

AESDIRECT
ACCOUNT ADMINISTRATION USER GUIDE

TABLE OF CONTENTS

Section	Page
OVERVIEW	3
Changes to AESDirect Administration Process	3
New Roles in AESDirect Defined	5
The Transition Process	7
AESDirect Rules	9
Username Rules	9
Password Rules	9
Session Rules	10
THE MANAGE USER FUNCTIONS	12
HOW TO	14
Create a New User	14
Create a User Manager	18
Reset Passwords	21
Disable a User	24
Reactivate a Disabled User	26
Reactivate a Locked Out User	30
Change an Account Administrator	34
WHAT HAPPENS IF THE ACCOUNT ADMINISTRATOR LEAVES?	38

OVERVIEW

Changes to *AESDirect* Administration Process

On October 1, 2008, changes will be made to the *AESDirect* administrative process to both increase the security of your Export data and to increase the flexibility and ease of accessing the application.

These changes include:

- Individual User Account Administration
- Stronger Password Requirements
- Shorter Password Expiration Timeframes
- Automatic Inactive Account Deactivation
- Session Timeout/Concurrent Login Limit
- Account Lockout after 3 Unsuccessful Logins
- Expanded Account Administration Functions

Currently, only one Username and Password are required per filing company and each person responsible for filing Electronic Export Information (EEI) is required to use that login information. Additionally, there is only one individual at the company, the designated Account Administrator, who is responsible for all account maintenance and communication with *AESDirect*.

For example, if the username and password combination is lost, or the expiration date for the password has come and gone, the Account Administrator is required to fax, on company letter, a written request to have the account reactivated. That request is processed by *AESDirect* technical support who will call the Account Administrator and direct him or her in the steps necessary to reactivate the account and reset the password. Once done, the Account Administrator has to distribute the new password to all *AESDirect* users in the company.

This process has posed significant problems for both *AESDirect* Users and *AESDirect* Support. One, it is both time consuming and cumbersome. There are many opportunities for delay. While you do not have access to *AESDirect*, you cannot file. With filing now mandatory, delays can adversely impact your business.

One Username for multiple users poses a security problem. Every time an individual who knows the password leaves your company, the Account Administrator must change the password and redistribute. This can be problematic even in companies with a few employees. If the password is not changed, that departed employee will continue to have access to your filing data.

The changes put into place in *AESDirect* will offer greater autonomy and flexibility to account holders. No longer will Account Administrators be burdened with the task of tracking which employee has access to *AESDirect* or when one password will expire. Nor will they have to manage the paperwork of resetting that password. The new features added into *AESDirect*

spread the responsibility for these tasks over a whole company, automating processes that were once manual and guaranteeing a level of security to your EEI not available before.

New User Roles in AESDirect Defined

The new AESDirect establishes three distinct User types, each with a different role in the AESDirect Account.

Account Administrator

As before, the Account Administrator is responsible for the AESDirect account. However, he or she can now spread some of that responsibility to two (2) other AESDirect users in their account. The Account Administrator should be a Customs Compliance specialists and a company officer.

An Account Administrator's responsibilities include:

Interacting with AESDirect - If any change needs to be made to the AESDirect account that requires direct interaction with AESDirect technical support, the Account Administrator should be the initiating party. They will be required to sign documents requesting any substantial change.

Creating and Managing Users Managers – The Account Administrator can create up to two User Managers to help in the day-to-day management of traditional AESDirect Users.

Creating and Managing Users - The Account Administrator, as the first User in AESDirect, is responsible for creating users, providing individuals with a Username and Password and managing access to AESDirect for those Users, by manually resetting passwords or disabling accounts, when necessary. The Account Administrator can also delegate this responsibility to User Managers.

User Managers

The Role of a User Manager is very similar to that of the Account Administrator. A User Manager can serve as a point of contact for Users, to help them establish AESDirect Accounts, make changes to their account and to help users reset their passwords or reactivate disabled accounts. A User Manager is an AESDirect expert. User Managers cannot act legally on behalf of the Account holder when contacting AESDirect or make any changes to the Account Profile.

A User Manager can be any existing User in your AESDirect account. Your Account is limited, however, to only two (2) User Managers. Both the Account Administrators and other User Managers can create a User Manager.

Users

Users hold the most fundamental role in AESDirect. They are responsible for the day-to-day filing of EEI. Users can also be limited to just viewing historical filing data.

This Administrative Guide was created to help the Account Administrator and the User Manager understand fully their role in AESDirect. Users and those Account Administrators and User

Managers who will file EEI should look to the **AES*Direct* User Guide** to understand that set of responsibilities.

The Transition Process

The transition to the upgraded Account Maintenance features will be driven by your password expiration date. Currently, all passwords expire every 180 days. After October 1st, all password expiration timeframes will be cut in half. If your expiration date is within 2 weeks or less of October 1st, no change will be made; your expiration date will remain the same.

Once an Account Password expires, the Administrator will be forced to upgrade their *AESDirect* Account to include the new features. Account Administrators, however, may choose to do this before their expiration date, but after October 1st. A link will appear under **Account Maintenance** that will allow you to initiate the transition on your schedule.

Otherwise, when your password has expired, you will be asked to create a new Account Administrator username and password. You may then create new usernames and passwords for those in your company responsible for filing. Your original username and password for *AESDirect* can still be used for 15 days following the upgrade. This username will not be subject to any of the new *AESDirect* security restrictions during this timeframe.

Use these 15 days wisely. Put in place a plan of action prior to the upgrade that includes identifying the person responsible for managing the upgrade and a strategy for disseminating the new usernames and passwords. This 15 day period should provide ample time to execute that plan of action.

When the 15 day transition period expires, lockout and session concurrency rules will be applied to your original *AESDirect* username. The password will expire and must be reset. At this time, all filers should file with their own Username and password.

A sample process is outlined below:

- 1) Log into *AESDirect* with the old *AESDirect* Username and Expired Password

A page will prompt you to enter your Admin Code, for the very last time, and create a new Username and Password

Note: Once upgraded, your password expiration date for the original username will be extended for 15 days. After 15 days, the password will expire. Notify all users in organization immediately.

- 2) Designate an Account Administrator
- 3) Create New Users

Users created should be determined by your organization and enhance your current workflow.

- 4) Create User Managers
- 5) Distribute new Individual Usernames and Passwords

Best Practice: Retake the Quiz

As you transition to the new Account Administration process and assign individual Usernames and Passwords, Users will not be required to retake the Certification Quiz. You may, however, ask your users to retake the Quiz before they can fully access AESDirect.gov. This may provide a good opportunity to refresh their memory on correct processes for using *AESDirect* to file and monitor their EEI.

AESDIRECT RULES

Username Rules

Each User in *AESDirect* should have their own Username. To clearly identify each User and to provide equal access to all users, strict rules are in place for the creation of Usernames.

Unique - All *AESDirect* usernames must be unique across the *AESDirect* system, even between different companies. For example, Company ABC creates username 'JohnDoe.' Company XYZ cannot also create a 'JohnDoe.' They may, however, create a version of this username, such as 'JohnDoe123' if available.

Complex – Usernames must be alpha-numeric and between 3 and 25 characters long

Usernames are Not Case Sensitive

One Life Only – Once a username is created, it is permanently assigned to the company that created it, even if the user moves to a new company.

