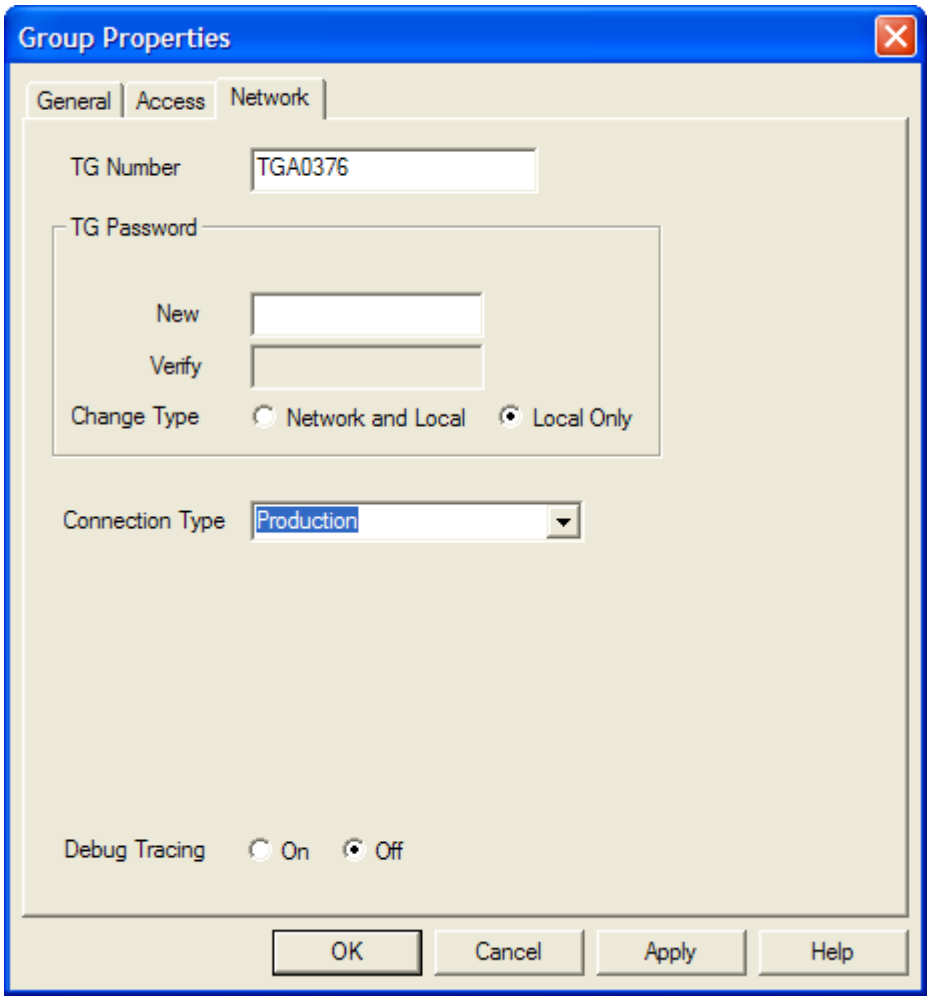
Important Note

For enhanced security, after three failed transmissions due to an expired or invalid **SAIG Password**, your account will be locked and you must call the SAIG Help Desk at 800-330-5947 to have it unlocked.

The SAIG Help Desk must talk directly to the Destination Point Administrator (DPA) or Secondary Destination Point Administrator (SDPA) to verify personal identifiers before resetting your **SAIG Password** or unlocking your account. The DPA or SDPA should be prepared to supply his or her Social Security Number (SSN) and date of birth (DOB).

SAIG Password Change Screen Example

Illustration of the password change screen for the **SAIG Password**:



5 Data Transmission

5.1 Sending and Receiving Data

5.1.1 Sending Data

You send data to the SAIG for processing by creating files containing data, then adding the files to the Transmission Queue as Send requests.

When EDconnect connects to your SAIG mailbox, it sends the files from your PC to the SAIG.

The appropriate Title IV Application System picks up your files, processes them, and returns the processed data to your mailbox.

5.1.2 Receiving Data

You *receive* data by adding requests to the **Transmission Queue**.

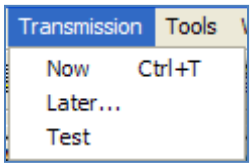
When EDconnect connects to your SAIG mailbox, it retrieves the processed files placed in your SAIG mailbox by a Title IV Application System and returns them to your PC.

Helpful Hint

- You can send and receive data as well as perform password changes during the same connection to the SAIG. You must have a Message Class table imported before you can make a transmission.

5.1.3 Data Transmission Menu

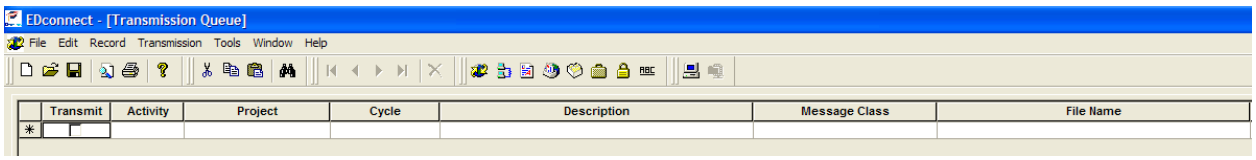
The **Transmission** menu on the main menu bar gives you three choices: **Now**, **Later**, and **Test**.



- Selecting the **Now** option starts a connection to the SAIG immediately. All data queued for sending to the SAIG and properly marked in the **Transmission Queue** are sent. All data queued for receiving from your mailbox and properly marked in the **Transmission Queue** are received, provided there are data files in your mailbox.
- Selecting the **Later** option opens the **Transmission** dialog box that enables you to select a time and date for EDconnect to connect to the SAIG.
- Selecting the **Test** option transmits a test file to the SAIG, then sends a request for the same file. EDconnect creates the test file, so you do not need to add it to the **Transmission Queue** before you perform the transmission test. The **Test** option will also send a **SAIG Password** change if you have one in your EDconnect **Transmission Queue**.
- Helpful Hint
- If you set up a later transmission, EDconnect must remain open until the time you select for the later transmission arrives. A message box tracks the time remaining until EDconnect transmits your data.

5.1.4 Transmission Queue (TQ)

The **Transmission Queue** (**TQ**) is a list of pending requests to send or receive data and/or to make a password change. Below is a partial image of the Transmission Queue.



Requests remain in the **TQ** until EDconnect processes them during a transmission or until you remove them from the **TQ**.

- You can open the **TQ** by selecting **New** from the **File** menu and choosing **Transmission Queue** from the list of views.
- You can also click the **Transmission Queue** button on EDconnect's main toolbar.

To add records manually to the TQ

1. Move the cursor to the first blank line in the **TQ**.
2. Complete each field either by typing your selection or by clicking the **down** arrow to display a menu of choices.
3. Complete the rest of the fields for the same row. EDconnect does not let you move to a new row until you have completed all the necessary fields for the current row.
4. You will know that a line is complete when the pencil symbol on the far left of the row disappears. The record is then ready for transmission.

Below is an example of the pop-up dialog that appears when you select the **down** arrow in the **File Name** field.

- This step is usually the final step in preparing a record in the **TQ**.
- The **Data File** dialog that appears enables you to select the specific file that you want to send.

Description	Message Class	File Name
04-05 COMMON RECORD DOCUMENTS	CRAA05IN	c:\iam\data\craa05in.*

Helpful Hints

- If you know the message class of a file you want to receive, typing the message class will fill in all necessary fields automatically.
- If you want to receive all data and messages, go to the **Description** column and select "All Data, All Messages" from the list. This action will fill in all necessary fields automatically.

5.1.5 TQ Templates

5.1.5.1 Creating TQ Templates

The **Transmission Queue** (**TQ**) is a list of pending requests to send or receive data or to make password changes.

Records remain in the **TQ** until EDconnect processes them during a transmission, or until you remove them from the **TQ**.

You can save a current view of the **TQ** and make that into a template file (**TQT**) that can be loaded back into the **TQ** later.

To create a template, follow these instructions

1. Create a group of records in the **TQ** that you plan to use repeatedly in the future.
2. Select **Save As…** from the **File** menu.
3. Choose a location to save the file and give it a name you will remember. As part of the file name, be sure to include the extension ".tqt" when naming the template file.
4. Click **OK**.

   Helpful Hints
   - Templates are "snapshots" of a current view saved to a file.
   - Templates can be especially useful for common tasks.
   - Instead of manually creating the same records each time, you can load a template with the records already created.

5.1.5.2 Opening TQ Templates

You can retrieve saved "snapshots" of a **Transmission Queue** (**TQ**) view by opening **Transmission Queue Template** (**TQT**) files using one of the following **methods**:

1. Select **Open** from the **File** menu within EDconnect and select the name of the **TQT** file.
2. Use your mouse to drag the **TQT** file from **Windows Explorer** to an open **TQ**.
3. Select a template from the **All Programs| EDconnect8** menu. There are pre-created templates in the EDconnect8 folder on the **Programs** menu. Selecting a template will open EDconnect8.

   Helpful Hints
   - EDconnect automatically places several common **TQT** files in the EDconnect directory during installation.
   - You cannot import **TQT** files associated with earlier versions of EDconnect into EDconnect 8.3.

5.1.6 Activity Log

The **Activity Log** stores a record of all transmissions made using EDconnect.

It lists files that have been sent and received, **SAIG Password** changes that have been transmitted, and any transmission errors that occurred while sending or receiving files.

You can open the **Activity Log** by selecting **New** from the **File** menu and selecting **Activity Log** from the list of views.

Activity	Project	Cycle	Description	Message Class	File Name
Transmit			Start of Transmission		
Send	CPS	02-03 Data	02-03 FDR	FDRS03IN	c:\iam\data\atest.txt
Send	CPS	04-05 Data	04-05 PIN DATA REQUESTS	RADD05IN	c:\iam\data\atest.txt

5.1.6.1 Archiving Activity Log Records

1. Open the **Activity Log**.
2. Select the records you want to archive.
3. Select **Save As…** from the **File** menu.
4. Name the file, preserving the ".arc" extension.
5. Select the drive and directory where you want to save the file.
6. Click **Save**.

Helpful Hints

- You can select records easily using the **Activity Log Filter**.
- Archiving records from the **Activity Log** does not automatically delete those records.
- To delete records, return to the open **Activity Log** and highlight the records you archived. If you filtered the records, highlight all the records in that view. Press **Delete**.
- You can import records archived with EDconnect 7.X into EDconnect8.0, but not records archived with earlier versions of EDconnect.

5.1.6.2 Retention Period

The **Retention Period** dialog box enables you to set the length of time that EDconnect retains records in the **Activity Log** before automatically deleting them.

To set the retention period

1. Choose **Properties** from the **Edit** menu while the **Activity Log** is active on your screen.
2. Select the **Received File** tab on the **Properties** dialog.
3. Click **Enable Automatic Delete** to activate the delete function.
4. Drag the vertical bar in the middle of the **Retention** field to set the number of days (the default is zero days).
5. Click **OK**.

