AES*DIRECT*
ACCOUNT ADMINISTRATION USER GUIDE

Updated August 25, 2010

TABLE OF CONTENTS

Section	Page
OVERVIEW	**3**
AES*Direct* Roles Defined	**3**
AES*Direct* Rules	**5**
Username Rules	**5**
Password Rules	**5**
Session Rules	**6**
THE MANAGE USER FUNCTIONS	**8**
HOW TO	**11**
Create a New User	**11**
Create a User Manager	**16**
Reset Passwords	**20**
Disable a User	**24**
Reactivate a Disabled User	**26**
Reactivate a Locked Out User	**31**
Change an Account Administrator	**37**
WHAT HAPPENS IF THE ACCOUNT ADMINISTRATOR LEAVES?	**41**

OVERVIEW

AES*Direct* Roles Defined

Each AES*Direct* Account includes three distinct types of Users, each with their own role to play in filing and their own set of reponsibilities.

This Administrative Guide was created to help the Account Administrator and the User Manager understand fully their role in AES*Direct*. 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.

Account Administrator

The Account Administrator is responsible for the AES*Direct* account and should be a Customs Compliance specialists and a company officer.

An Account Administrator's responsibilities include:

Interacting with AES*Direct* - If there are changes to be made to your AES*Direct* Account which require interaction with AES*Direct* technical support, the Account Administrator must be the initiating party. The Account Administrator must be the signator on all documents requesting any substantial change to an account.

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 AES*Direct* Users.

Creating and Managing Users - The Account Administrator, as the first User in AES*Direct*, is responsible for creating Users, providing those Users a Password and managing their access to your AES*Direc Account*, by manually resetting passwords or disabling accounts, when necessary. The Account Administrator may delegate this responsibility to a User Manager.

User Managers

A User Manager is an AES*Direct* expert. A User Manager serves as a point of contact for those who wish to use a company's AES*Direct* account. A User Manager can do everything an Account Administrator can, such as create Users and manage their access. User Managers cannot act legally on behalf of the Account holder when contacting AES*Direct* or make any changes to the Account Profile.

Any new or existing User in your AES*Direct* Account can be a User Mananger. Your Account is limited, however, to only two (2) User Managers.

Users

Users hold the most fundamental role in AES*Direct*. They are responsible for the day-to-day filing of EEI. Users may also be limited to viewing historical filing data.

AESDIRECT RULES

Username Rules

Each User in AES*Direct* 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 AES*Direct* usernames must be unique across the AES*Direct* 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

AES*Direct* Password Rules are strictly enforced case, to maximize security. Common words and phrases are not acceptable.

Complex – All passwords must be at least 12 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 4 years

- Passwords must be unique within the last 24 passwords

Temporal - Passwords on standard User accounts will expire every 60 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.

Passwords cannot be changed more than once per day.

Session Rules

Every time you log in to AES*Direct*, 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.

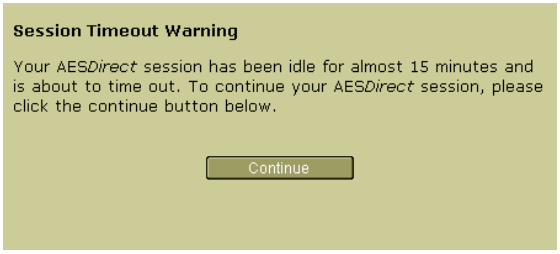
Account Inactivity

- Accounts will be deactivated if they have not been accessed by any Users in 30 days.
- Once deactivated, the Account Administrator will need to contact AESDirect Technical Support to have the Account reactivated.

User Inactivity

- Users will be deactivated if they have not logged in for 90 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



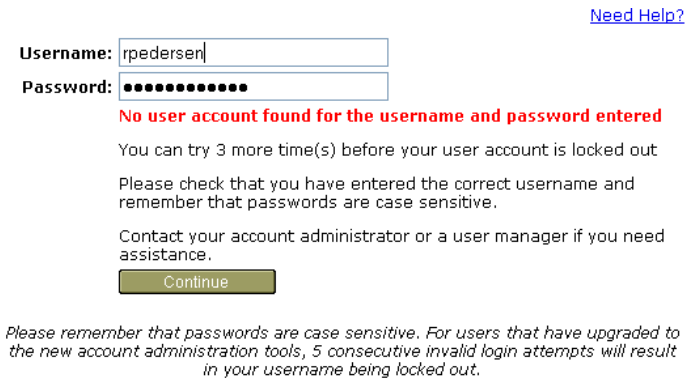
- All AES*Direct* User sessions will time-out after 15 minutes of inactivity.
  A pop-up will notify a User 5 minutes before time-out.
- Actions, such as opening a window or moving from one page to another, will reset the 30 minute timer

- Once inactive for more than 15 minutes, the User will be forced to log in again. All data that was not saved before the timeout will be lost

Concurrent Sessions

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

Lockout

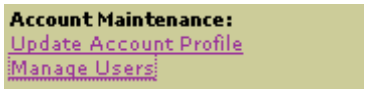


- After 5 consecutive, invalid login attempts within 15 minutes the user will be locked out
- The locked out User can only be reactivated by the Account Administrator and only 15 minutes after the final failed login attempt

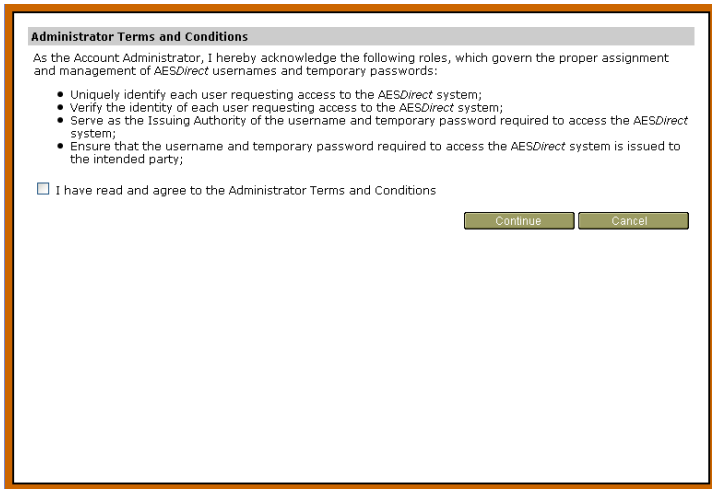
THE MANAGE USERS FUNCTIONS

Account Administrators and Users Managers have access to the **Manage Users** screen and will see the link to those functions on the AES*Direct* interface.