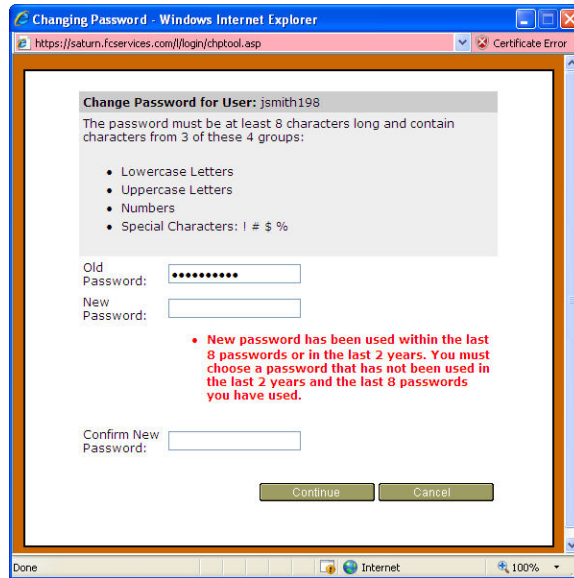
Password Rules

As with Usernames, *AESDirect* Password Rules are strictly enforced, in this case, to maximize security. Common words and phrases are not acceptable.

Complex – All passwords must be at least 8 characters long and contain characters from 3 of the following 4 groups:

- Lowercase letters
- Uppercase letters
- Numbers
- Non-alphanumeric characters (!, \$, #, %);

At least 6 of those characters may occur only once in the password



Unique – Passwords cannot contain any familiar words or sequential character strings. They must also vary significantly each time they are reset.

- Passwords cannot contain any string that is also contained in the username
- Passwords cannot contain any dictionary words
- Passwords cannot contain any common strings such as
 - A sequential series of letters (e.g. abcd)
 - A sequential series of numbers (e.g. 1234) or pattern of numbers (e.g. 2468)
- Password must be unique for 2 years
- Passwords must be unique within the last 8 passwords

Temporal - Passwords on standard User accounts will expire every 90 days. Each new Password must meet the above parameters. You will be notified each time you login of the number of days remaining until your password expires.

Session Rules

Every time you log in to *AESDirect*, a timer is activated. This timer serves both as a session regulator and an activity counter. To improve security, User Accounts may only be inactive for a finite amount of time, whether for an individual session, or the accounts lifespan.

Account Inactivity

- Users will be deactivated if they have not logged in for 45 days
- E-mail warnings will be delivered to the User once a day after 40 days of inactivity. The E-Mail will remind of the need to change their password and direct them to the appropriate resources.

- Once deactivated, the Account Administrator or User Manager will need to reactivate the User

Session Timeout

- All *AESDirect* User sessions will time-out after 30 minutes of inactivity. A pop-up will notify a User 5 minutes before time-out.
- Actions, such as opening a window or moving from one page to another, will reset the 30 minute timer
- Once inactive for more than 30 minutes, the User will be forced to log in again. All data will be lost

Concurrent Sessions

- Each Username can be used for up to three simultaneous sessions. That is, a user can login to three different computers, or three different types of web browsers on one machine, at the same time.
- The fourth session attempt will fail. The attempt will be logged.

Lockout

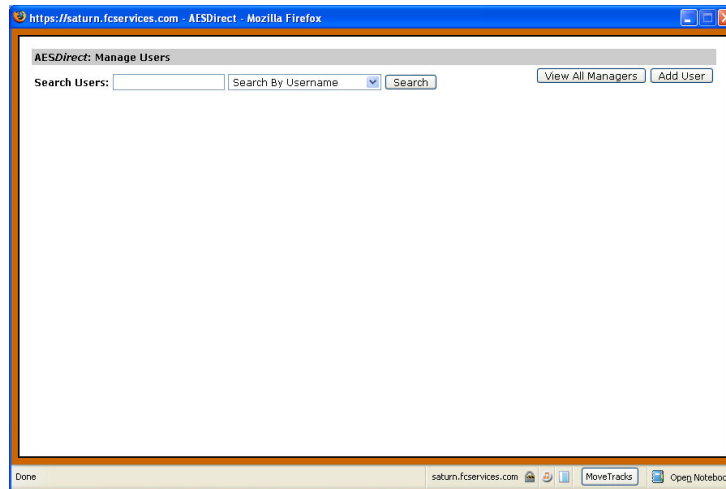
- Users are permitted 3 attempts to login to their account
- After 3 consecutive, invalid login attempts within 24 hours the user will be locked out
- Locked out User must be reactivated by the Account Administrator, only 15 minutes after the final failed login attempt

THE MANAGE USERS FUNCTIONS

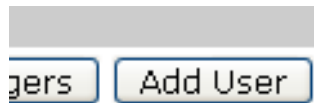
Very little has changed in *AESDirect* in terms of filing EEI. As a matter of fact, except for being granted their own Username and Password, most users will see no difference in the application itself. Account Administrators and Users Managers, however, will have access to the **Manage Users** screen and will see the link to those functions on the *AESDirect* interface.

To access the Manage User Functions...

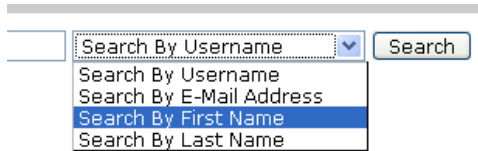
Under **Account Maintenance**, click ‘Manage Users’



From the *AESDirect: Manage Users* screen, you may add new Users as well as search for and modify existing Users.



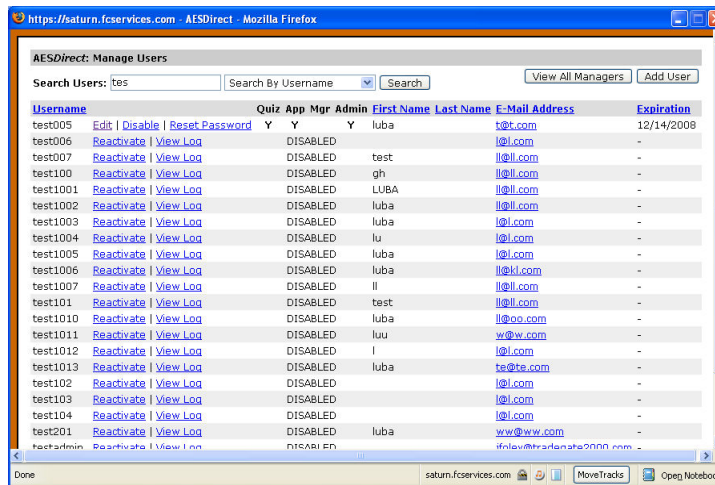
Click ‘Add User’ to create a new User. Creating a new User is as simple as filling in their information, choosing their permissions and then delivering their Username and Password.



Account Administrators can search for existing Users by a variety of criteria, including:

- Username
- E-Mail Address
- First Name
- Last Name

Enter at least the first character of the search criteria and click ‘Search’ to return a list of matches.



Easily identify the current status of each of your Users, including which permissions they have and whether they have been Disabled or Locked Out.

Sort your list of Users by simply clicking a highlighted column name, such as Username, First Name, Last Name and E-Mail Address.

HOW TO...

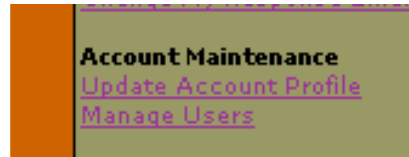
This section will help guide you through the step-by-step process of completing each administrative task in *AESDirect*.