Helpful Hints

- You can use your left and right **Arrow** keys to fine tune your selection.
- Pressing the **left Arrow** key **lowers** the **Retention Period** by one day and pressing the **right Arrow** key **increases** it by one day.

5.1.7 Mailbox Query

View Records in my Mailbox

You can use the **Mailbox Query** to get a "snapshot" of the current contents of your SAIG mailbox. After performing a **Mailbox Query**, you can place requests for specific files in your **Transmission Queue**.

	Move to TQ	Message Class	Batch Number	Item Number	Description	Sender ID
	☐	MESSAGTB	12062011171724	20120112A00008494692	MESSAGE TABLE DISTRIBUTION	BATCHMB
	☐	CORE12OP	01234567890012345678 90	20120112A00008494697	11-12 Errors - Corrections	TG50002
	☐	CORE13OP	01234567890012345678 90	20120112A00008494698	12-13 Errors - Corrections	TG50002
	☐	DELQFFOP	01234567890012345678 90	20120112A00008494707	NSLDS DELINQ BORROWER REPORT FIXED LENGTH	TG53161
	☐	DELQCMOP	01234567890012345678 90	20120112A00008494708	NSLDS DELINQ BORROWER REPORT COMMA DELIMITED	TG53161

5.1.7.1 To use the Mailbox Query

1. With no records selected for transmission or receipt in your **Transmission Queue**, select **Now** from the **Transmission** menu to connect to the SAIG.
2. After the transmission completes, open the **Mailbox Query** by selecting **New** from the **File** menu and selecting **Mailbox Query** from the list of views. You can also click the **Mailbox Query** button on EDconnect's main toolbar.
3. Select the items you want to receive in the next transmission by putting a checkmark in the **Move to TQ** column.
4. Close the **Mailbox Query** by selecting **Close** from the **File** menu. This places a request in the **Transmission Queue** for each file that you selected.

Helpful Hints

- At the end of each transmission, EDconnect updates the **Mailbox Query** to reflect what is currently in your SAIG mailbox.
- If you receive all the data in your mailbox, the **Mailbox Query** will be empty because your mailbox is empty.
- To get a "snapshot" of the current contents of your SAIG mailbox, follow the steps above to perform a new **Mailbox Query**.

5.1.8 Received File View

The **Received File View** lists the files that you have recently downloaded.

This view displays files that you have downloaded from your SAIG mailbox over the previous ten days.

Move to TQ	Message Class	Batch Number	Item Number	Description	Sender ID
☐	AHSLDEOP	0123456789001234567890	20120112A00008494728	AD HOC EXTRACTS	TG50012
☐	AHSLDSOP	0123456789001234567890	20120112A00008494729	AD HOC QUERY AND PRODUCT DEL	TG50012
☐	AHSLDEOP	0123456789001234567890	20120119A00008495544	AD HOC EXTRACTS	TG50012
☐	AHSLDSOP	0123456789001234567890	20120119A00008495545	AD HOC QUERY AND PRODUCT DEL	TG50012

You can download files listed in the **Received File View** without having the files restored by the SAIG Help Desk.

5.1.8.1 To re-download files

1. Open the **Received File View** by selecting **New** from the **File** menu and selecting **Received File View** from the list of views.
2. Place a checkmark in the **Move to TQ** checkbox to the left of the batch you want to restore.
3. Close or save the **Received File View**. Once the **Received File View** is closed or saved, each record that you selected is added to the **Transmission Queue**.
4. Select **Now** from the **Transmission** menu to receive the selected files again.

Helpful Hints

- If a file has been restored to your mailbox by the SAIG Help Desk, the **Restored Date** field will be populated with the date the file was put back in the Archive.
- The date listed in the **Add Date** column of the **Received File View** represents the date a given item was placed in your SAIG mailbox by the Application System that processed that item.
- To restore files older than ten days to your SAIG mailbox, use the **Transaction Delivery CommunityManager** (**TDCM**) **Archive View** or contact the SAIG Help Desk at 800-330-5947. The **TDCM** is available online at **saigportal.ed.gov**.

The SAIG Help Desk can restore any file to your mailbox if it is not older than 180 days. Files older than 180 days are archived and cannot be restored.

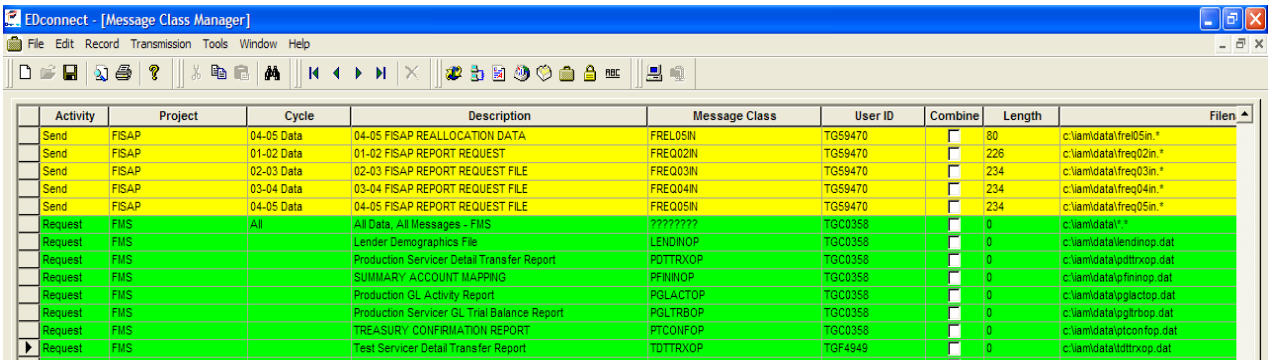
5.1.9 Message Class Manager View

The Message Class Manager controls the allowable message classes that can be sent and received.

The Message Class Table must be imported to send or receive messages and is updated periodically by FSA. The Message Class table is available on the FSA Download site (www.fsadownload.ed.gov).

Note! EDconnect will automatically import this table once you have established a connection with FSA.

Sample illustration of Message Class Manager



Activity	Project	Cycle	Description	Message Class	User ID	Combine	Length	Filen
Send	FISAP	04-05 Data	04-05 FISAP REALLOCATION DATA	FREL05IN	TG59470	☐	80	c:\iam\data\frel05in.*
Send	FISAP	01-02 Data	01-02 FISAP REPORT REQUEST	FREQ02IN	TG59470	☐	226	c:\iam\data\freq02in.*
Send	FISAP	02-03 Data	02-03 FISAP REPORT REQUEST FILE	FREQ03IN	TG59470	☐	234	c:\iam\data\freq03in.*
Send	FISAP	03-04 Data	03-04 FISAP REPORT REQUEST FILE	FREQ04IN	TG59470	☐	234	c:\iam\data\freq04in.*
Send	FISAP	04-05 Data	04-05 FISAP REPORT REQUEST FILE	FREQ05IN	TG59470	☐	234	c:\iam\data\freq05in.*
Request	FMS	All	All Data, All Messages - FMS	????????	TGC0358	☐	0	c:\iam\data*.*
Request	FMS		Lender Demographics File	LENDINOP	TGC0358	☐	0	c:\iam\data\lendinop.dat
Request	FMS		Production Servicer Detail Transfer Report	PDTTRXOP	TGC0358	☐	0	c:\iam\data\pdttrxop.dat
Request	FMS		SUMMARY ACCOUNT MAPPING	PFININOP	TGC0358	☐	0	c:\iam\data\pfininop.dat
Request	FMS		Production GL Activity Report	PGLACTOP	TGC0358	☐	0	c:\iam\data\pglactop.dat
Request	FMS		Production Servicer GL Trial Balance Report	PGLTRBOP	TGC0358	☐	0	c:\iam\data\pgltrbop.dat
Request	FMS		TREASURY CONFIRMATION REPORT	PTCONFOP	TGC0358	☐	0	c:\iam\data\ptconfop.dat
Request	FMS		Test Servicer Detail Transfer Report	TDTTRXOP	TGF4949	☐	0	c:\iam\data\tdttrxop.dat

5.1.10 Views

The table below lists all the views within EDconnect that play a role in data transmission.

The middle column displays the toolbar button for each view (clicking a view's toolbar button opens that view).

View	Toolbar Icon	Description
Transmission Queue (TQ)		Lists pending **Send** and **Receive** requests, which remain in the **TQ** until processed or until you remove them.
Activity Log		Lists processed requests to send and receive data from the SAIG.
Message Class Manager		Lists all the message classes, by project, that are available to send and receive.
Mailbox Query		Lists the data, by message class, available in your SAIG mailbox.
Received File		Lists data records, by message classes that have already been received from your SAIG mailbox during the last ten days.
Security		Lists **Security Groups** and **User IDs** and controls access to EDconnect and the SAIG.

5.1.11 Import (.imp) files

An .imp file is very large version of a .tqt file. This is the most effective way for an institution to send large batches of records in one transmission. Only users that are set-up as “unattended” users can use .imp files.

All .imp files must be created in a specific record layout in order to transmit successfully. Using an application such as Textpad is recommended to create the records, as they are dependent on the exact placement of information, and Textpad displays this information.

5.1.11.1 Setting up an .imp file

Below are the specific requirements for creating an .imp file.

Header Record

Field Number	Description	Type	Required	Length	Position
1	Serial Number	Numeric	No	4	1-4
2	Return Code	Numeric	No	4	5-8
3	Group ID	AlphaNum	No	50	9-58
4	Unattended User ID	AlphaNum	No	50	59-108
5	Encrypted User Password	AlphaNum	Yes	8	109-116
6	Response File Name	AlphaNum	Yes	260	117-377

Data Record

Field Number	Description	Type	Required	Length	Position
1	Serial Number	Numeric	No	4	1-4
2	Return Code	Numeric	No	4	5-8
3	Action	Alpha	No	1	9
4	Message Class	AlphaNum	Yes (Except for Action = T)	8	10-17
5	Fully qualified Path and File Name	AlphaNum	No	260	18-277
6	Batch Number	AlphaNum	No	50	278-327
7*	Mailbox	AlphaNum	No	7	328-334

* Ignored unless Servicer Mode is enabled. Contact the SAIG Help Desk to enable Servicer Mode if it is applicable to your institution.

Field Descriptions

Serial Number—This field is for positional reference only. No editing is performed on this field and it is not required. Mainframe systems should use this position to sequentially number the commands in the input file.

Return Code—This field represents the success or failure of processing this command. This field is ignored on input records, so it can be populated or left blank. However, this field will be populated with the return code for this record's activity in the Response File. (See Response File Name below.)

Unattended User ID—This field represents the **Unattended User ID** to use with the processing of this import file. This field is not required. If no **Unattended User ID** is specified for the current user, the user specified in the **EDconnect.ini** file is used. If an **Unattended User ID** is specified, that **Unattended User ID** must be listed in the Group ID that is provided. If no Group ID is specified for the current user, and the **Unattended User ID** is provided, it must be unique across all groups. Note that this is *not* the **User Name** field. The **User Name** field is used for auditing purposes by the Student Aid Internet Gateway.