To access the Manage User Functions…



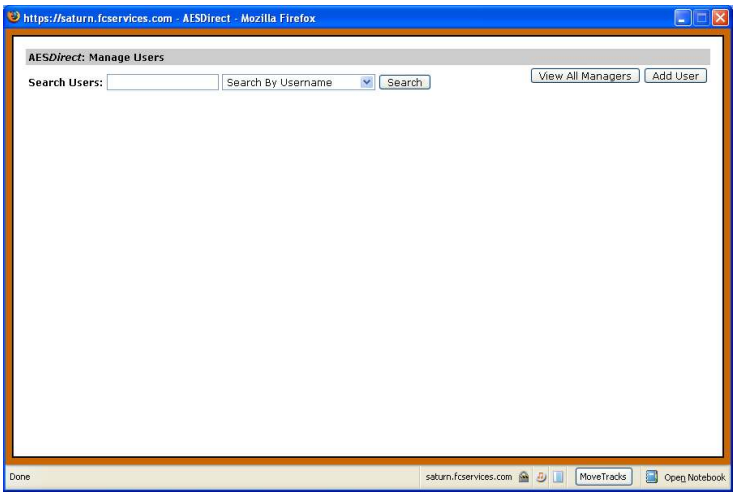
Under **Account Maintenance**, click 'Manage Users'



If this is the first time you are accessing these functions, you will be asked to confirm the **Administrator Terms and Conditions.**

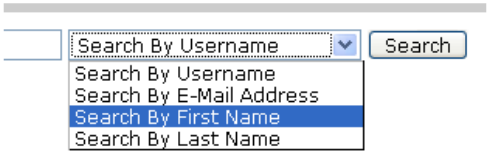
Check the box to acknowledge you have read and unders stood the Administrator Terms and Conditions.

Click 'Continue.'



You will be brought to the **AES*Direct*: Manage Users** screen. From the **AES*Direct*: Manage Users** screen, you may add new Users as well as search for and modify existing Users.

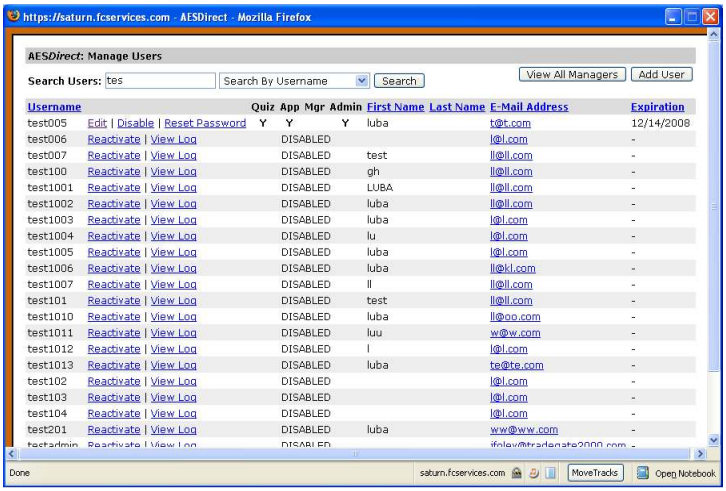
Click 'Add User' to create a new User. Creating a User is as straight forward as filling in their information, choosing their permissions and then delivering their Username and Password.



Account Administrators can search for existing Users by one of these criteria:

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

Enter at least the first character of the search term and click 'Search' to return a list of matches.



Username		Quiz	App	Mgr	Admin	First Name	Last Name	E-Mail Address	Expiration
test005	Edit | Disable | Reset Password	Y	Y		Y	luba		t@t.com	12/14/2008
test006	Reactivate | View Log		DISABLED					l@l.com	-
test007	Reactivate | View Log		DISABLED			test		ll@ll.com	-
test100	Reactivate | View Log		DISABLED			gh		ll@ll.com	-
test1001	Reactivate | View Log		DISABLED			LUBA		ll@ll.com	-
test1002	Reactivate | View Log		DISABLED			luba		ll@ll.com	-
test1003	Reactivate | View Log		DISABLED			luba		l@l.com	-
test1004	Reactivate | View Log		DISABLED			lu		l@l.com	-
test1005	Reactivate | View Log		DISABLED			luba		l@l.com	-
test1006	Reactivate | View Log		DISABLED			luba		ll@kl.com	-
test1007	Reactivate | View Log		DISABLED			ll		ll@ll.com	-
test101	Reactivate | View Log		DISABLED			test		ll@ll.com	-
test1010	Reactivate | View Log		DISABLED			luba		ll@oo.com	-
test1011	Reactivate | View Log		DISABLED			luu		w@w.com	-
test1012	Reactivate | View Log		DISABLED			l		l@l.com	-
test1013	Reactivate | View Log		DISABLED			luba		te@te.com	-
test102	Reactivate | View Log		DISABLED					l@l.com	-
test103	Reactivate | View Log		DISABLED					l@l.com	-
test104	Reactivate | View Log		DISABLED					l@l.com	-
test201	Reactivate | View Log		DISABLED			luba		ww@ww.com	-

Easily identify the current status of User, including their permissions or if they have been Disabled or Locked Out.

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

HOW TO…

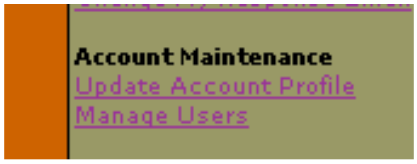
This section will help guide you through the step-by-step process of completing each administrative task in AES*Direct*.