Create a New User

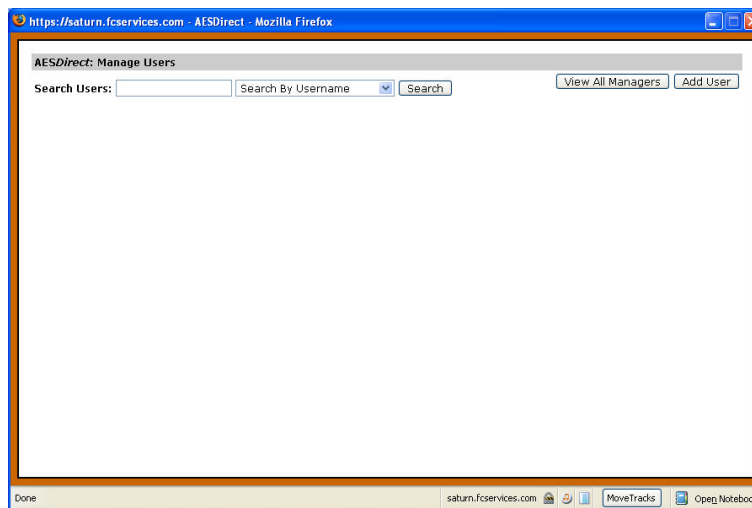
Users are the backbone of the *AESDirect* filing experience. Anyone who accesses *AESDirect* is a User. Users access the system with a Username and a Password to perform the tasks to which they are assigned. Usernames must be 3-25 characters in length. Passwords for Users expire every 90 days.

To create a New User...

- 1) Login to *AESDirect*



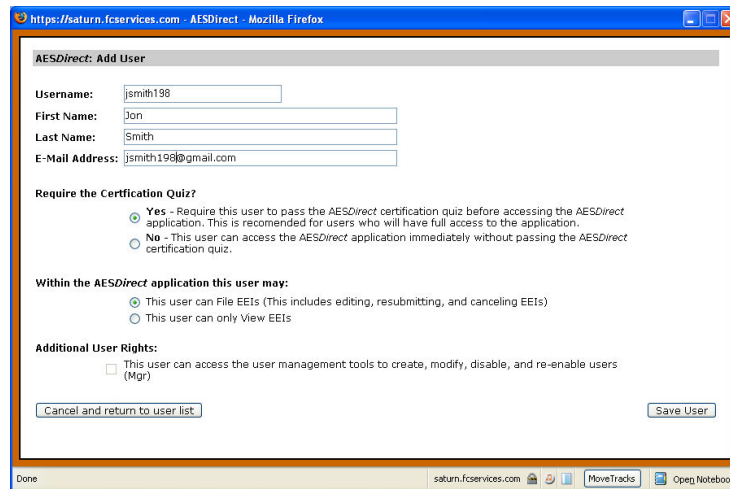
- 2) Under **Account Maintenance**, Click 'Manage Users'



- 3) The **AESDirect: Manage Users** screen will open

A rectangular button with rounded corners and a light blue gradient, containing the text "Add User" in a dark blue font.

4) Click the 'Add User' button

A screenshot of a web browser window titled "AESDirect: Add User". The browser address bar shows "https://saturn.fcservices.com - AESDirect - Mozilla Firefox". The form contains the following fields: "Username" (jsmith198), "First Name" (Don), "Last Name" (Smith), and "E-Mail Address" (jsmith198@gmail.com). Below the fields are three sections of radio button options: "Require the Certification Quiz?" (Yes selected), "Within the AESDirect application this user may:" (File EETs selected), and "Additional User Rights:" (unchecked). At the bottom are "Cancel and return to user list" and "Save User" buttons. The browser status bar at the bottom shows "Done" and "saturn.fcservices.com".

The **AESDirect: Add User** screen will open

5) Enter a Username

The Username must be unique to *AESDirect*. If the Username already exists, you will be notified and given a chance to choose another Username.

6) Enter the User's First Name

7) Enter the User's Last Name

8) Enter the User's E-Mail Address

9) Under **Require the Certification Quiz?**

- a) Choose 'Yes' if you want to require the User to take and pass the *AESDirect* certification quiz before accessing the *AESDirect* application. This is recommended for Users who will have full access to the application.
- b) Choose 'No' if you do NOT want to require the user to take and pass the *AESDirect* certification quiz before accessing the *AESDirect* application.

10) Under **Within the AESDirect application this user may:**

- a) Choose 'File EEI' which will give them permission to Create, File and Edit EEI
- b) 'Only View EEI' which will give the User Read Only access to EEI created by others

11) Under **Additional User Rights:**

- a) Click the (Mgr) checkbox to allow the User access to user management tools to create, modify, disable, and re-enable users

Note: Each AESDirect account is only allowed two (2) User Managers. If this checkbox has been grayed out, you have already selected two User Managers. If you have questions about the number of User Managers, please contact AESDirect Technical Support.

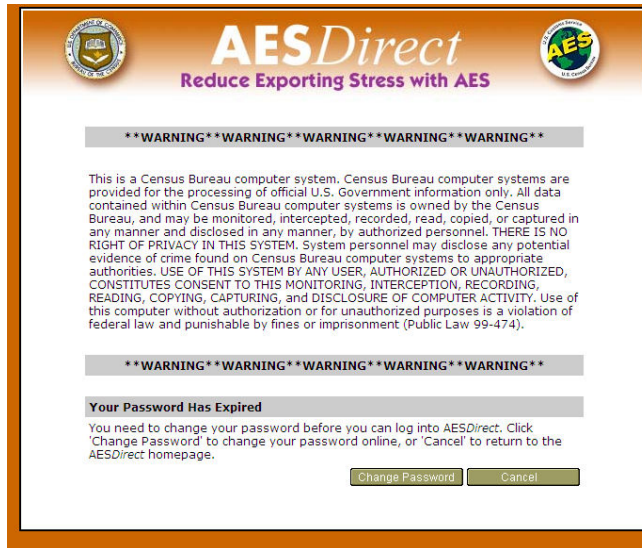
Save User

12) Click 'Save User'

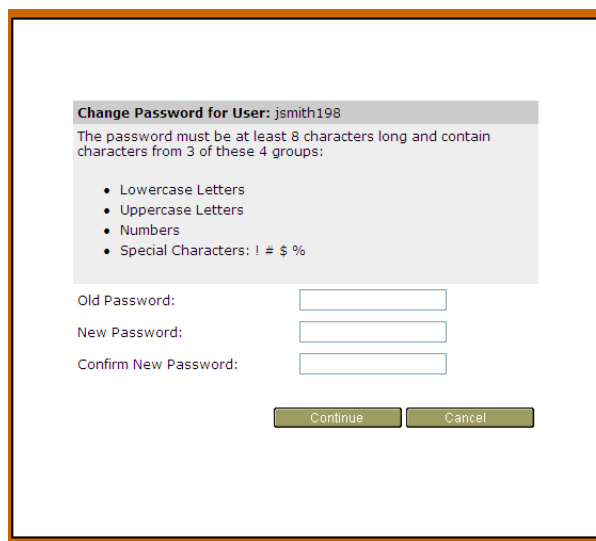


If all is successful, you will be brought to the User Created screen. The Username will be displayed and a temporary password assigned

13) Provide this information to the User



When the User first logs in to their account, they will be forced to change their password



All passwords must be at least 8 characters long and contain characters from 3 of these 4 groups:

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

See **Password Rules** for all password parameters.

Once they have successfully updated their password, the User will have access to the *AESDirect* functions you have granted.

Create a User Manager

The role of a User Manager is very similar to that of the Account Administrator. A User Manager can serve as a point of contact for Users, and help them:

- Establish *AESDirect* Users
- Make changes to their user accounts
- Help users reset their passwords or reactivate disabled accounts.