Group ID—This field represents the **Group ID** to use with the processing of this import file. This field is not required. If no Group ID is specified for the current user, and the **FSA User ID** is provided, it must be unique across all groups. If neither **FSA User ID** nor Group ID is specified, a password must be provided for the user importing the file.

Encrypted Password—This field represents the password to be used with the specified or current user name. In EDconnect 8.3, the password is encrypted for extra security. The encrypted password can be found on the User Profile in EDconnect. If no FSA User ID or Group ID is specified, this password should match the user specified in the EDconnect.ini file. If the password does not match, the import process is aborted and the appropriate return code is written to the response file. The encrypted password can be found by going to the Security View screen, User, Properties tab, under the Verify Password field.

Passwords can contain special keyboard characters, such as @, #, and $, but because some computer platforms and programs use special characters as command characters, we recommend avoiding % (percent), ^ (caret), & (ampersand), < (less than), > (greater than), and | ("pipe" symbol). Do not use \ (backslash), / (forward slash), " (double quotation mark), or ? (question mark).

Response File Name—This field represents the file to which EDconnect writes the return codes associated with each command record. This field is not required and if not completed, a file called TQ.ERR in the current EDconnect directory is created. This response file contains an exact copy of the input file with the return code column filled in with the result of executing the command. This field must be a valid long file name, if present.

Action—This field represents the action to perform with the current record. "T" is currently the only valid action value. A command record with a "T" in the action column

will immediately transmit the batch-mode added contents of the **TQ** and record all transmission activity in the **Activity Log**. Note that only records within the **TQ** that have the "Batch Mode" field set to **True** are transmitted during an import transmission. The "T" record must be the last record in the import file, if present at all. Only one "T" record should be present in a given import file. If the action column contains a "T", all fields on the same record following "Action" are ignored. Leaving the action space empty will set the transmission to “Manual”, and after loading the batch mode contents, the user will transmit the batch-mode added contents using the “Transmit” feature.

Message Class—This field represents the message class to use for this command. This field is used to cross-reference the message class database to populate the majority of the **TQ** records. This field is required for all data records that do not have an Action Type of "T".

File Name—This field may represent the path and/or file name in which the user receives the requested message class data. This field may also represent the file to transmit to the Student Aid Internet Gateway for Send requests. This field is required on Send requests. When this field is blank on Receive requests, it is populated with the file name value from the associated message class database record.

Batch Number—This field is a pass-through value that each Application System can utilize as it wants. There is no editing done on this field.

Mailbox—This is a restricted use field and can only be used by Data Providers within the Student Aid Internet Gateway. This field will be rejected if used and the proper setup has not been completed. If you are a data provider and want to use EDconnect, please contact the SAIG Help Desk.

This field is used to indicate to which mailbox data is to be sent on Send records. Validation of this field is limited to checking the length, as a complete list of all mailboxes within the SAIG system is not available until a connection with the SAIG is established. If this field is left blank, the import process defaults the mailbox value to the corresponding mailbox specified in the **Message Class Manager** table.

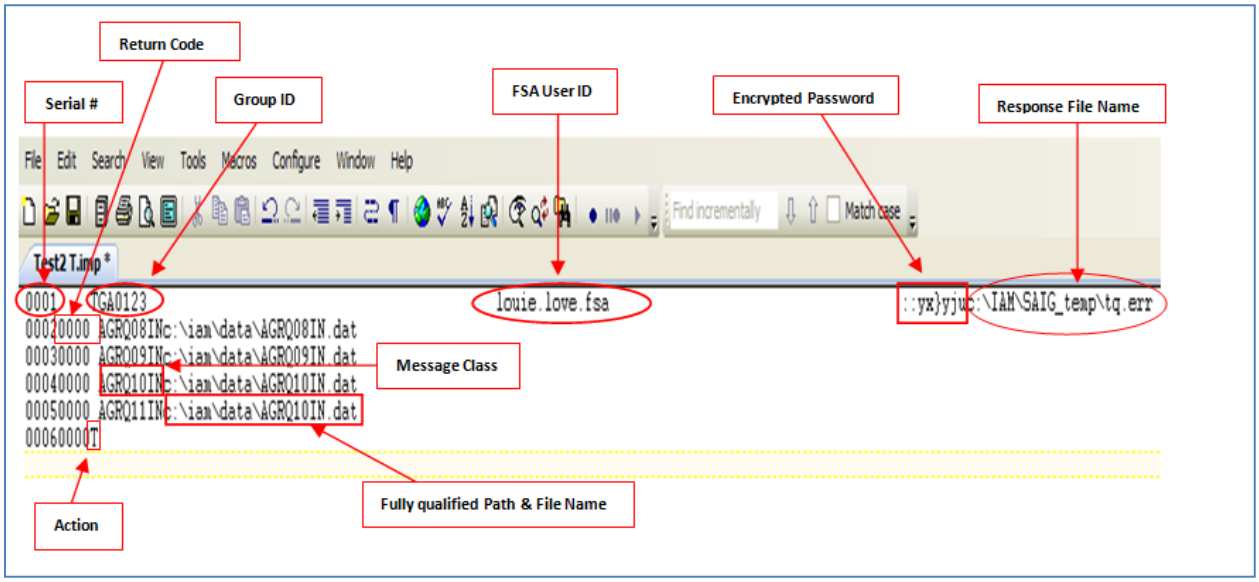
Return Codes

Below is the list of possible return codes you may receive if your .imp file is not created correctly. These will appear in the error log, the location and name of which is designated in the Response File Name field.

Value	Description	Corrective Action
0000	Command Successful	None
9999	User Error—The supplied user could not be loaded	1. Insure that the specified user exists in the EDconnect **Security View**. 2. Execute a disk verification program (Scandisk).

9998	Transmission Error—The import process was unable to completely finish the requested import transmission process.	1. See the EDconnect Help system for connectivity problem resolution. 2. Review **Activity Log** for possible causes.
9997	General Error—A general error has occurred.	Contact CPS/SAIG Technical Support.
9996	Duplicate—A record was requested to be added to the TQ that was already present.	Remove the duplicate request from the import file or from the existing **TQ**.
9995	Unknown Action—A record with an unknown action type was submitted.	Validate that all records in the import file have a valid action type.
9994	Password Error—An incorrect password was given for the user.	Verify that the password being used is valid for the specified user.
9993	Access Error—The user does not have access to perform this operation.	Verify that the security group in which the user belongs has update rights to the **TQ**.
0006	Message Class—Invalid value.	Verify that the message class import record exists in the Message Class database.
0007	File name—Invalid value.	Ensure that the file path is correct, and that a corresponding file exists in the specified directory.
0009	Incorrect Relationship b/t ID & Message Class	Verify the relationship between the ID and Message Class is correct.
0010	Batch Number—Invalid value.	Ensure a correct length for the Batch Number.
0012	Mailbox—Invalid value.	1. Ensure that a correct length mailbox is specified. 2. If adding a send record, ensure that the mailbox is specified in either the record or the message class database for the associated message class.
0013	Missing TG Number	Applies to Servicer Mode only. Verify that the TG number is in the correct spaces of record layout.
All others		Contact CPS/SAIG Technical Support.

Below is a partial image of a correctly set up .imp file.



The 'T' in the bottom line indicates that this is an automatic file. By placing the 'T' there, this will bypass the Security Authentication process and transmit automatically.

The other option is to leave that space empty. This creates a manual transmission, meaning that after the Security Authentication process is bypassed, the 'Transmit' icon or the 'Now' option in the Transmission menu must be selected by the user.

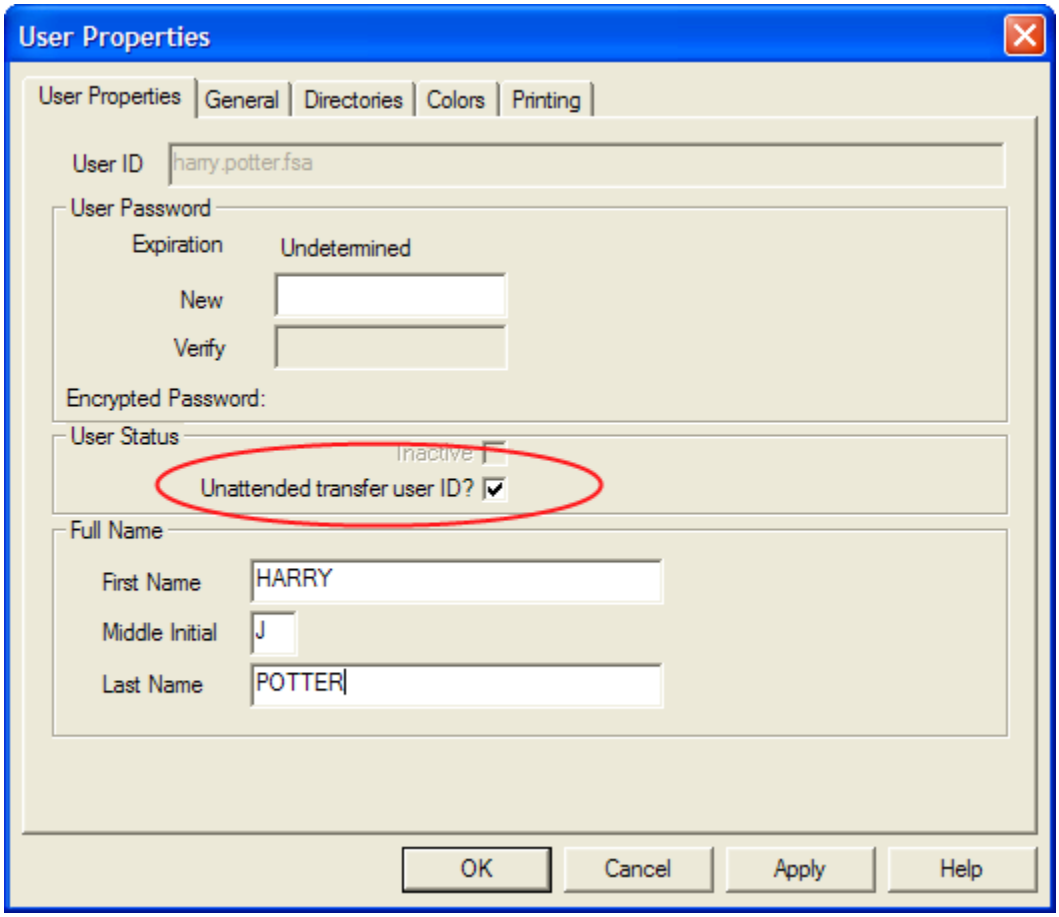
5.1.12 Unattended Transfer User ID and .imp files

Unattended transfers are normally used for sending large .imp files during off-peak hours to avoid slowing down the system. Only users marked as **unattended users** can use .imp files. For the purpose of this document, these users will be referred to as **Unattended User IDs.**

In the Security view, the user that will be making the unattended transfer must be marked as an unattended user, making it an **Unattended User ID.** Any username can be created for an **Unattended User ID**; it does not have to be an **FSA User ID**. **Unattended User IDs** will not be visible in the Security Authentication screen or able to log into EDconnect following a transmission in order to verify success.