Create a New User

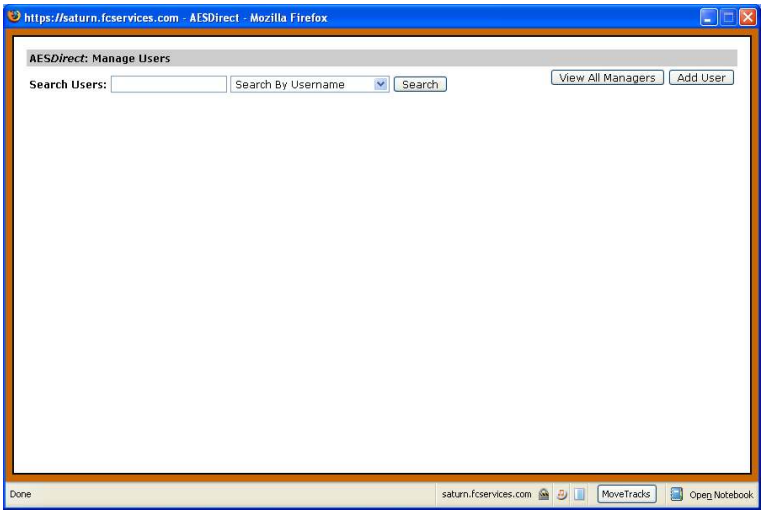
Users are the backbone of the AES*Direct* filing experience. Anyone who accesses AES*Direct* is a User. Users access the system with a Username and a Password to perform the tasks to which they are assigned. Usernames must be 3-25 characters in length. Passwords for Users expire every 90 days.

To create a New User…

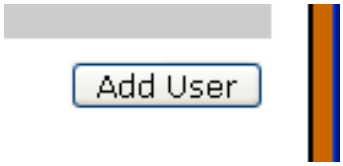
1) Login to AES*Direct*



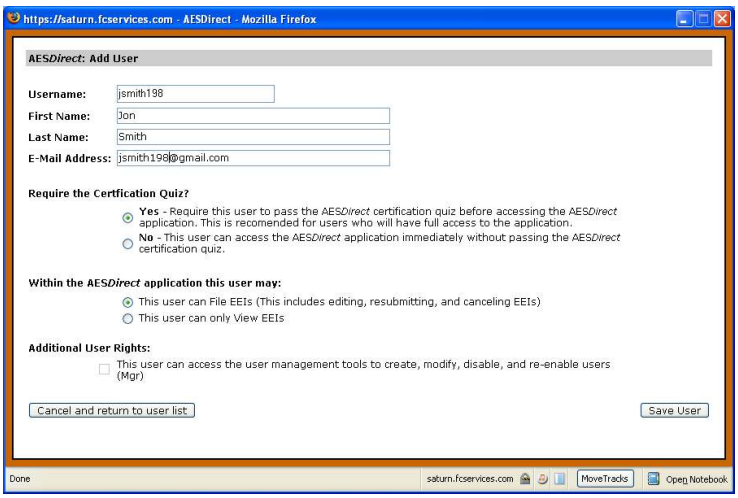
2) Under **Account Maintenance**, Click 'Manage Users'



3) The **AES*Direct*: Manage Users** screen will open



4) Click the 'Add User' button



The **AES*Direct*: Add User** screen will open

5) Enter a Username

The Username must be unique to AES*Direct*. 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 AES*Direct* certification quiz before accessing the AES*Direct* application. This is highly.

   b) Choose 'No' if you do NOT want to require the user to take and pass the AES*Direct* certification quiz before accessing the AES*Direct* application.

10) Under **Within the AES*Direct* 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:**

Additional User Rights:

☐ This user can access the user management tools to create, modify, disable, and re-enable users (Mgr)

a) Click the (Mgr) checkbox to give the User access to User Management tools. This will make the User a User Manager, with the ability to create, modify, disable, and re-enable Users

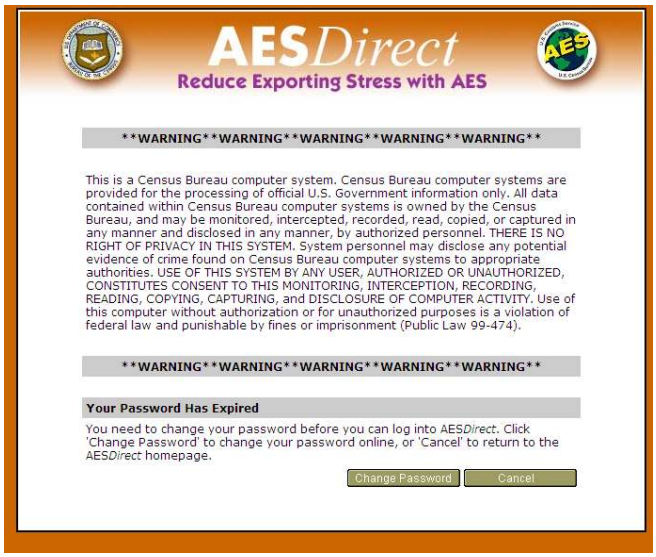
> **Note:** Each AESDirect account is only allowed two (2) User Managers. If this checkbox is grayed out, you have already selected two User Managers. Questions about the number of User Managers you may create should be directed to AESDirect Technical Support.

Save User

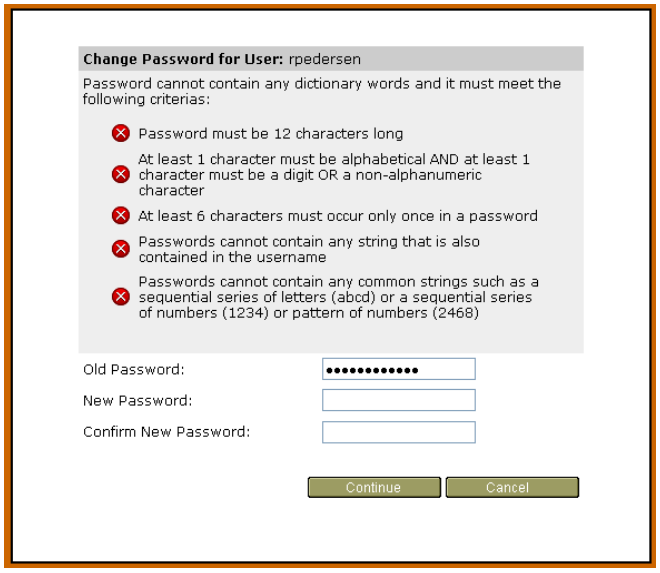
12) Click 'Save User'

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 by email or, preferably, telephone.