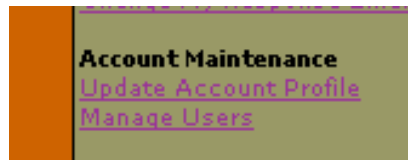
A User Manager is an *AESDirect* expert.

The only thing a User Manager cannot do is act, legally, on behalf of the Account holder when contacting *AESDirect* to do such things as Reactivate a Locked Out *AESDirect* Account.

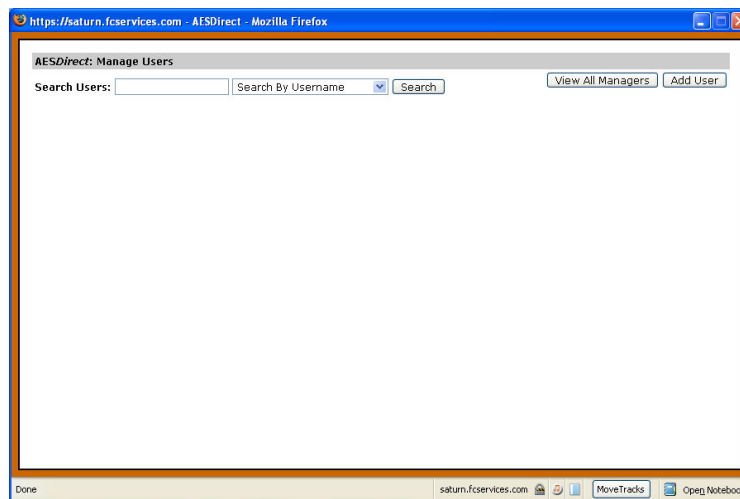
A User Manager can be a new or existing User. Your Company Account is limited, however, to only two (2) User Managers. Both the Account Administrator and a User Manager can create a User Manager.

To create a User Manager...

- 1) Login to *AESDirect*

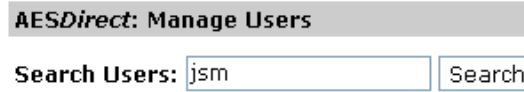


- 2) Under **Account Maintenance**, Click 'Manage Users'

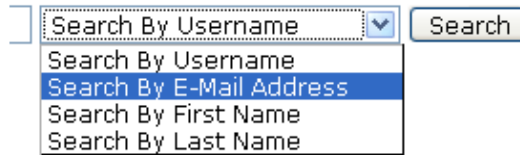


The **AESDirect: Manage Users** screen will open

- 3) Either follow the instructions to Create a New User and give that User Manager Permissions
or
- 4) Search for an existing User



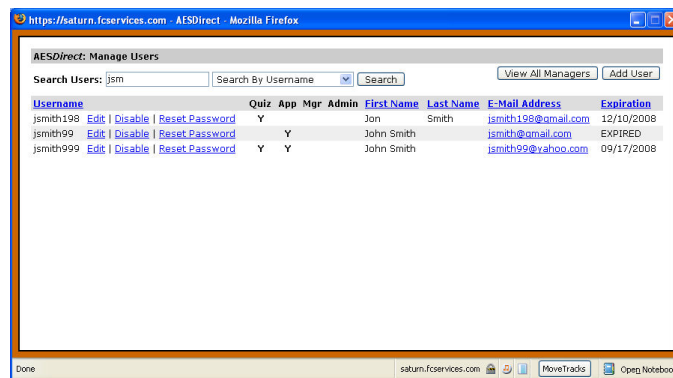
- a) Enter at least one character of a search string



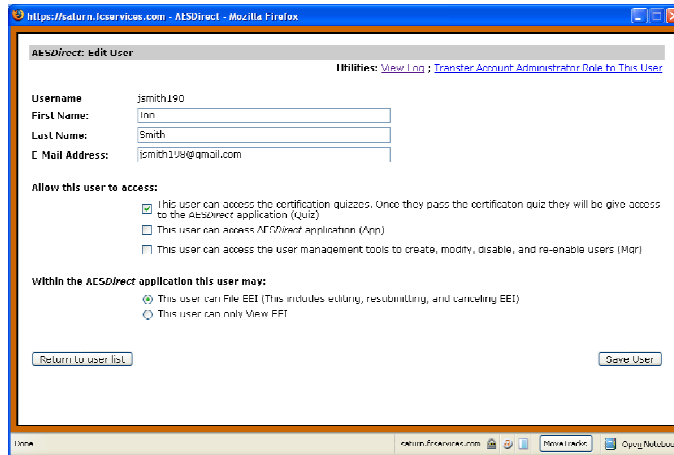
- b) Choose how you will 'Search by...'

 - Username
 - E-Mail Address
 - First Name
 - Last Name

- c) Click 'Search'
- d) A list of matches will be returned



- 5) Click 'Edit' next to the Username you would like to Modify



The **AESDirect: Edit User** screen will open

6) Click the (Mgr) checkbox

Note: Each AESDirect account is only allowed two (2) User Managers. If this checkbox has been grayed out, you have already selected two User Managers. If you have questions about the number of User Managers, please contact AESDirect Technical Support.

7) Click 'Save User'

	Quiz	App	Mgr
word	Y	Y	Y
word	Y	Y	
word	Y		

The screen will refresh and the Username will be displayed. Under 'Mgr' you should see a 'Y' indicating that the User is now a User Manager.

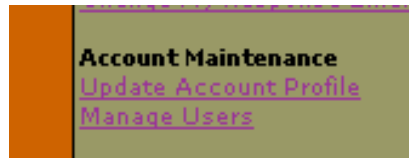
The next time the User logs in to their account, they will see the Account Maintenance section.

Reset Passwords

All Users forget their passwords. As an Account Administrator or a User Manager, it is your responsibility to reset these passwords. Resetting a Password is simple.

To reset a User's Password:

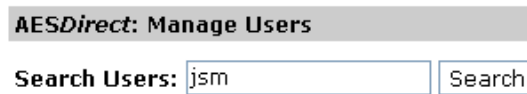
- 1) Login to *AESDirect*



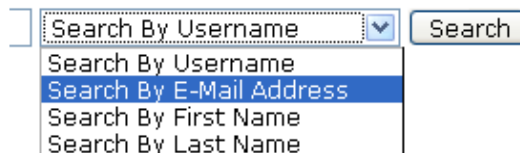
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



- a) Enter at least the first character of a search string



- b) Choose how you will 'Search by...'

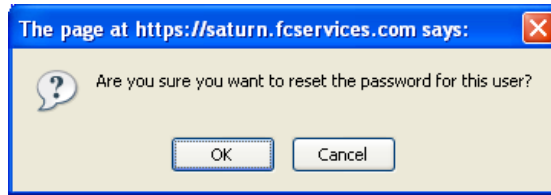
- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

<u>Username</u>	<u>Qu</u>
jsmith198 Edit Disable Reset Password	1
jsmith99 Edit Disable Reset Password	1
jsmith999 Edit Disable Reset Password	1

A list of matches will be returned

4) Click 'Reset Password' next to the Username you would like to update



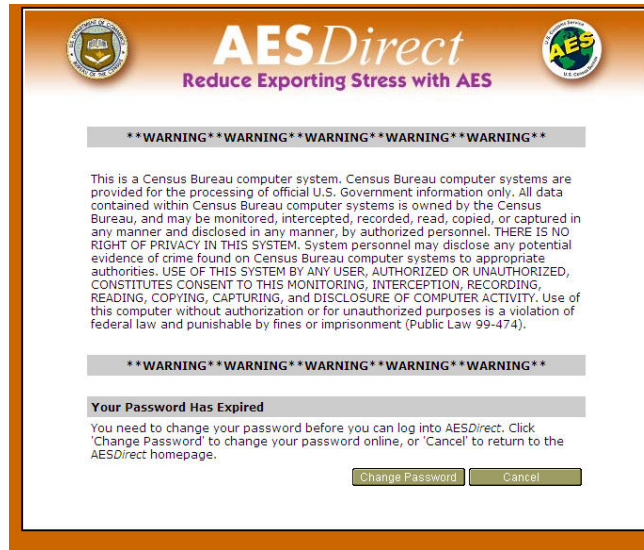
A box will open and ask you to confirm that you would like to reset the User's password