An **FSA User ID** can be marked as an unattended user by checking the box in the User Properties dialog box, as shown below. Once this box is checked, the password fields will appear, allowing the **FSA User Password** to be entered and stored.

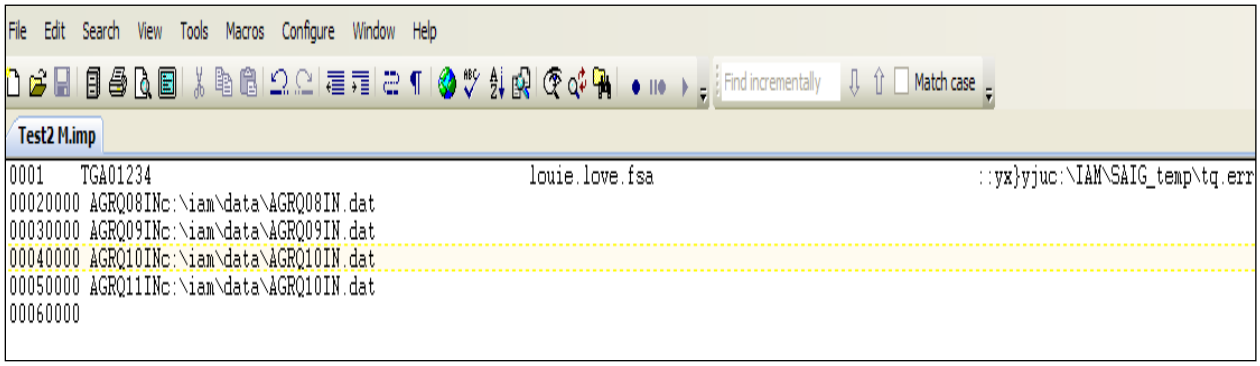
NOTE: Since an **Unattended User ID** is not able to log into EDconnect, an **FSA User ID** marked as unattended will not be able to log in. If Unattended User is marked accidently, a different **FSA User ID** will have to login in order to **uncheck** the **Unattended User ID**. It is highly recommended to create a username different from your **FSA User ID** to use as an unattended user.


User Properties
User Properties
General
Directories
Colors
Printing
User ID
harry.potter.fsa
User Password
Expiration
Undetermined
New
Verify
Encrypted Password:
User Status
Inactive
Unattended transfer user ID?
Full Name
First Name
HARRY
Middle Initial
J
Last Name
POTTER
OK
Cancel
Apply
Help

5.1.12.1 Loading .imp files into the TQ and Manually Transmitting as an Unattended User

For the manual transmission, you will need your .imp file to have the last link as blank.

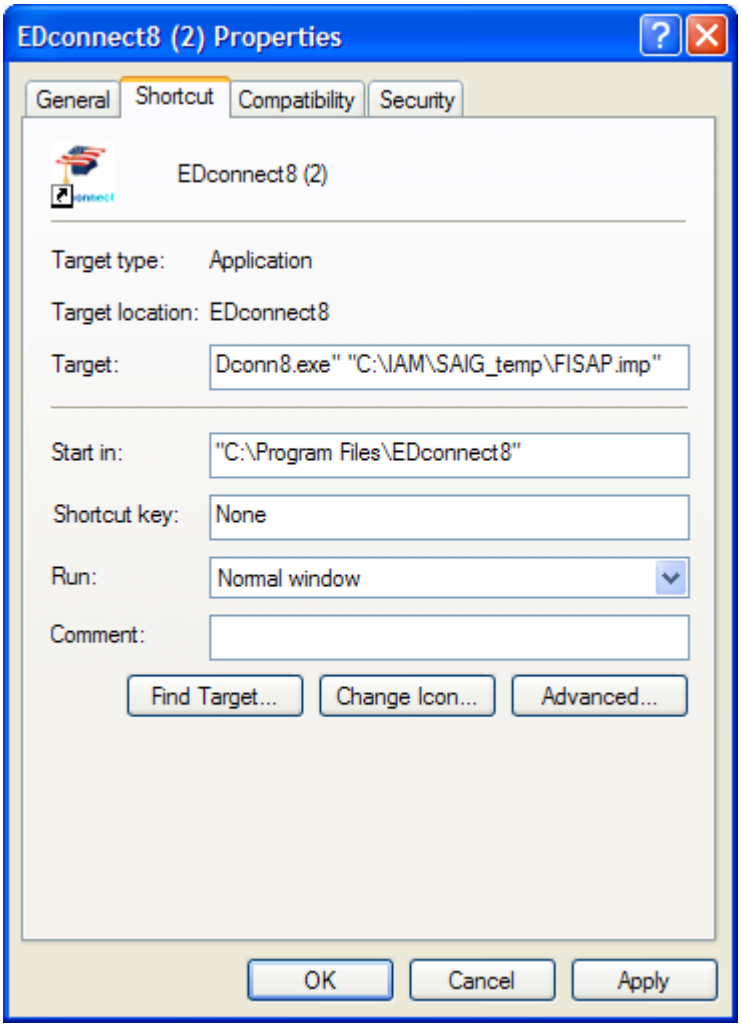
> **Note -** the last line reads 00060000. There is no 'T' following the number. This means a user will have to physically select the 'Transmit' icon or the 'Now' option under the Transmission menu.



1. On your desktop, where your EDconnect shortcut is, right-click on the shortcut and select 'Create Shortcut'. A second shortcut icon should appear. You can rename this as '.imp shortcut'.

You will need to add a string to the Target path where the .imp file is stored-in this case, it is in the C:\IAM\SAIG_temp\ directory. The Target path will display where your EDconn8.exe file is stored. In this example, the EDconn8.exe database is in the C:\ProgramFiles/EDconnect8 directory.

2. Right click on the '.imp shortcut' icon and select Properties. At the end of the Target path, enter "C:\IAM\SAIG_temp\FISAP.imp" so that it reads "C:\Program Files\EDconnect8\EDconn8.exe" "C:\IAM\SAIG_temp\FISAP.imp". Click **Apply**, then **OK**.



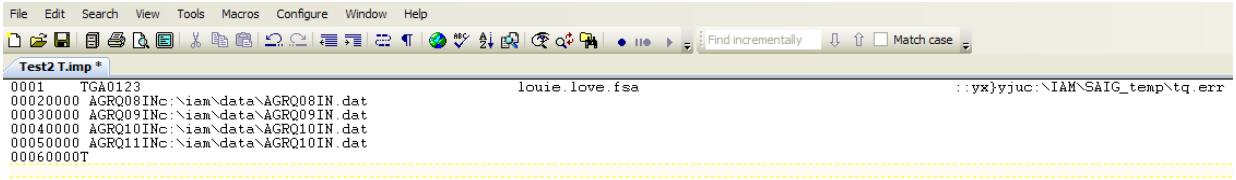
3. Double-click the '.imp shortcut' icon. The EDconnect logo will appear, and then minimize to the task bar. Click on this to view EDconnect and verify that you are looking at the Security View.
4. Click on the **TQ icon** and verify that the files loaded.
5. Click the '**Transmit'** icon or the '**Now'** option in the **Transmission** menu.
6. Verify transmission is successful. You also double check this looking at the **Activity Log**.

Helpful Hints

- For Windows Vista and Windows 7, the .imp files must be stored outside of the Program Files directory. It is recommended you place them in the C:\IAM\SAIG_temp\ directory for all operating systems.

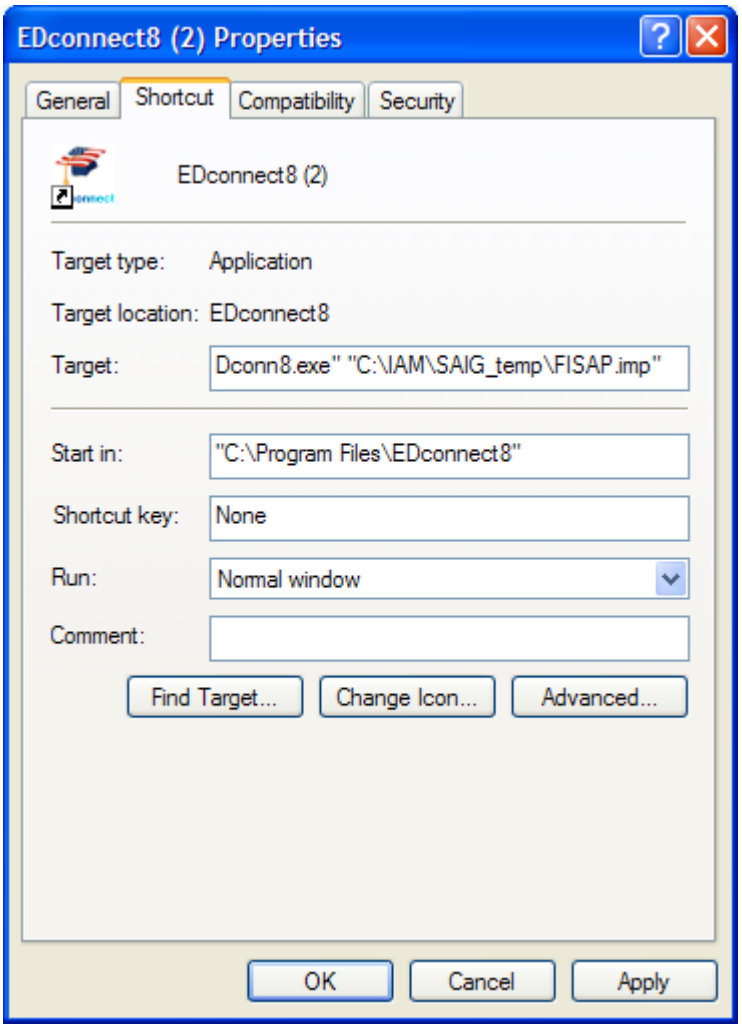
5.1.12.2 Loading .imp files into the TQ and Automatically Transmitting as an Unattended User

- For the manual transmission, you will need your .imp file to have an extra 'T' in the last line.
  Note in the example, the last line reads 00060000T. This 'T' is the designator for an automatic, unattended transmission. This also means that a user does not have to physically select the 'Transmit' icon or the 'Now' option under the Transmission menu.



- On your desktop, where your EDconnect shortcut is, right-click on the shortcut and select 'Create Shortcut'. A second shortcut icon should appear. You can rename this as '.imp shortcut'.
- You will need to add a string to the Target path where the .imp file is stored-in this case, it is in the "C:\IAM\SAIG_temp\" directory. The Target path will display where your EDconn8.exe file is stored. In this example, the EDconn8.exe database is in the C:\ProgramFiles/EDconnect8 directory.

1. Right click on the '.imp shortcut' icon and select Properties. At the end of the Target path, enter "C:\IAM\SAIG_temp\FISAP.imp" so that it reads "C:\Program Files\EDconnect8\EDconn8.exe" "C:\IAM\SAIG_temp\FISAP.imp". Click **Apply**, then **OK**.