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

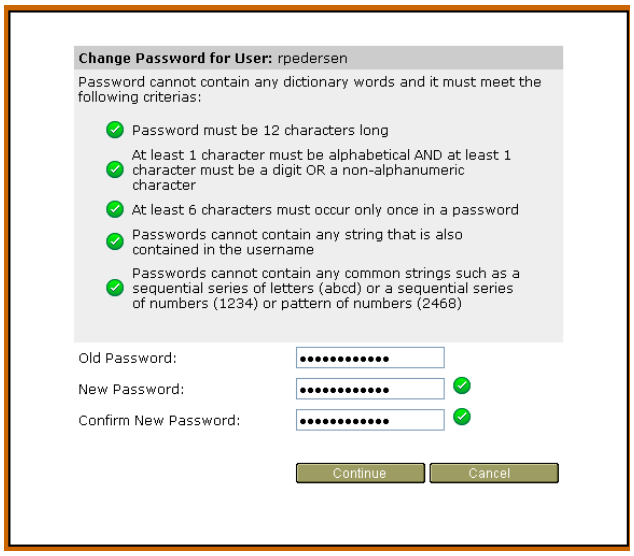


All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

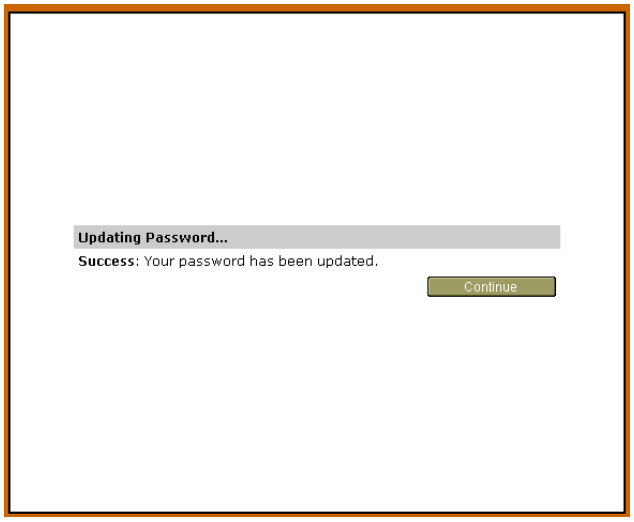
- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # $ %

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

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



AESDirect will validate the password as the User creates it.



Once the Users has successfully updated their password, that User will have access to the AES*Direct* functions you have granted to them.

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:

- Establish new AES*Direct* Users
- Make changes to existing Users
- Reset passwords or reactivate disabled Users

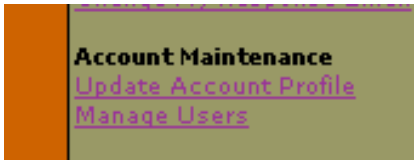
A User Manager is an AES*Direct* expert.

The only thing a User Manager may not do is act legally on behalf of the Account holder when contacting AESDirect. For instance, only an Account Administrator may contact AESDirect to reactivate a locked out Account.

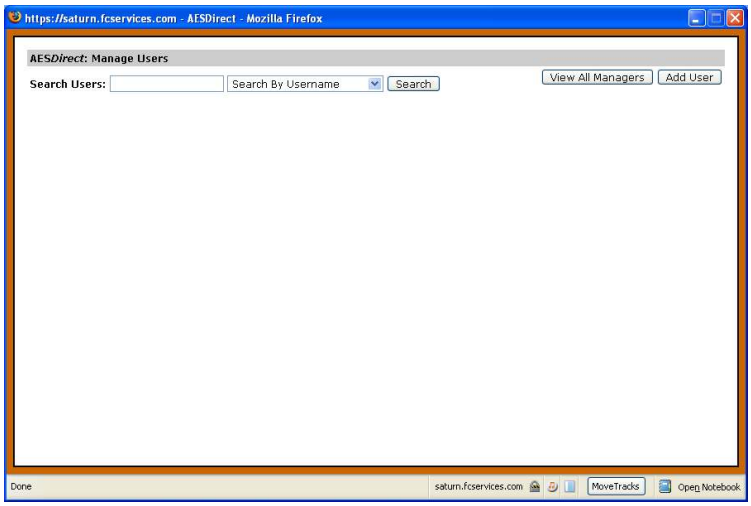
A User Manager can be a new or existing User. Your Company Account is limited, however, to only two (2) User Managers. Both the Account Administrator and a User Manager can create a User Manager.

To create a User Manager...

1) Login to AES*Direct*

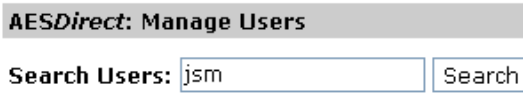


2) Under **Account Maintenance**, Click 'Manage Users'



The **AES*Direct*: Manage Users** screen will open

3) Either follow the instructions to Create a New User and give that User Manager Permission or search for an existing User



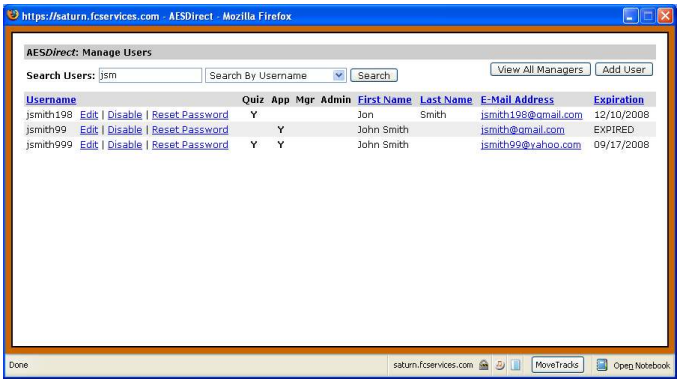
a) Enter at least one character of a search string

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

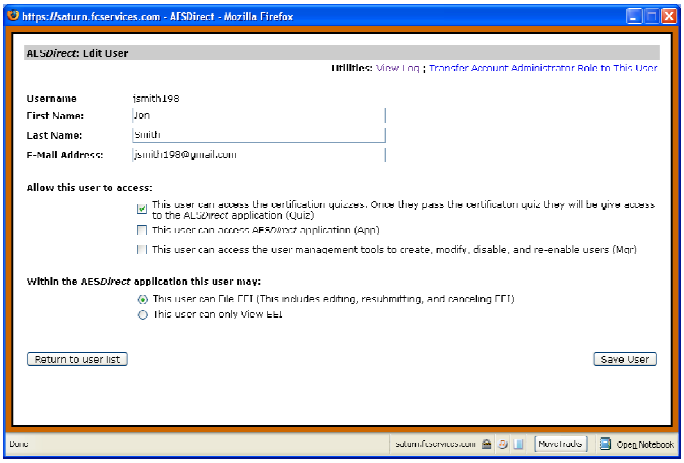
- Username
- E-Mail Address
- First Name
- Last Name

c) Click 'Search'