5) Click 'OK'

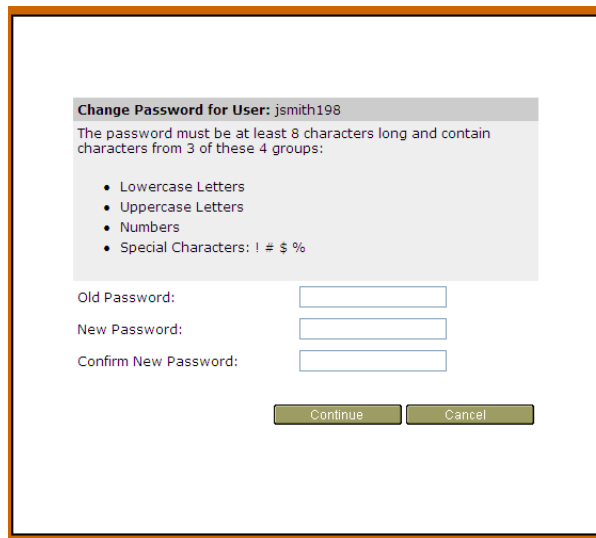


A new window will open. The password will be reset and a new temporary password displayed

6) Deliver this password directly to the User.



7) When the User attempts to login, they will be forced to change their password



All passwords should be least 8 characters long and contain characters from 3 of these 4 groups

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

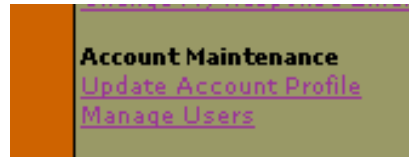
See **Password Rules** for all password parameters.

Disable a User

When a User is no longer responsible for filing in *AESDirect* or leaves your company, you should disable their Username. Disabled Users are not removed from *AESDirect* permanently, nor are their EEI. You may reactivate a disabled User at any time.

To disable a User Account

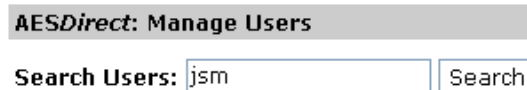
- 1) Login to *AESDirect*



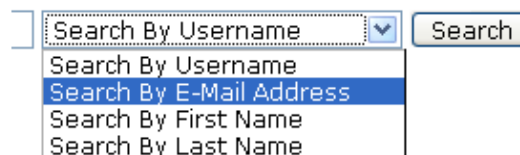
- 2) Under **Account Maintenance** click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



- a) Enter at least one character of a search string



- b) Choose how you will 'Search by...'

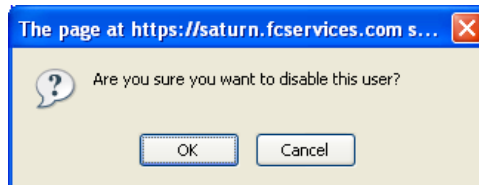
- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

Username			
jsmith198	Edit	Disable	Res
jsmith99	Edit	Disable	Res

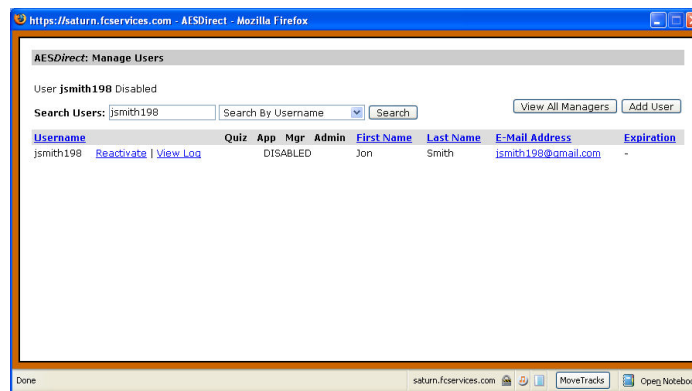
A list of matches will be returned.

4) Click 'Disable' next to the Username you would like disabled



A window will open and ask you to confirm

5) Click 'OK'



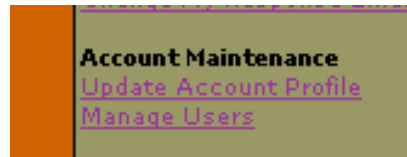
DISABLED will appear where a Username's permissions are normally indicated.

Reactivate a Disabled User

Users can be disabled for a number of reasons. If they have left the company, Account Administrators should disable them. Also, if a User has been in-active for more than 120 days, the User will be disabled. When a User is disabled, the User still exists in *AESDirect* and they can be reactivated at any time.

To reactivate a disabled User

- 1) Login to *AESDirect*



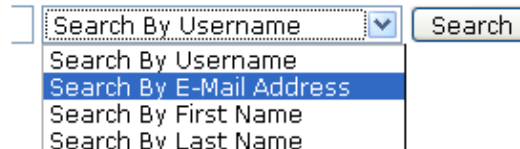
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



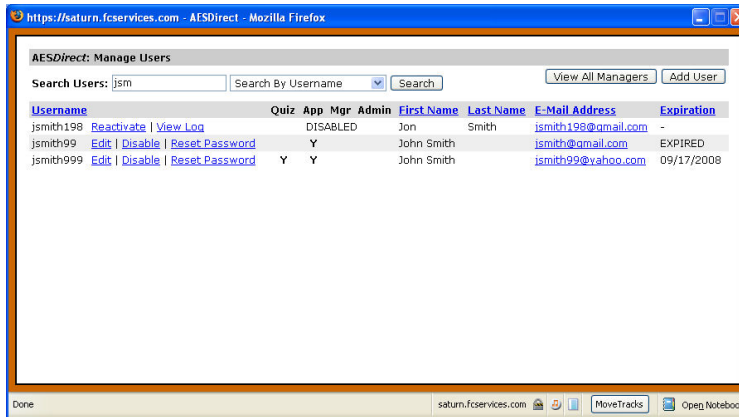
- a) Enter at least one character of a search string



- b) Choose how you will 'Search by...'

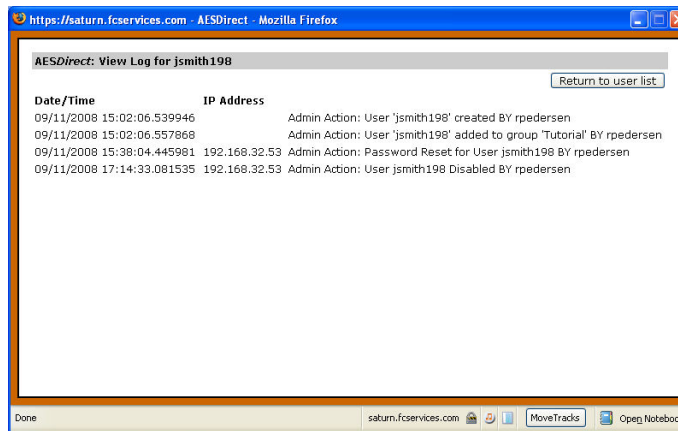
- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'



A list of matches will be returned. **DISABLED** will appear where a Username's permissions are indicated.