2. Double-click the '.imp shortcut' icon. The EDconnect logo will appear, and then minimize to the task bar. Click on this and verify that the transmission process has begun.

3. Verify transmission is successful. You can also double check this looking at the **Activity Log**.

Helpful Hints

- For Windows 7 and Windows Vista, the .imp files must be stored outside of the Program Files directory. It is recommended you place them in the C:\IAM\SAIG_temp\ directory for all operating systems.

6 EDconnect Error Codes

If a transmission fails, EDconnect asks you to review the **Activity Log** for details. In most cases, the error message in the **Activity Log** consists of an error number followed by a brief explanation of the error.

The first section of the *EDconnect 8.3 Error Code List* provides descriptions of **Numerical Errors** you may receive and their possible resolutions. Some of the resolutions may require the help of your technical support staff or network administrators.

Under certain circumstances, you may receive non-numerical error messages or other program errors. These are described in the **Non-numerical Errors** section of the list.

Entries are arranged alphabetically unless the most common cause of a particular error is noted first.

Security Authentication Errors occur when a user tries to login to EDconnect without the proper credentials. You will need your assigned **FSA User ID** and **Password**, and **One-Time Password,** if applicable, from FSA before you can login to EDconnect.

The instructions assume that the EDconnect program files have been installed to the default **C:\Program Files\EDconnect8** folder. The program files will typically be located on the local hard drive even if the EDconnect database is on a network drive. If EDconnect has been installed to a different folder, adjust the instructions accordingly.

Before Calling SAIG Help Desk

Before contacting the SAIG Help Desk (800-330-5947, or by e-mail at **CPSSAIG@ed.gov**) for assistance with transmission problems, make sure that you are able to access the Internet. EDconnect uses your existing Internet connection. If you are unable to view Web pages in your Web browser, EDconnect will not be able to connect to the Student Aid Internet Gateway (SAIG).

You may also want to try one or more of the following to resolve transmission problems:

- Exit EDconnect, log back in, and try another transmission.
- Restart your computer and try another transmission. If you connect to the Internet though a Local Area Network (LAN), restarting your computer may establish a better connection.
- If you connect to the Internet through a modem and an Internet Service Provider (ISP), disconnect from the Internet and connect again. Try another transmission.
- Wait and try another transmission later. If you have been successfully sending and receiving files using EDconnect, many transmission errors (Error -1 and Error 4xx, in particular) will resolve themselves.

Note: After a failed transmission, a **Mailbox Query** will usually report that your “Mailbox is empty.” This does not mean that your files have been lost. A successful transmission

is required before a **Mailbox Query** will accurately reflect the contents of your SAIG mailbox.

Under normal circumstances, you will not lose any files due to transmission failures. The EDconnect **Activity Log** can help you determine which files you have successfully received.

6.1 Numerical Errors

An error code may be preceded by a minus sign, as in **Error -1**. The presence or absence of a minus sign does not change the meaning of the numerical codes listed below.

Note: The SAIG Help Desk cannot provide specific information for configuring firewalls and proxy servers, although we may be able to offer general assistance.

6.1.1 Error -1

Error -1 indicates that EDconnect cannot connect to the SAIG. You will receive **Error -1**, for example, if your Internet connection is not responding or if a firewall is preventing EDconnect from accessing the Internet.

Listed below are some of the possible causes of **Error -1**.

Table 1: Error -1

Problem	Solution
CheckPoint firewall asks for a password	CheckPoint firewalls can be configured to request passwords from users before allowing outbound Internet transmissions. EDconnect may generate **Error -1** if CheckPoint prompts you for a password. Your technical support staff may need to remove the password requirement for EDconnect.
Dial-up ISP is not currently connected to the Internet	If you connect to the Internet through a modem and an ISP, you will need to connect to the Internet *before* transmitting with EDconnect. Make sure you have selected "Direct Connection" from the **Connection to use** drop-down box in EDconnect by clicking on the **Tools** menu and selecting **Customize**.
Inadequate permissions or settings	You may not have the necessary permissions or access rights on your workstation or network to transmit with EDconnect. Check with your technical support staff. Have one of your network technicians log into your workstation as an administrator and try a transmission. If the transmission is successful, the technician will need to change your permissions or access rights.
Internet connection is not working	Make sure you are able to view Web pages in your Web browser. If you are unable to access the Internet, EDconnect will not be able to connect to the SAIG.
Local Area Network (LAN) connection is not plugged in	Make sure the LAN cable is connected to your workstation. If it is not plugged in, plug the cable back into the network card in your workstation.
Microsoft Winsock Proxy Client (WSP Client) is not enabled	If your workstation has WSP Client, WSP Client needs to be enabled for EDconnect to connect to the SAIG.
Network interface card (NIC) driver may be corrupt	Try uninstalling and reinstalling the NIC driver. If you have multiple instances of the same NIC driver on your workstation, delete the extra instances of the driver, reboot, and try transmitting again.

Problem	Solution
NIC card may be "mapped" to a specific physical location	The SAIG Help Desk talked with a customer who had moved her workstation to another location and received **Error -1** when she tried to transmit. When she moved her workstation back to its previous location, she no longer received the error. Her technician determined that the NIC card in her computer was "mapped" to the network connection in her original location.
Packateer software is running	See **Error 4xx**.
Port 26581 is closed by a firewall	Port 26581 must be open for outbound TCP/IP transmissions and enabled for FTP sessions, and you will need to be able to connect to saigmailbox.ed.gov. If you have never successfully transmitted with EDconnect, contact your network administrators to see if you are behind a firewall.
Proxy client not installed	**Error -1** may occur if a proxy server is running on the network but there are no proxy clients on the workstations using EDconnect. Installing the proxy client on any workstation that uses EDconnect may allow transmissions to go through.
Proxy server is not configured correctly	If you have a proxy server, port 26581 must be open for outbound TCP/IP transmissions and enabled for FTP sessions. Your network administrators may need to add rules to the proxy filters. Common proxy servers include WinProxy, MS Proxy Server, WinGate, and BorderManager (Novell). Product vendors may be able to provide specific information about proxy setup.
Temporary problem with the SAIG	Occasionally, there may be a momentary disruption of the SAIG, causing you to receive **Error -1**. If you normally do not have trouble transmitting with EDconnect, the problem will usually resolve itself in a short time. Try another transmission later. You may want to wait until after peak SAIG network demand, which is between 8:00 a.m. and 10:00 a.m. Central Time.
Workstation has no firewall client	If your network has a firewall, the firewall may require a client on workstations that use EDconnect. You may receive **Error -1** if the client is not installed. Your technical support staff should install the firewall client, if necessary, on workstations that use EDconnect. The firewall vendor may be able to provide technical assistance.
Your network uses Microsoft Proxy II	The following information was provided by a customer's technician: The Microsoft Proxy II client may need to be installed on workstations that use EDconnect. The name of the clientfile is WSPCLNT. It is located in the share folder with the proxy server.
Your network uses Novell Border Manager (Novell proxy)	The following information was provided by a customer's technician: Create an exception that allows the client to contact the server from the private interface to the public interface over TCP (as opposed to IP or UDP) with a source port of "all" and a destination port of 26581. Create another exception that allows the server to respond to the client from the public interface to the private interface addresses would also narrow the exception.
Your network uses WinProxy (proxy server)	If your network uses WinProxy, you or your technical support staff should edit the HOSTIPNAME entries in the *tdclient.ini* file, located by default in the **C:\Program Files\EDconnect8** folder, to add the proxy server

Problem	Solution
	IP address. Change the two lines as follows: HOSTIPNAME=*add proxy server IP address here* HOSTIPNAME2=saigmailbox.ed.gov If this does not solve the problem, change HOSTIPNAME back to saigmailbox.ed.gov and delete the entry for HOSTIPNAME2.

6.1.2 Special Requirements for Specific Firewalls

Table 2: Specific Firewalls

Firewall	Requirement
CheckPoint firewall	Version 4.0 with Service Pack 6 and version 4.1 with service pack allow SSL (TLS) negotiation and file transfer. Version 4.0 with Service Pack 7 and version 4.1 with Service Pack 2 or 3 require the application of a patch provided by CheckPoint.
Cisco firewall	The following information was provided by a customer's technician: FTP is a "jump port." It jumps between FTP port 21 and FTP port 20. With a Cisco firewall, you need to modify or add to the fix-up table, where it lists the common "jump port" protocols, and tell it that FTP [for EDconnect] is using a port other than the norm—in this case port 26581.
Gauntlet firewall, Alta Vista firewall, and Netscape Proxy	These firewalls require socks 5. NEC's eBorder Client is a socks 5 client available for downloading from the NEC website at nominal cost. Other socks clients are available from other vendors.
Raptor firewall	Raptor firewall earlier than 6.5 will not accept the AUTH command. Upgrading to version 6.5 will solve the problem.

6.1.3 Error 2

Error 2 occurs when EDconnect cannot establish an FTP session. See **Error -1** for possible solutions.

6.1.4 Error 4.xx

Error 4xx (the "xx" can denote any number combination) is the result of a slow network connection, which may be due to problems on your network or unusually high network traffic. If you have been transmitting successfully with EDconnect, **Error 4xx** is usually a temporary problem that will resolve itself. Waiting and trying another transmission later will frequently solve the problem without any further action on your part.

Listed below are some of the possible causes of Error 4xx.

Table 3: Error 4xx

Problem	Solution
General connectivity problems	• Your network may be running slowly or dropping its connection to the Internet. Check with your technical support staff to see if there are problems with your network connection. • Unusually heavy traffic on your local network may cause **Error 4xx**. If you only experience **Error 4xx** at certain times of day, check with your network administrators to see if those times coincide with peak network demand. • Unusually heavy traffic on the SAIG may cause **Error 4xx**. Try another transmission later. Peak SAIG usage is often between 8:00 a.m. and 10:00 a.m. Central Time. • If you access the Internet through a LAN, rebooting your computer may help resolve **Error 4xx**. Restarting your computer will establish a new connection to your network. • If you use a dial-up ISP, disconnecting from the Internet and connecting again may create a faster or more stable connection.
You may have too many programs running	See if closing some programs will stop the error or increase transmission speed.
Your network uses Packateer or other software to set priorities for Internet connections or to limit Internet access	Packateer is a program that sets priorities for Internet traffic. If the priority for EDconnect is set too low, EDconnect may "time out" with either **Error -1** or **Error 4xx**. Other programs that may affect transmissions include NetEnforcer, ESafe, and many software firewalls. Any program that filters Internet packets or scans files during transmission may interfere with EDconnect. Check with your network administrators. They may want to disable these types of programs temporarily to see if the programs are causing the problem.

6.1.5 Error 5.xx

Listed below are some of the possible causes of Error 5xx.