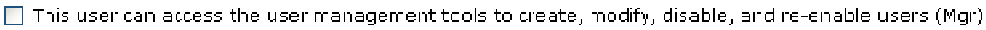
A list of matches will be returned



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



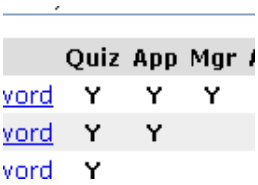
The **AES*Direct*: Edit User** screen will open



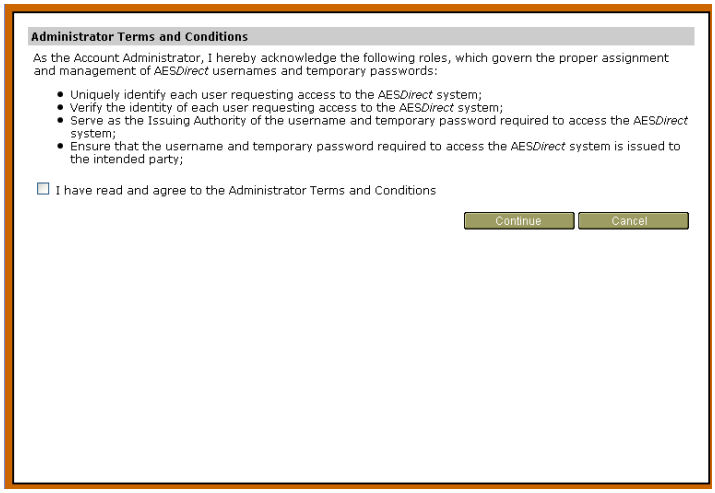
5) Click the (Mgr) checkbox

> **Note:** Each AESDirect account is only allowed two (2) User Managers. If this checkbox is grayed out, you have already selected two User Managers. Questions about the number of User Managers you may create should be directed to AESDirect Technical Support.

6) Click 'Save User'



The screen will refresh. Next to the Username a 'Y' should appear in the **Mgr** column. The User is now a User Manager.



When the new User Manager accesses the Account Maintenance functions the first time, they will be asked to confirm the **Terms and Conditions**.

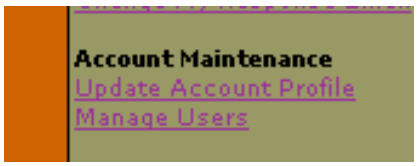
The must Check the box to acknowledge that they have read and understand the Administrator Terms and Conditions, or they will nto be able to access these functions.

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:

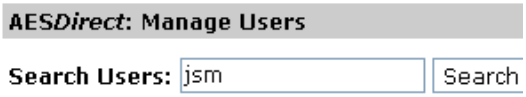
1) Login to AES*Direct*



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

The **AES*Direct*: 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

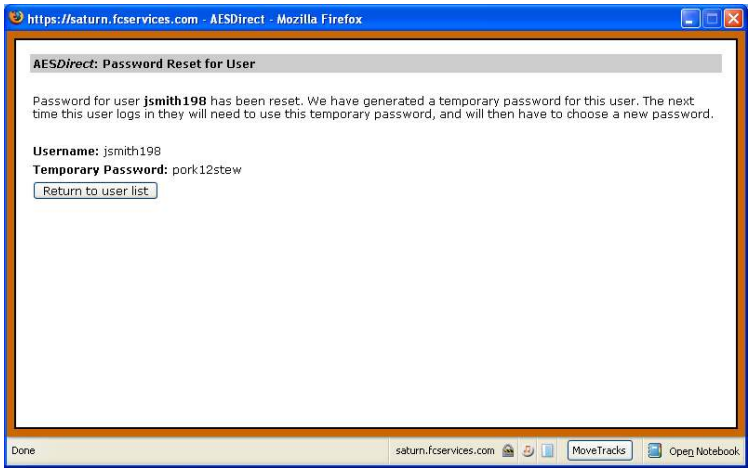
c) Click 'Search'

A list of matches will be returned

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

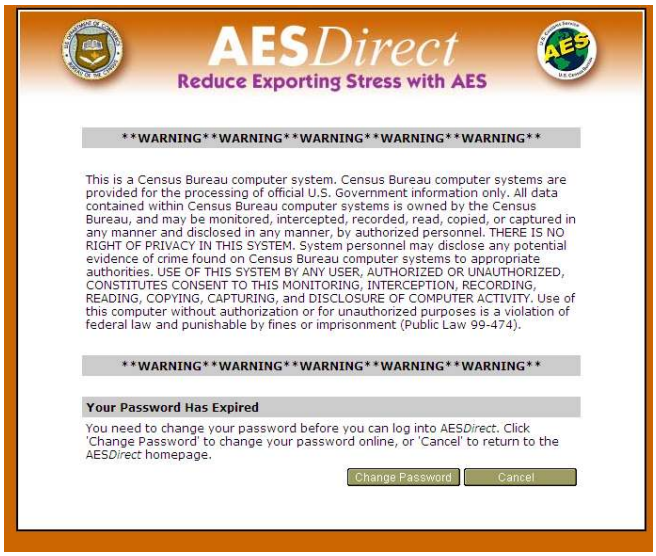
A box will open and ask you to confirm that you would like to reset the User's password

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 by email or, preferably, telephone.



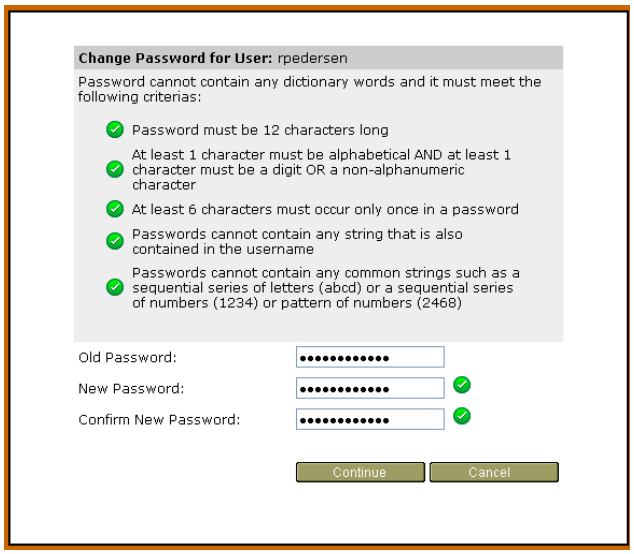
7) When the User attempts to login, they will be forced to change their password