If you do not know why the account is disabled click 'View Log'

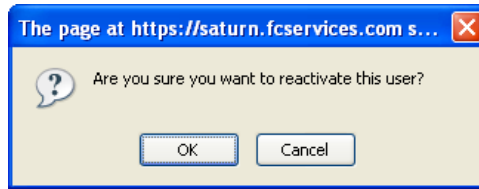


View Log allows you to review the attempts the User or any other individual made to gain access to the account.

Click 'Return to user list'

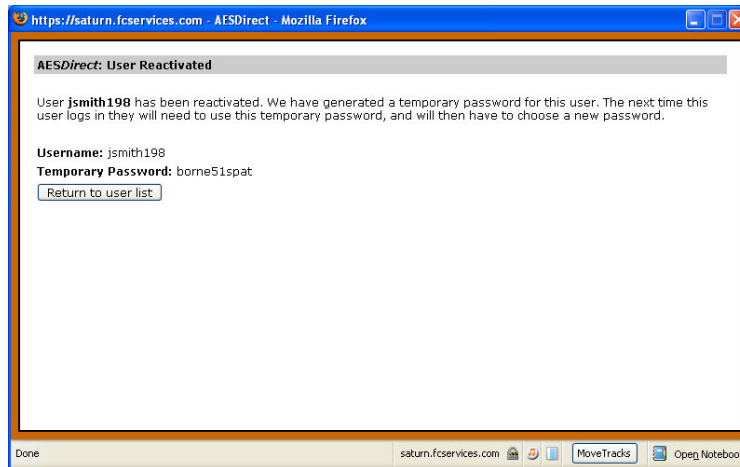


4) Click 'Reactivate'



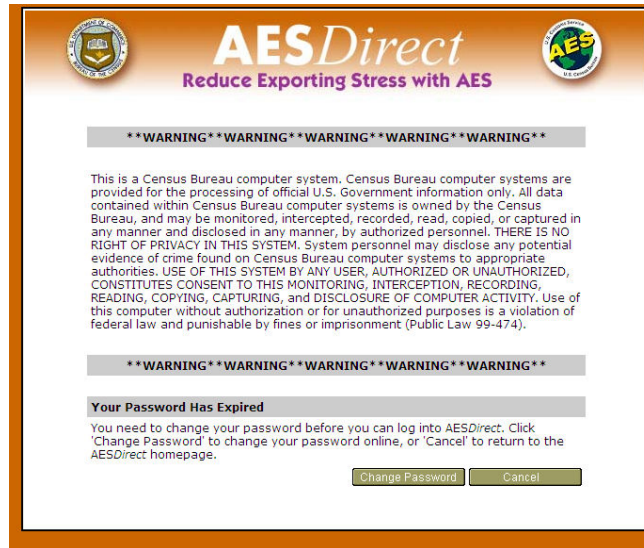
A window will open and ask you to confirm

5) Click 'OK'

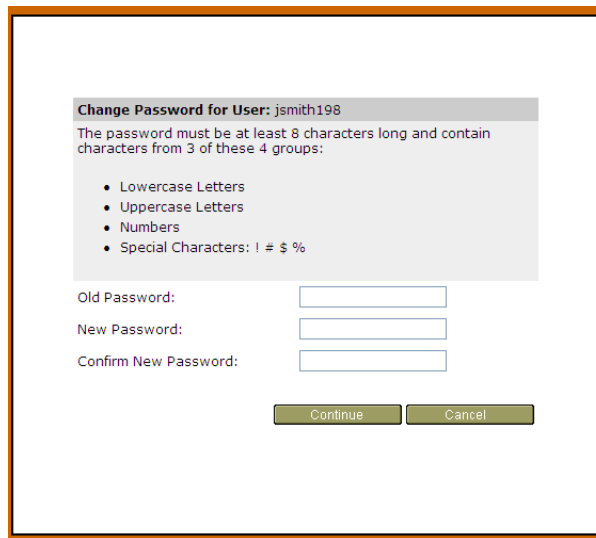


A new window will open. The Username will be reactivated and a new temporary password will be displayed

6) Deliver this password directly to the User.



7) When the User attempts to login, they will be forced to change their password



All passwords must be at least 8 characters long and contain characters from 3 of these 4 groups

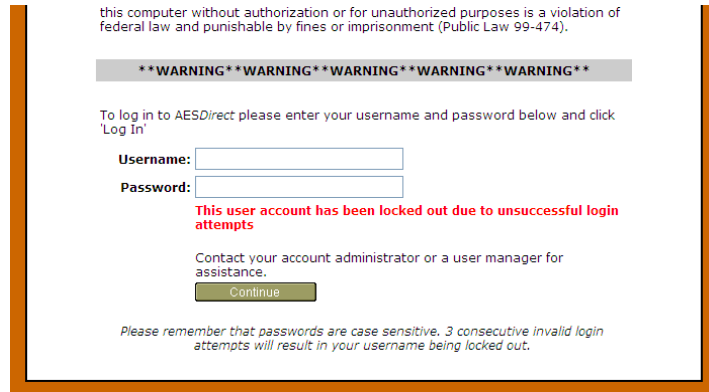
- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

See **Password Rules** for all password parameters.

Reactivate a Locked Out Account

Users who attempt to log in to *AESDirect* with their Username but make three consecutive invalid attempts within 24 hours will, as a security precaution, be locked out.



This computer without authorization or for unauthorized purposes is a violation of federal law and punishable by fines or imprisonment (Public Law 99-474).

****WARNING**WARNING**WARNING**WARNING**WARNING****

To log in to *AESDirect* please enter your username and password below and click 'Log In'

Username:

Password:

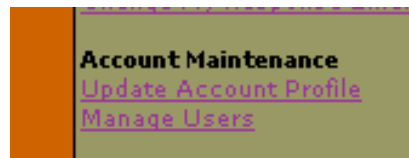
This user account has been locked out due to unsuccessful login attempts

Contact your account administrator or a user manager for assistance.

Please remember that passwords are case sensitive. 3 consecutive invalid login attempts will result in your username being locked out.

It is the responsibility of the Account Administrator or the User Manager to reactivate Locked Out accounts. Usernames can only be unlocked following a 15 minute 'time out.'

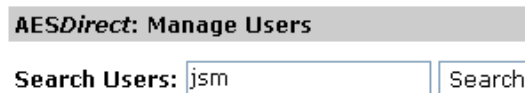
- 1) Login to *AESDirect*



- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



AESDirect: Manage Users

Search Users:

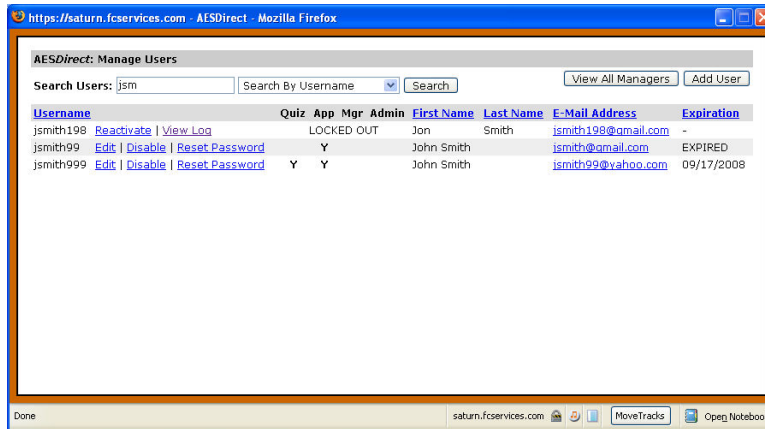
- a) Enter at least one character of a search string



b) Choose how you will 'Search by...'