Table 4: Error 5xx

Problem	Solution
Error 531 **"Your SAIG network password has expired."**	If you receive **Error 531**, you need to transmit a new SAIG password. This error code appears in the Activity Log or the More window of the Transmission screen. Following the failed transmission, EDconnect asks if you would like to complete a SAIG password change. If you select **Yes**, the program takes you to the appropriate network wizard security screen and walks you through the password change. You will need to perform another transmission in order to transmit the new password. See **Error 536**, below, for SAIG password rules. Please note that performing a Network and Local SAIG password change does not change your user password. "Local," in this context, refers to the fact that EDconnect stores the SAIG password locally (i.e., within the database).
Error 533 **"Login incorrect. Please check your TG Number and/or TG Password."**	If you receive **Error 533**, you first need to confirm that the TG number you are using to transmit is the correct TG number. You can check by selecting **File**, **New**, **Security View** from the EDconnect menu bar, right-clicking on the *group* (not the *user*) your FSA user ID is under, choosing **Properties**, and clicking on the **Network** tab of the Group Properties dialog box. The TG number field is at the top of the tab. If the TG number is correct, your TG password (SAIG network password) is incorrect, and you will need to call the SAIG Help Desk to have your password reset. In order to reset your password, CPS/SAIG Technical Support requires the Social Security Number and date of birth of the Destination Point Administrator assigned to the TG number.
Error 534 **"Login incorrect. Please check your TG Number and/or TG Password."**	See **Error 533**, above.
Error 535 **"You are attempting to reuse a previously used TG Password. Please select a new TG Password."**	Your network password cannot be the same as any of the five network passwords you have used most recently.

Problem	Solution
Error 536 **"Your password does not meet the minimum criteria. Please see the EDconnect error codes listed in the EDconnect Installation and User Guide for further information."**	EDconnect has specific rules for SAIG passwords: • Must be a minimum length of eight characters. • Must begin with an alpha character • Must contain at least two alpha characters of different cases (uppercase/lowercase) and at least one numeric character • Cannot be the word "PASSWORD" (uppercase, lowercase, or mixed case) • Cannot be the same as any of the previous five passwords • Password will be locked out after three failures. (You must wait 30 minutes for your password to be unlocked. After 30 minutes, you can try again. If you have forgotten your password, you should use the Forgot Password button to retrieve it.) Can contain special characters • SAIG passwords can contain special keyboard characters, such as @, #, and $, but because some computer platforms use certain special characters as command characters, we recommend avoiding % (percent), ^ (caret), & (ampersand), \ (backslash), / (forward slash), < (less than), > (greater than), and | ("pipe" symbol).
Error 537 **"You have exceeded the maximum number of attempts to log in and your account has been locked. Please call CPS/SAIG Technical Support at 800/330-5947 to have your account unlocked."**	For enhanced security, after three failed transmissions due to an invalid SAIG password, your SAIG account will be locked, and you will be unable to transmit successfully until it is unlocked. You need to call the SAIG Help Desk to have it unlocked. In order to unlock your account, the SAIG Help Desk requires the Social Security Number and date of birth of the Destination Point Administrator assigned to the TG number.
Error 540 **"Either the TG Number or existing TG Password you provided was incorrect. Please verify accuracy of information and resubmit."**	See **Error 533**, above.

6.1.6 Error 10

Table 5: Error 10

Problem	Solution
"No networks defined" in the tdclient.ini file	**Error 10** usually indicates that EDconnect was not installed correctly. Back up the database (**EDconn8.mdb**) and uninstall EDconnect. Perform a full installation. Replace the blank **EDconn8.mdb** with the database you backed up. Please call the SAIG Help Desk for assistance if necessary.

6.1.7 Error 13

Table 6: Error 13

Problem	Solution
"Passwords must match"	You may receive **Error 13** if EDconnect has performed an illegal operation and shut down during a previous transmission. Under most circumstances, you can eliminate the error by resetting your network password using the **TDCommunity Manager** (**TDCM**) and performing a **Local Only** SAIG password change in EDconnect. For instructions on using the **TDCM**, see the **TDCommunity Manager (TDCM) User's Guide**, available at the FSA Download website (**fsadownload.ed.gov)**. Instructions for changing the SAIG password are included in the EDconnect Help file. To locate the information, choose **Help Topics** from the **Help** menu and click on the **Index** tab. Type in "Change My SAIG Password" (without the quotation marks) to locate the topic.
The "list.fil" file is in use by another program.	During testing, SAIG encountered this error when the "list.fil" file was open in another program during a transmission.

6.1.8 Error 31

You will receive **Error 31** if there is not sufficient free space on the drive on which the **Send** and **Receive** folders are located. Make sure the drive has enough free space.

6.1.9 Error 48

If you receive **Error 48**, check with your technical support staff to see how you connect to the Internet. If you use a "virtual modem," it may be configured incorrectly. Your technical support staff will need to resolve the issue. CPS/SAIG does not support virtual modems.

6.1.10 Error 70

EDconnect may be trying to access a file or folder on a network drive that another user is also trying to access. Restart your computer and try the transmission again.

6.1.11 Error 103

Restart your computer and try another transmission. If you continue to get **Error 103**, back up your EDconnect database (**EDconn8.mdb**) and uninstall and reinstall EDconnect. Restore your original database. Please contact CPS/SAIG Technical Support if you need assistance.

6.1.12 Error 107

Table 7: Error 107

Problem	Solution
An FTP session cannot be initiated	This error occurs when an FTP session cannot be initiated by EDconnect. See Error -1 for possible causes of this error.
Some of the EDconnect program files or folders are read-only	Files that have been saved to CD have the read-only attribute set by default. If you have restored any EDconnect files from a CD backup, make sure you remove the read-only attribute from all restored files.

6.1.13 Error 118

Error 118 is similar to Error 4xx, but seems to occur more often when a dial-up ISP is used to connect to the Internet. See Error 4xx for possible resolutions.

6.1.14 Error 203

EDconnect may be attempting to access a file or a folder on a network drive that is in use by another user or program. Restart your computer and try another transmission

6.2 Non-Numerical Errors

Table 8: Non-numerical Errors

Problem	Solution
"Access denied because the username and/or password is invalid on the domain"	You may have selected "T4WAN-X" or "SAIG-X" as the **Connection to use**. Select **Customize** from the **Tools** menu. Under most circumstances, you will want to choose "Direct Connection." If you connect to the Internet through a dial-up ISP, you will need to establish a connection *before* using EDconnect.
"EDconnect must shut down" when opening EDconnect (Windows XP)	Right-click on the Desktop shortcut for EDconnect and select **Properties** from the pop-up menu. The **Convert** box must not be checked on the **Compatibility** tab.
"Failed to create an empty document" when starting EDconnect or during transmission	Two EDconnect files need to be in the same folder as the EDconnect database: **T4api.exe** and **t4api.ini**. During a local installation of EDconnect, the files are installed by default into the **C:\Program Files\EDconnect8** folder. During a network installation, the files are installed into the network folder containing the database. If your EDconnect database is on a network, check to see if the **T4api.exe** and **t4api.ini** are in the network folder containing the database. If the files are not in the network folder, move the files from your local drive to the network folder. If the files are on both your local drive and in the network folder containing the database, delete the files from your local drive.
"Invalid page fault in module Ssockapi.dll"	If you receive this error, you will need to uninstall and reinstall EDconnect. Back up your EDconnect database first **(EDconn8.mdb).** After you reinstall EDconnect, restore the backed-up database and try another transmission. If you still receive the error, contact the SAIG Help Desk for further assistance.
"Invalid sender for message class" error referencing CONNCT32 files	EDconnect sends a CONNCT32 file each time you transmit. Under normal circumstances, the file is automatically deleted from your mailbox. If the file is not deleted promptly, EDconnect will try to download it, generating the error. You may see the error if you have tried several transmissions over a short period of time. Clicking the OK button on the error message dialog (this sometimes requires several clicks) will usually allow you to download your files. The next time you use EDconnect, you should not receive the error.
"Invalid sender for message class" error referencing files other than CONNCT32	Contact the SAIG Help Desk at 800-330-5947 for assistance with this error.

Problem	Solution
"Path does not exist" during Transmission	This error refers to the **Send** or **Receive** paths that have been set up in EDconnect, such as **C:\IAM\Data**. If you receive this error, first check to make sure the paths are valid. This is particularly important if your **Send** and **Receive** paths are on a network drive. Your workstation may have temporarily lost its connection to the drive. If the paths exist, you will need to check the folder properties to see if the folder attributes have been set to read-only. Right-click on each folder in the path (such as **C:\IAMm**) and select **Properties** from the pop-up menu. Check the folder **Attributes**. If the folder is read-only, uncheck the read-only box and click **OK**. Right-click on the folder again to make sure the change has "stuck." If you find any read-only folders in the EDconnect **Send** or **Receive** paths and cannot remove the read-only attributes, contact your technical support staff. They may need to use the "attrib" command to remove the read-only property from folders that are "stuck" by opening a command prompt and using the command "attrib -r c:*folder name*". The command must be used on each read-only folder in the **Send** and **Receive** paths.
"System error: error encountered during shell execute" (Windows 2000)	If you receive this error when starting EDconnect, clicking OK will usually allow you to continue normally. To fix the problem, select New from the File menu and Security View from the list of views. Right-click on your User ID and choose Properties from the pop-up menu. On the General tab, uncheck the "Show splash screen on startup" checkbox and click OK. Exit EDconnect and start it again. You should no longer see the error message.
"System error: unable to remove headers and trailers" (Windows 2000)	You may receive this error if you are not a Power User or Administrator of your Windows 2000 workstation, or if you do not have permission to download files to certain network folders (in particular, the **Receive** folder specified in EDconnect). Have one of your technical support staff log on as an administrator and try a transmission. If this works, your technical support staff will have to change your permission levels.

7 Security Authentication Errors

An error message will display when the security authentication process fails and you are denied access to EDconnect.

Table 9: Security Authentication Errors

Problem	Solution
"Your password is about to expire. Choose Yes to go to the web page to change it."	Click "yes" to be routed to the change password website.
"Your password is expired. Choose Yes to go to the web page to change it, then return to authenticate."	Click "yes" to be routed to the change password website. Return to Security Authentication screen to authenticate.
"Authentication failed. You have used an invalid User ID or password."	If you receive this error, you need to confirm that the FSA User ID and FSA User Password you are authenticating are the correct FSA-issued ID and Password for the assigned TG Number. If the FSA User ID, FSA User Password, and TG number are correct, you may need to call the SAIG Help Desk to have your password reset. In order to reset your password, the SAIG Help Desk requires the Social Security Number and date of birth of the Destination Point Administrator assigned to the TG number.
"Authentication failed. This account has been temporarily locked for 30 minutes due to too many failed login attempts. Please wait 30 minutes and try again. **If you have forgotten your password, please select the Forgot Password button to reset your password. You may log in with the new password after the initial 30 minute wait has elapsed."**	If you receive this error, you will need to wait 30 minutes to login again.
"Authentication failed. You have an account that has been disabled. Please contact the SAIG Help Desk for Assistance."	If you receive this error, you will need to call the SAIG Help Desk.