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

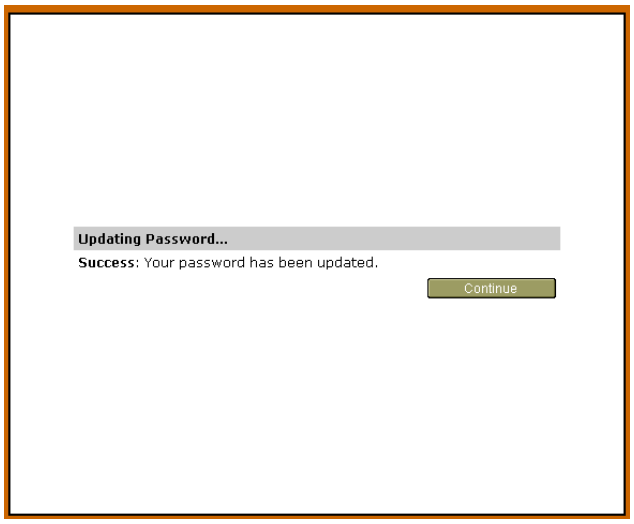
- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # $ %

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

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



AESDirect will validate the password as the User creates it.



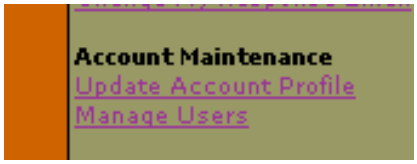
Once updated, the User will have access to your AESDirect Account.

Disable a User

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

To disable a User Account

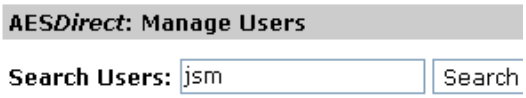
1) Login to AES*Direct*



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

The **AES*Direct*: 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

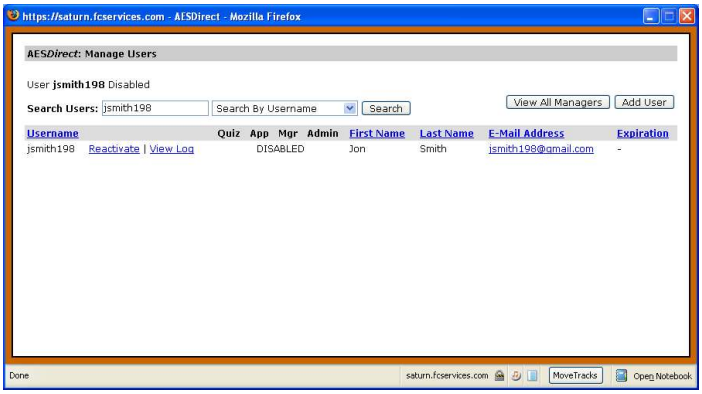
c) Click 'Search'

A list of matches will be returned.

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

A window will open and ask you to confirm

5) Click 'OK'



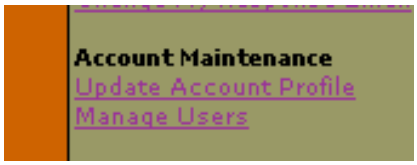
DISABLED will appear where a User's permissions are normally indicated.

Reactivate a Disabled User

Users can be disabled for a number of reasons. If they have left the company, the Account Administrator or User Manager should disable them. Also, if a User has been in-active for more than 90 days, the User will be disabled. When a User is disabled, the User still exists in AES*Direct* and they can be reactivated at any time.

To reactivate a disabled User

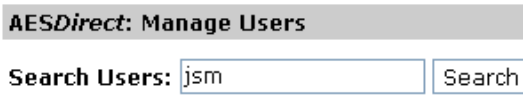
1) Login to AES*Direct*



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

The **AES*Direct*: Manage Users** screen will open

3) Search for the User

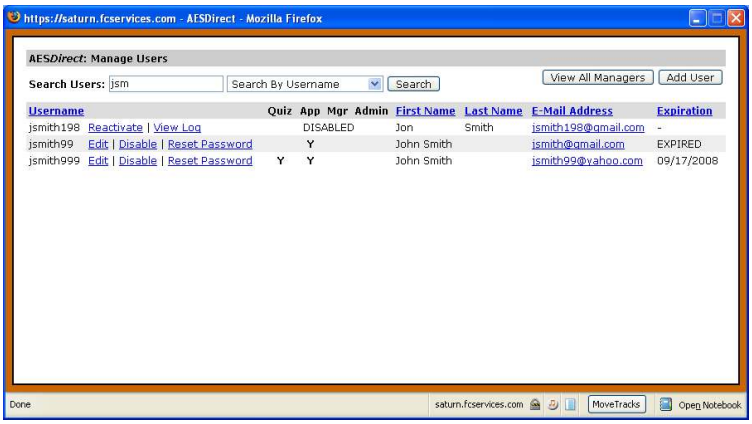


a) Enter at least one character of a search string

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

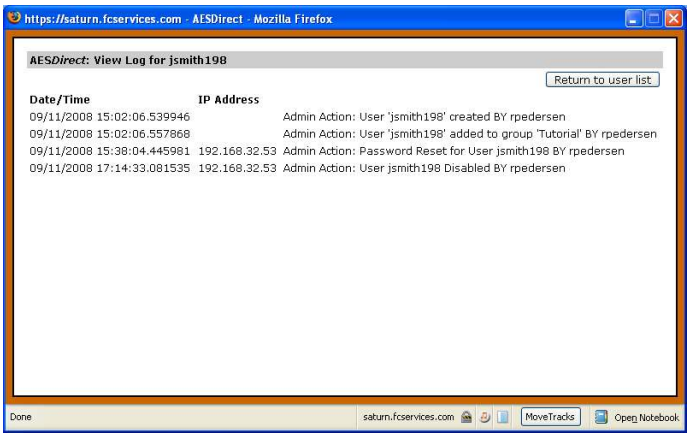
- Username
- E-Mail Address
- First Name
- Last Name

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’