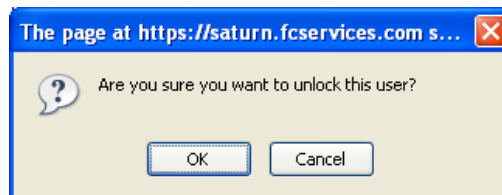
- Username
- E-Mail Address
- First Name
- Last Name

c) Click 'Search'



A list of matches will be returned. **Locked Out** will appear where a Username's permissions are indicated.

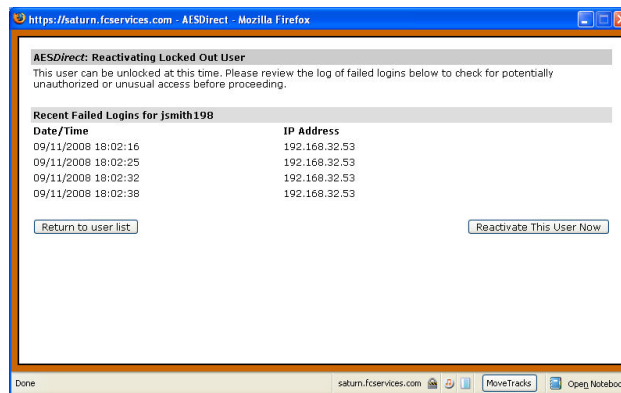
4) Click 'Reactivate'



A window will open and ask you to confirm

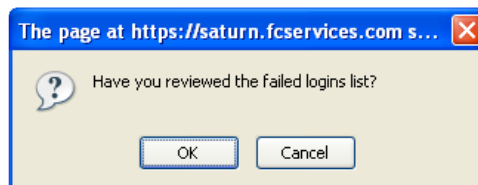
5) Click 'OK'

The **AESDirect: Reactivating Locked Out User** screen will open and display all recent attempts to login. You will only be able to reactivate this User if it has been 15 minutes since the last failed attempt.



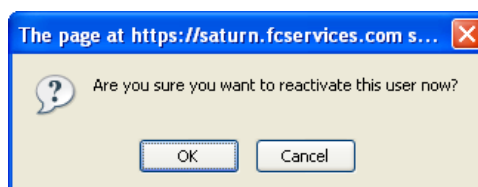
View Log allows you to review the number of attempts the User or any other individual made to try to gain access to the account. If the number of attempts is significantly more than the three that would lock the account, your account may be subject to a malicious attack. If you suspect you are the victim of an attack, contact **AESDirect** Technical Support immediately.

- 6) Review the log in attempts again to identify any abnormalities
- 7) If all seems right, click 'Reactivate This User Now'



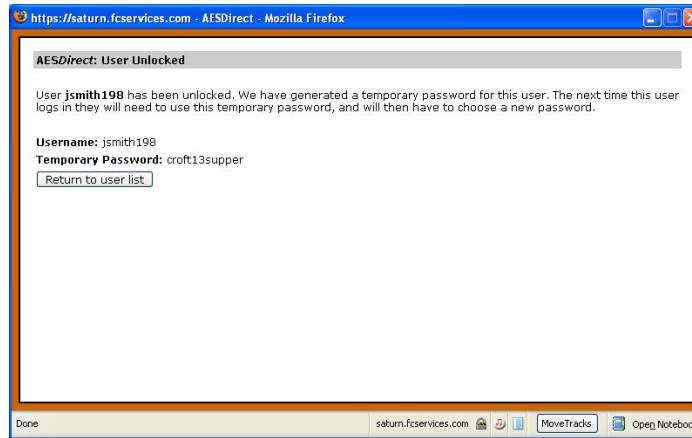
A window will open and ask you to confirm you have reviewed the failed Logins list

- 8) Click 'OK'



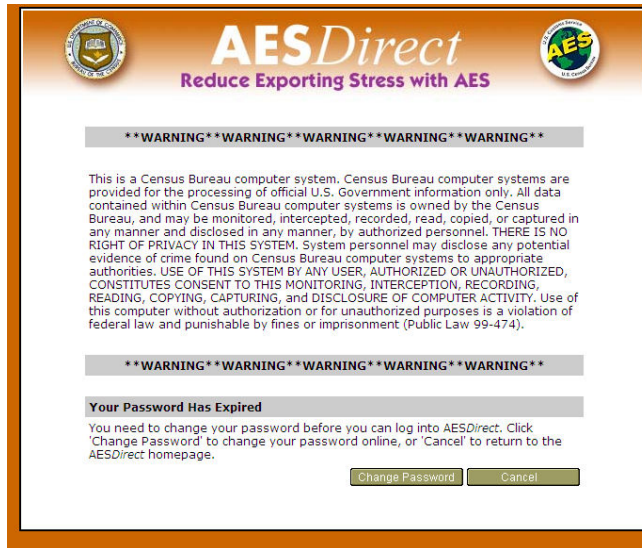
Another window will open and ask if you are sure you would like to reactivate the User.

- 9) Click 'OK'

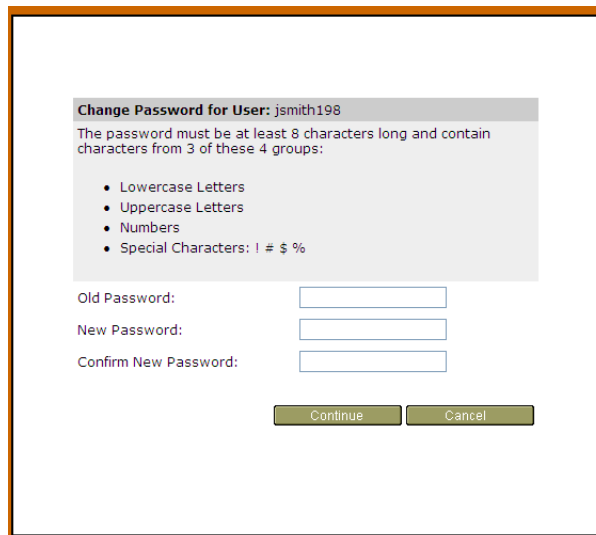


A new window will open. The password will be reset and a new temporary password displayed

10) Deliver this password directly to the User.



11) When the User next logs in to their account, they will be forced to change their password



All passwords at least 8 characters long and contain characters from 3 of these 4 groups

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

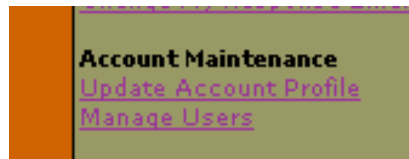
See **Password Rules** for all password parameters.

Change an Account Administrator

As with all Users, when the Account Administrator leaves, their account will need to be disabled. Unlike Users or User Managers, additional steps must be taken to identify a new Account Administrator in *AESDirect*, as they are the individual directly responsible for *AESDirect* maintenance.

To Change an Account Administrator...