Problem	Solution
"Authentication failed. You have used an invalid Security Code. If you have forgotten your token, choose Yes to go to the FORGOT Token web page." "Otherwise, please contact the SAIG Help Desk for assistance."	If you receive this error, you will need to call the SAIG Help Desk.
"Authentication failed. Your token information was not found. Please register your token. Choose Yes to go to the web page to register it, then return to authenticate."	Select "yes" and your browser will route to the register your token website. After you register your token, you will need to return to the Security Authentication screen to authenticate your credentials.
"Authentication failed. Operation not allowed in current state of credential. Please contact the SAIG Help Desk for assistance. "	If you receive this error, you will need to call the SAIG Help Desk.
"You do not have permission to use EDconnect. Please contact Participation Management for details about how to participate. Choose Yes to go to the PM Enrollment web page."	Select "yes" and your browser will route to the PM enrollment website.
"Error Communicating with Authentication Service. Please wait a while and try again, or contact the SAIG Help Desk for assistance."	If you receive this error, you will need to call the SAIG Help Desk.

8 Miscellaneous

8.1 Sorting Records

The sort function enables you to organize records within a particular view.

To sort records in a view

1. Select **Sort** from the **Tools** menu.
2. Click the **down** arrow to the right of the text box to display a list of all the fields upon which you can perform a sort within a particular view.
3. Highlight the **sort** preference.
4. Click **OK**.

Helpful Hints

- You can also sort records based on a particular field by double-clicking the column header for that field.
- The records in that field sort in ascending order after the first double-click.

Double-click again on the same column header to reverse the order.

8.1.1 Filtering Records

Using the **Filter** option, you can filter out records of a particular type in a view so that you only see certain records.

You can filter records in the **Activity Log**, **Message Class Manager**, **Received File View**, **Mailbox Query**, and **Transmission Queue**.

To filter records

1. Select **Filter** from the **Tools** menu.
2. Click on the field you want to use as the filter criteria.
3. Enter the field contents you want to use to filter the records.
4. Click **OK**.

Helpful Hints

- You can filter on several criteria at once.
- To get the entire view back, open the Filter dialog box and click OK without entering information in any of the fields.

8.1.2 Changing File Paths

Follow these steps to change the file paths for data you send and receive:

1. Open the **Security View** by selecting **New** from the **File** menu and selecting **Security View** from the list of views. You can also click the **Security View** button on EDconnect's main toolbar.
2. Right-click on your **FSA User ID** in the **Security View** and select **Properties** from the pop-up menu, or highlight your **FSA User ID** and select **Properties** from the **Edit** menu.
3. Select the **Directories** tab of the **User Properties** dialog.
4. Click the **down** arrow on the right side of the selection box (the field at the top of the **Directories** tab).
5. Select **Send** or **Receive** from the list, depending on which directory you want to change.
6. Enter the path and folder in the next field. If you do not know the path, click **Browse** to select the path and folder.
7. If you would like all users within a **Security Group** to use the same file paths, place a checkmark in the box labeled "Set all users of this group to the specified directories." Create all users in the group first.
8. Click **OK** to save the directory settings.
9. Log out of EDconnect and log back in before performing your next transmission.

Helpful Hints

- There are three ways to set file paths:
  - On the Directories tab of the User Properties dialog.
  - In the Message Class Manager.
  - In the Transmission Queue.
- If you accept the default values during installation, EDconnect sets the default path for all files to "C:\IAM\DATA" but leaves the file path blank on the **Directories** tab of the **User Properties** dialog. If this field is blank, paths entered into the **Transmission Queue** or **Message Class Manager** take precedence over the default "C:\IAM\DATA" path.
- During a transmission, EDconnect checks the **TQ** to see if you have specified paths for particular files. If you have not specified paths, EDconnect defaults to the paths defined in the **Message Class Manager**. If the **Message Class Manager** does not contain path information, EDconnect uses the default path established on the **Directories** tab of the **User Properties** dialog, if it exists.
- If, on the other hand, you specify a default path during setup, such as "D:\IAM\DATA," EDconnect will ignore changes made to file paths in the **Message Class Manager**. Only changes made in the **TQ** will override the default path ("D:\IAM\DATA," in this example) established on the **Directories** tab of the **User Properties** dialog.

Before you can assign the path to a folder through the **Security View**, the folder must exist. Otherwise, you will get a “Directory does not exist” error message.

8.2 Getting Help

8.2.1 Online Help

There are several ways to access help.

To access Online Help within EDconnect

1. Select **Help Topics** from the **Help** menu.
2. Click on **Help,** which is available on many dialog boxes and windows.
3. Click into a field and press **F1**.

Note: If you are a Windows 7 or Vista user and are unable to view the help files system in EDconnect, you will need to download an additional "Windows Help Program" to your computer.

To download the Windows Help Program

1. Click on the "Microsoft Help and Support link" from the "Windows Help and Support" pop up box located in EDconnect.
2. Scroll down to the "Resolution" section of the "Microsoft Support" page
3. Under the sub section "How to obtain the correct version of the Windows Help program (WinHIp32.exe)" select the Windows Operating System (OS) link that you are running on your computer.
4. The Microsoft webpage will then navigate you to the "Download Center" where the files for downloading the Windows Help Program can be accessed.
5. Under "Files in this download" select the green button "Continue" to start the download process

To access the Online Help Index

1. Click the **Index** tab on EDconnect's Help system.
2. Start typing the name of a topic in which you are interested.
3. Look for the topic in the selection box.
4. Highlight the desired topic.
5. Click **Display**.

Note: The Index can help you find topics related to a similar subject or function.

Helpful Hints

- Be sure to expand the Help Contents books. Each book contains several individual Help topics.
- Check the **How Do I?** topics for frequently performed operations (select **How Do I?** from the Help menu).
- Watch for links to other topics.

- You can print topics by selecting **Print** from the **Options** menu on the Help screen.
- Use the **Find** tab on the Help screen to locate specific words or phrases anywhere within the Help text.

Note: You can also use the Help system **Options** menu to change the size of the font, keep a Help topic on top of other dialogs so it remains visible, create a note to be kept with a Help topic, or copy text from a Help topic.

8.2.2 The SAIG Help Desk

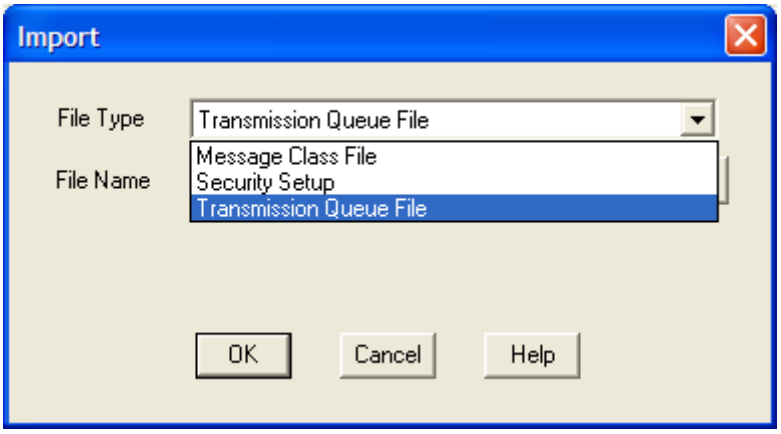
- Telephone: 800-330-5947 (no cost per call)
- TDD/TTY: 800-511-5806
- E-mail: **CPSSAIG@ed.gov**
- Fax: 319-358-4260
- Working hours are 8am–8pm (ET) Monday through Friday

9 Frequently Asked Questions

9.1 How do I import files?

Follow these steps to import files into EDconnect:

1. Select **Import** from the **File** menu.
2. On the **Import** dialog, choose the **File Type** of the file you will be importing. This can be either a **Message Class File** or a **Transmission Queue File** or a **Security Setup**.



3. Click the **Browse** button to select a file to import.
4. Click **OK**.

Helpful Hints

- The **Import** function can be especially useful if you have several PCs using the same **TG number**.
- Once you have downloaded the message class file on one PC, you can copy the file to a diskette and import it into the **Message Class Manager** on the other PCs using the **Import** dialog.
- The **Transmission Queue File** option is for .imps and can only be used with a .imp file that is set up for an **Unattended User ID**.

9.2 How do I print PMessages?

The U.S. Department of Education (ED) periodically sends out Program Messages (Pmessages) that automatically appear on your screen when you connect to the SAIG.

You can print a PMessage by selecting **Print** from the **File** menu while the PMessage is on your screen.

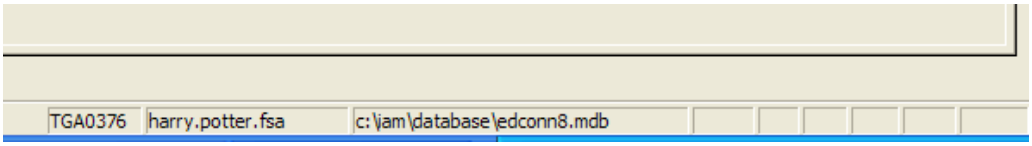
EDconnect also saves these messages on your PC for future reference. Follow these instructions to print a PMessage later:

1. Close all open views.
2. Select **Open** from the **File** menu.
3. Use the **Open** dialog to select the directory in which your PMessages are stored.
4. Choose the PMessage you want to print and click **OK**.
5. Select **Print** from the **File** menu, or the **Print** button from the toolbar.
6. Click **OK**.

9.3 What files do I need to move when changing PCs?

After installing EDconnect on a new computer, be sure to copy the **EDconn8.mdb** file from the EDconnect folder on your old PC to the folder of the same name on your new PC.

If you are uncertain about the location of **EDconn8.mdb**, EDconnect displays the path to the database at the bottom right of the EDconnect screen.



You should also move any folders that contain files you have sent or received, maintaining the same file paths, if possible. On a stand-alone PC, this is often C:\IAM\DATA.

9.4 Why am I getting an “Invalid Value” error message?

In most cases, the “Invalid Value” error message occurs because a field is empty or incomplete. EDconnect 8.3 highlights this field so you can fill it in correctly.

9.5 How do I combine files?

The **Combine** feature permits you to combine all files of the same message class into one file, if more than one is downloaded during a given transmission.

To combine files, go to **File, New, Message Class Manager View**. Within the **Message Class Manager**, place a check in the box located under the **Combine** column for each message class you wish to combine.

Warning! In order to maintain batch integrity, if you try to combine message classes that should not typically be combined, you will receive a warning message. The **Combine** feature should not be used, in particular, to combine files sent to you by the Common Origination and Disbursement (COD) System. COD files cannot be imported into the EDExpress or any third party software if the individual COD files are combined.

9.6 Why am I getting an error notification that cannot send a file?

Prior to transmitting a batch to the SAIG, EDconnect checks the first 8 bytes of the file for the text “O*N05.”

If EDconnect detects an O*N05 header in the first 8 bytes of the first record of a file, you will receive a pop-up error message that EDconnect has detected the presence of a transmission header record and the transmission will not proceed.

You must remove transmission headers and trailers from any files you attempt to send to SAIG.

9.7 What is the difference between a Security Authentication error and a Numerical Error?

A Security Authentication error exclusively occurs when a user tries to access EDconnect without the proper credentials. When these messages appear, always double check your credentials to make sure they are correct.