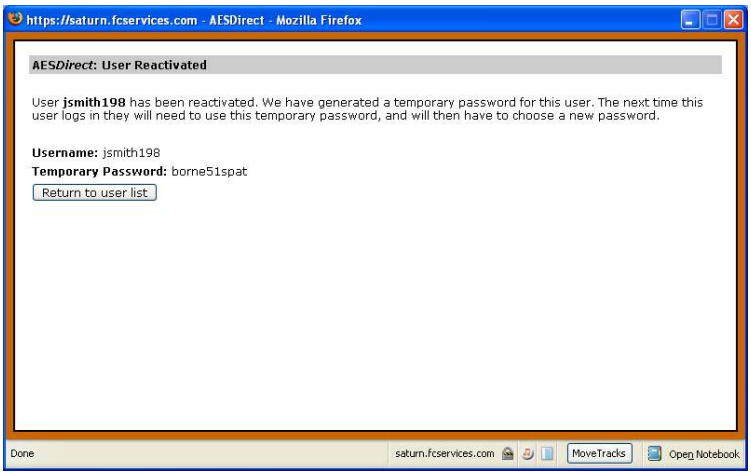
View Log allows you to review the attempts the User or any other individual made to gain access to the account.

Click 'Return to user list'

4) Click 'Reactivate'

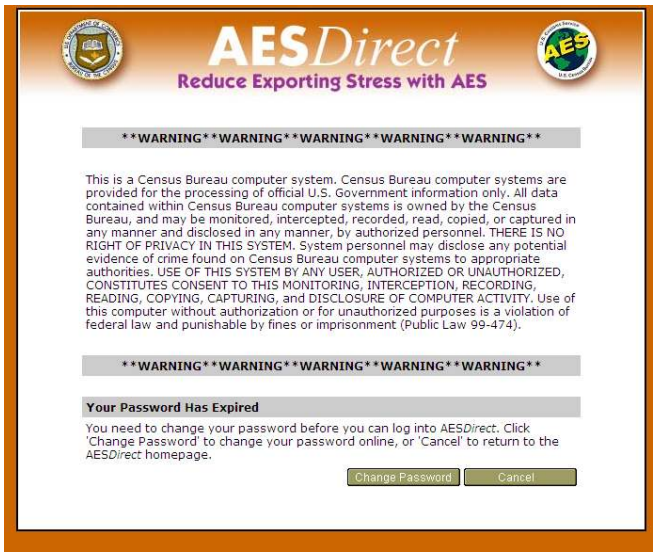
A window will open and ask you to confirm

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 by email or, preferably, telephone.



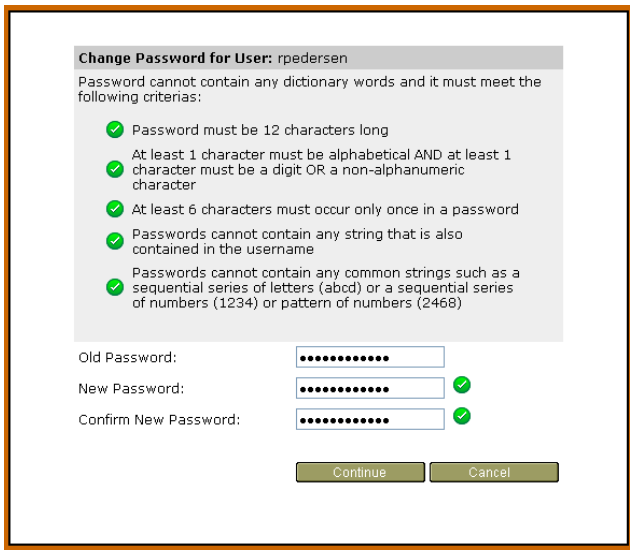
7) When the User attempts to login, they will be forced to change their password

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

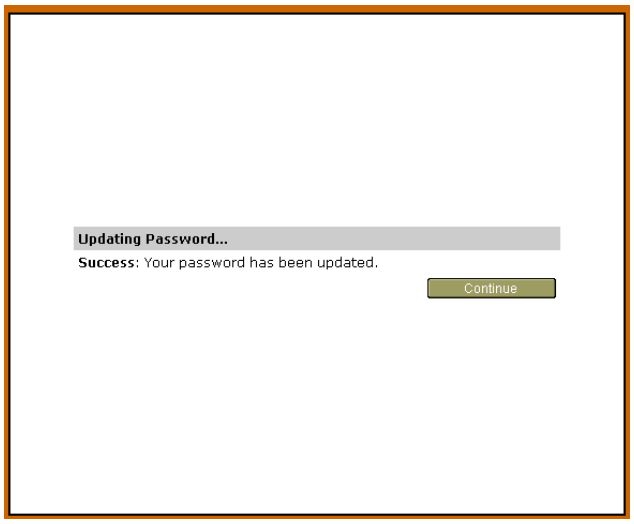
- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # $ %

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

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

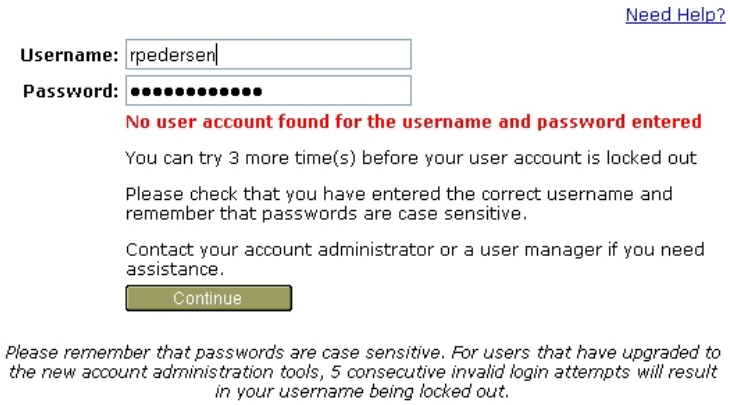


AESDirect will validate the password as the User creates it.



Reactivate a Locked Out User

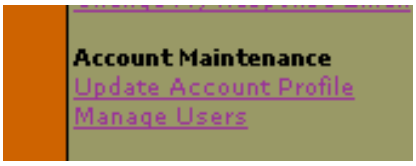
Users who attempt to log in to AES*Direct* with their Username but make 5 consecutive invalid attempts within 15 minutes will, as a security precaution, be locked out.