- 1) Login to *AESDirect*



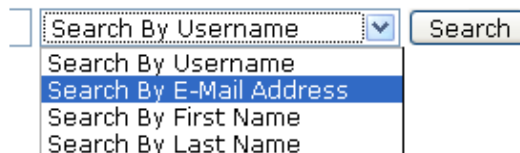
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



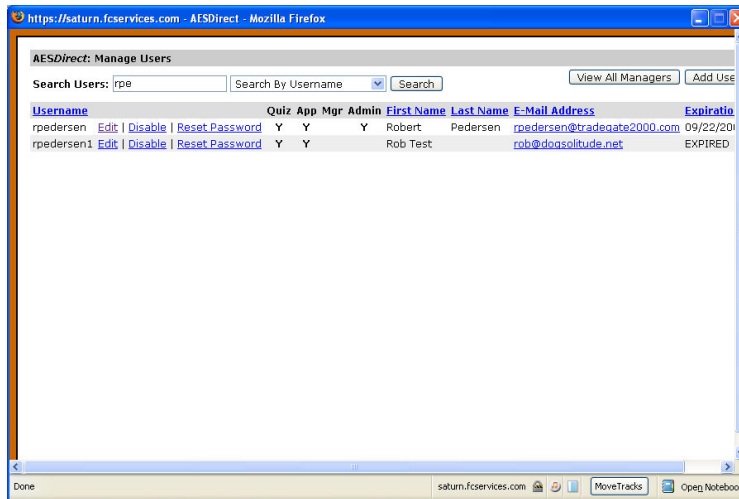
- a) Enter at least one character of a search string



- b) Choose how you will 'Search by...'

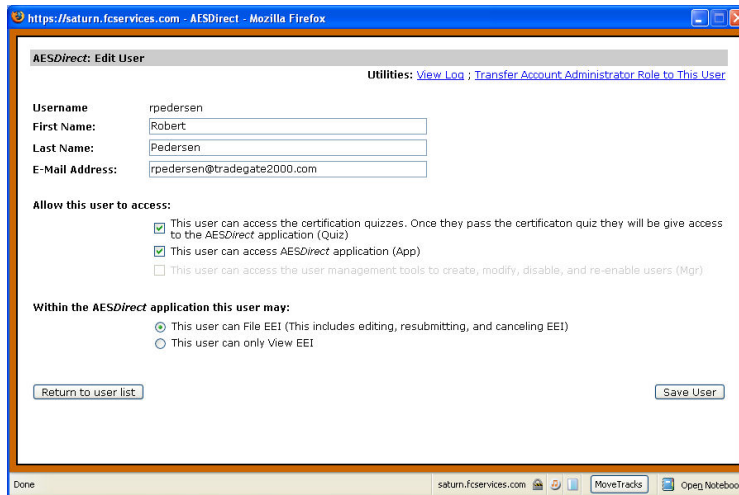
- Username
- E-Mail Address
- First Name
- Last Name

c) Click 'Search'

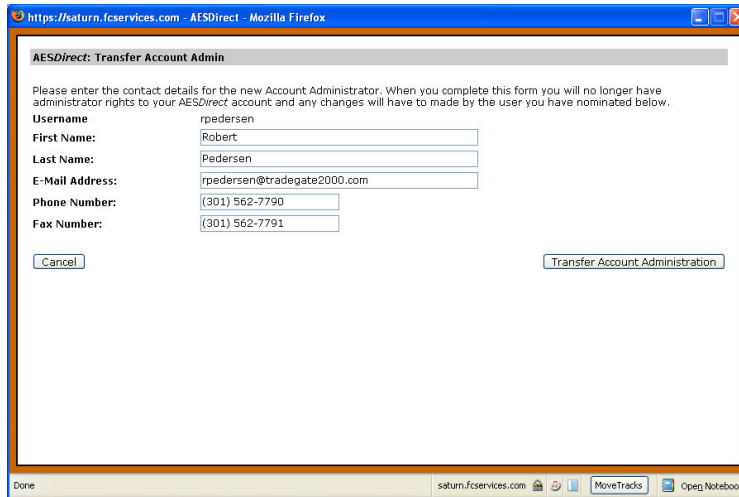


A list of matches will be returned.

4) Click 'Edit' next to the User you would like to make the Account Administrator



5) Click 'Transfer Account Administrator Role to This User'



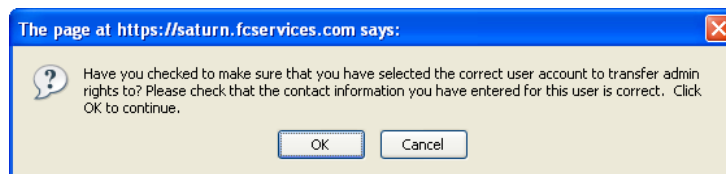
The **AESDirect: Transfer Account Admin** window will open.

- 6) Complete any profile information that may be missing. All fields must be completed.
- 7) Click 'Transfer Account Administration'



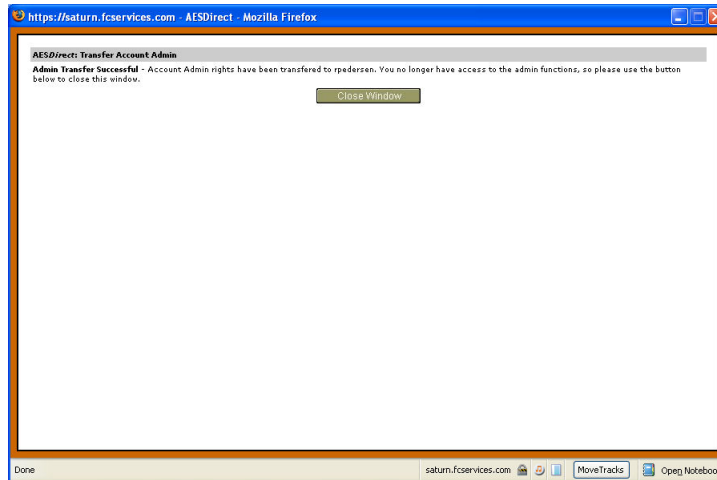
You will be asked to confirm the change of Account Administrator a first time

- 8) Click 'OK'



You will be asked to confirm the change of Account Administrator for a second time

- 9) Click 'OK'



You will see **Admin Transfer Successful** if there are no problems. Account Administrator privileges will transfer to the User selected. You will no longer be an Account Administrator.

10) Check on the Status of your changes.



11) Under **Account Maintenance**, click 'Update Account Profile'

Administrator	
Name	Robert Pedersen
Email	rpedersen@tradegate2000.com
Phone	(301) 562-7790
Fax	(301) 562-7791

The new Account Administrator contact information should be listed

WHAT HAPPENS IF ACCOUNT ADMINISTRATOR LEAVES?

If the User designated as an Account Administrator leaves the company and does not nominate a replacement Account Administrator before their password expires, there are manual steps you can take to have a new Account Administrator nominated. These steps are very similar to those outlined when an Activation Code was required to reset a password.

- 1) FAX a Letter Requesting the Change of Account Administrator

Fax # (301) 562-7795

This request must be on company letterhead from an authorized company officer (President, CEO, etc.) and signed by that company officer. The letter must specifically request that you wish to nominate a new Account Administrator as the one on file is no longer employed by the company.

Include the following:

- Company Name
 - Company ID Number (EIN, SSN, or DUNS)
 - *AESDirect* Username. Either
 - New Username you wish to be created; or
 - Existing Username
 - The new administrator information:
 - Name
 - Phone Number
 - Fax Number
 - E-Mail Address
 - Mailing Address
 - Signature & Title of the person requesting the change
- 2) Once we have received your fax, we will contact the new Account Administrator and provide a Username, if new, and a Password.
 - 3) The New Account Administrator must login. They will be forced to reset their password

All passwords at least 8 characters long and contain characters from 3 of these 4 groups

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

See **Password Rules** for all password parameters.

- 4) Under Account Maintenance, click 'Update Account Profile' to verify your information is correct.