A Numerical or Non-Numerical Error occurs when there is an error not related to the Security Authentication process. These can include Internet connection problems and SAIG password problems.

9.8 I changed my SAIG password and now I can't transmit.

When you change your SAIG password, remember you have to update your local password as well. Your local password must match the current SAIG password.

If you continue to have an issue transmitting, please contact SAIG Help Desk at 800-330-5947 or by e-mail at **CPSSAIG@ed.gov**.

Appendix A – SAIG User Statement

Anyone who accesses Title IV program data and uses resources that access SAIG (such as computers or workstations) must read and sign this statement. Keep a copy of the signed statement for your records. A signed original SAIG User Statement must be completed and maintained by the destination point administrator for each of the destination points (electronic mailboxes) to which you have access.

A SAIG User understands that if he or she intentionally submits false or misleading information to the U.S. Department of Education, he or she will be subject to a fine up to $10,000, imprisonment for up to five years, or both, under provisions of the United States Criminal Code (including 18 U.S.C. 1001). The SAIG User also agrees to comply with all provisions of Section 483 of the Higher Education Act of 1965, as amended.

A SAIG User understands that the information provided to him or her by the U.S. Department of Education is protected by the Privacy Act of 1974, as amended. Protecting this information, once it is entrusted to the SAIG User, becomes his or her responsibility. Therefore, the SAIG User agrees to protect the privacy of all information that has been provided to him or her by the U.S. Department of Education. The SAIG user understands that any person, including himself or herself, who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and may be fined not more than $5,000.

Appropriate Use

At a minimum, appropriate use consists of the following:

- Using SAIG computing resources only for official government business. Any other use must be approved expressly by the U.S. Department of Education.
- Knowing the SAIG destination point administrator for each of the destination points you access and how to contact them.
- Protecting all SAIG information from access by or disclosure to unauthorized personnel.
- Reporting immediately to your destination point administrator any security incidents, potential threats, or vulnerabilities that involve SAIG resources.
- Protecting any tools, such as passwords, that allow you access to SAIG (these tools are called "authenticators").
- Reporting to your destination point administrator any compromise, suspected compromise, or incidents of sharing of a password or any other authenticator.
- Accessing only systems, networks, data, control information, and software for which you are authorized.
- Ensuring that all information that comes from SAIG is marked according to its sensitivity and is properly controlled and stored.
- Informing your destination point administrator when you no longer need access to a SAIG resource, such as when you change jobs or leave employment.
- Avoiding the introduction of any code that might be harmful to SAIG.

TG#_____ Destination Point Administrator (DPA) Name_____

SAIG User Name _____
(Print)

SAIG Job Title_____SSN_____Phone #(____)_____

SAIG User Signature_____Date_____

DPA Signature _____Date_____

NOTE: This statement, with an original signature, must be maintained by the Destination Point Administrator. DO NOT SEND THIS TO SAIG.

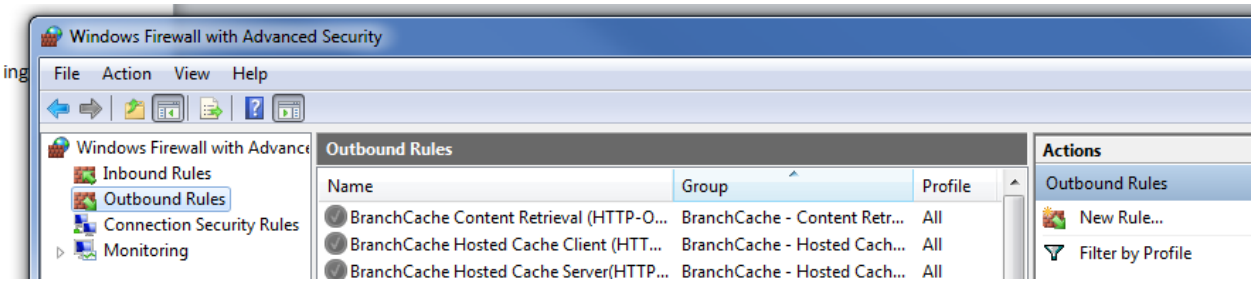
Appendix B – Installing EDconnect 8.3 On Computers That Have FDCC Security Settings

FSA users with FDCC security settings on their computer will need to follow an additional step after installing EDconnect 8.3 in order to enable transmissions to the SAIG mailbox server.

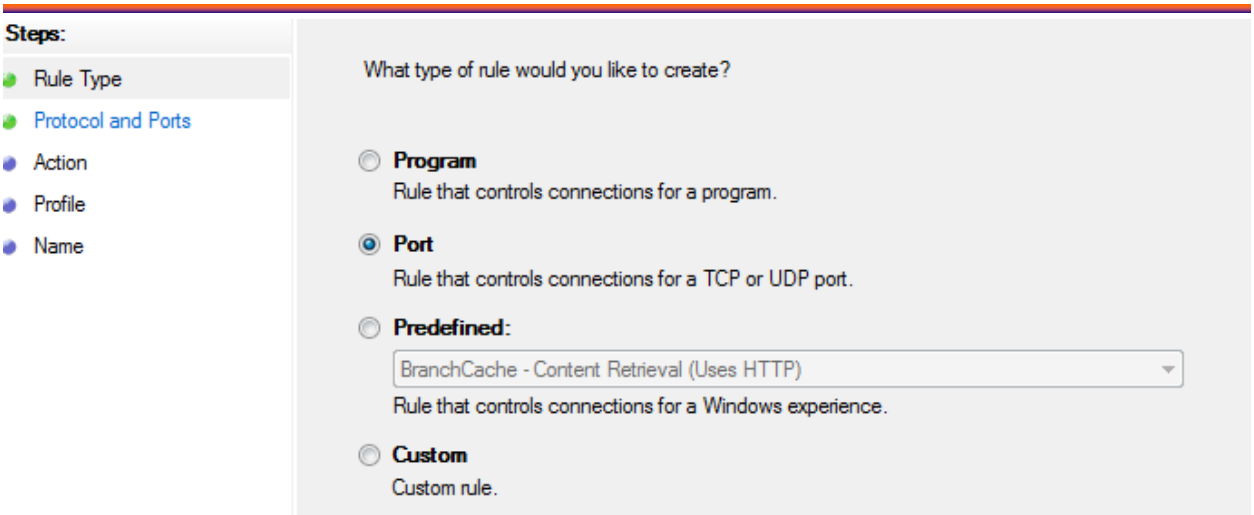
Please note that this additional step also requires local or domain administrator rights.

1. Log in with administrator rights and from the Control Panel window click on the Windows Firewall icon:

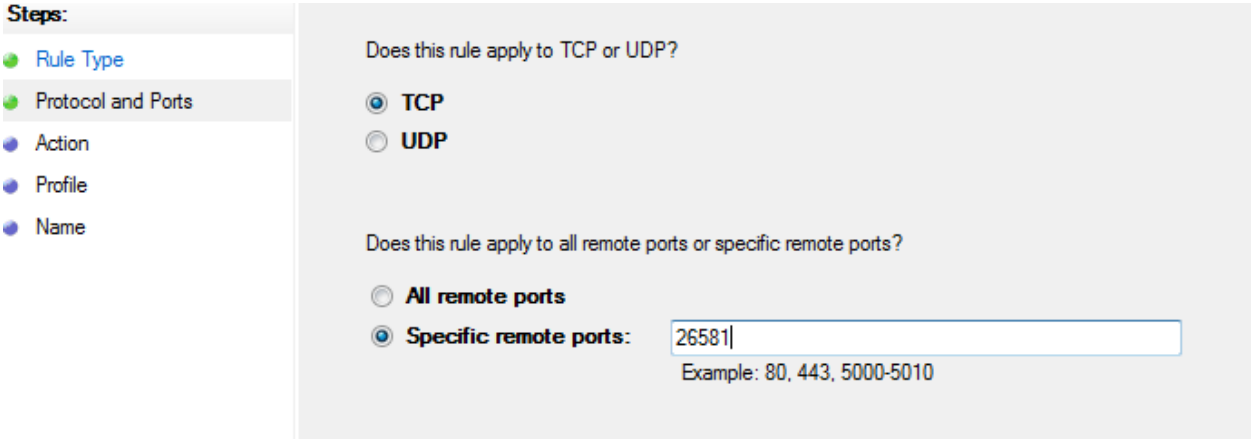
2. Click on "**Advance Settings**" to open the "**Windows Firewall with Advanced Security**" window.
3. Now we need to add an outbound rule for EDconnect 8.3 to connect to the mailbox server. Click on "**New Rule**" in the "**Actions**" panel:



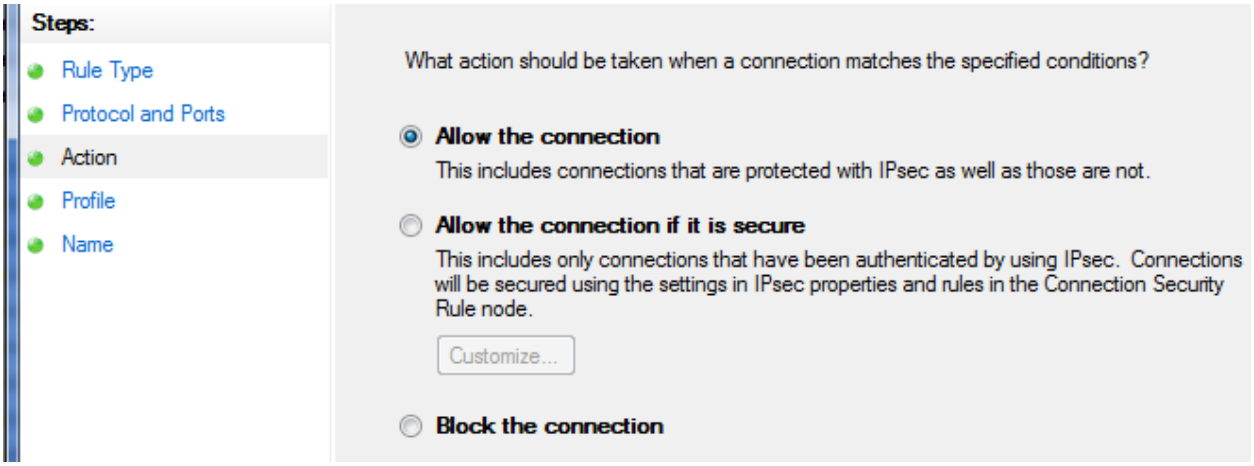
4. On the "**New Outbound Rule Wizard**", select "**Port**" and click "**Next**:"



5. Under the "**Protocol and Ports**" step, select "**TCP**" and "**Specific Remote Ports**" and enter **26581**, click "**Next**":



6. Next under the "**Action**" step select "**Allow the Connection"** and click "**Next**":



7. To apply this rule to different network profiles, select "**Domain, Private and Public**" in the "**Profile**" section.

8. Enter a name to identify this new outbound rule and click “**Finish**”.

Once this Firewall Outbound Rule is created EDconnect 8.3 will be ready to use with a FDCC compliant computer.