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

To reactivate a locked out User…

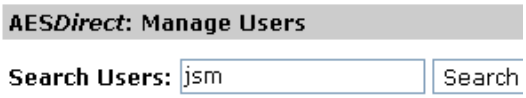
1) Login to AES*Direct*



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

The **AES*Direct*: Manage Users** screen will open

3) Search for the User

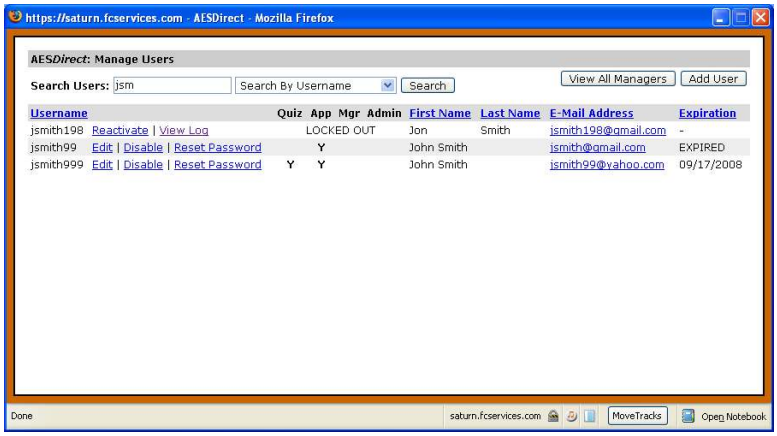


a) Enter at least one character of a search string

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

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

c) Click 'Search'



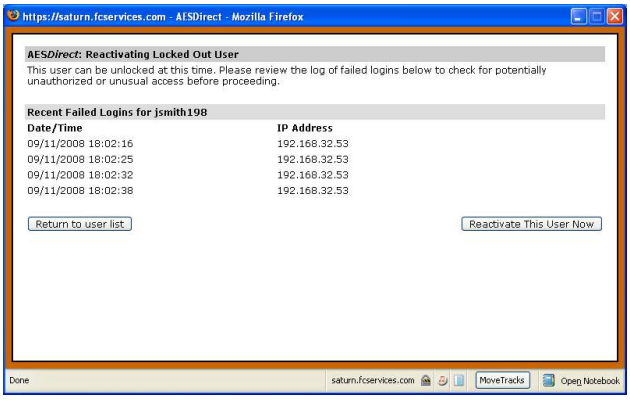
A list of matches will be returned. **Locked Out** will appear where a Username's permissions are indicated.

4) Click 'Reactivate'

A window will open and ask you to confirm

5) Click 'OK'

The **AES*Direct*: 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 five that would result in a lockout, your AESDirect Account may be subject to a malicious attack. If you suspect you are the victim of an attack, contact AES*Direct* Technical Support immediately.

6) Review the log in attempts again to identify any abnormalities

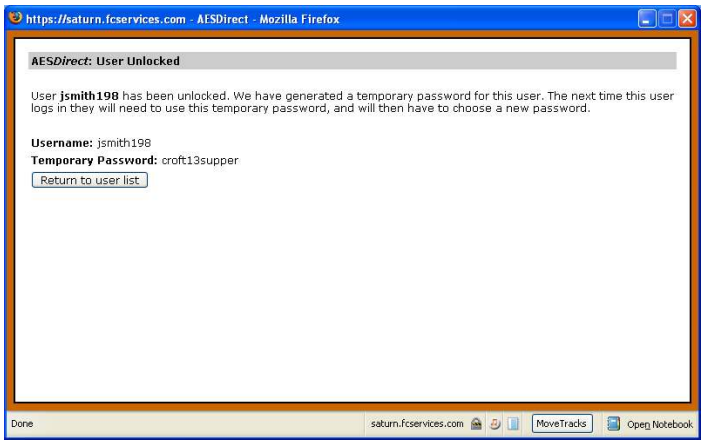
7) If all seems right, click 'Reactivate This User Now'

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

8) Click 'OK'

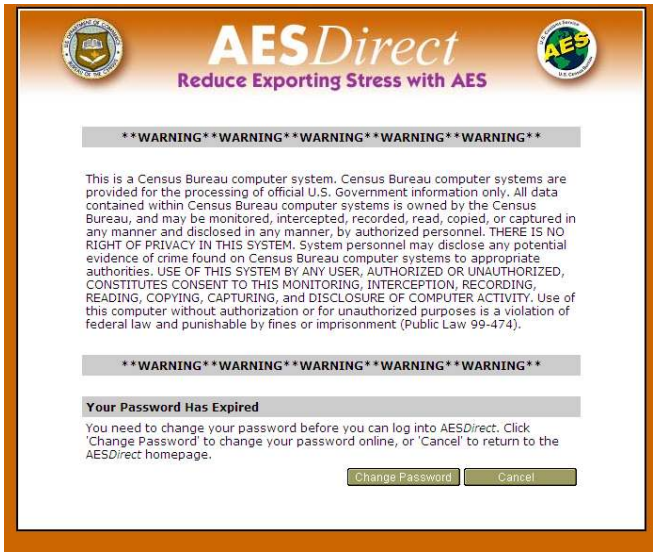
Another window will open and ask if you are sure you would like to reactivate the User.

9) Click ‘OK’

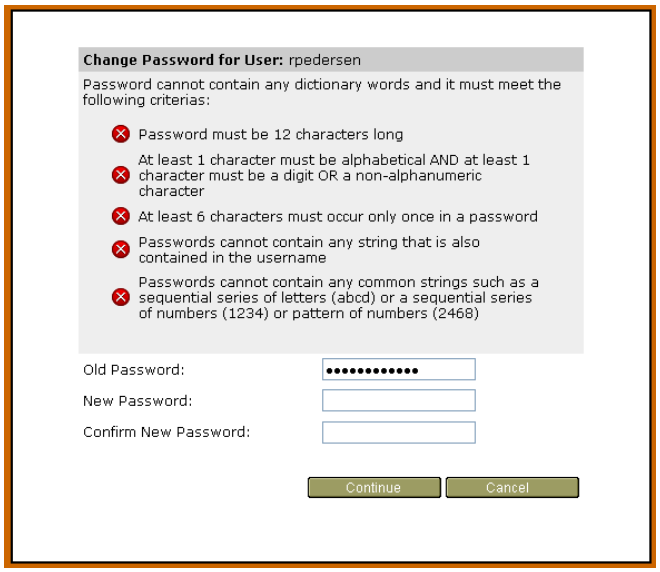


A new window will open. The password will be reset and a new temporary password displayed

10) Deliver this password directly to the User.



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

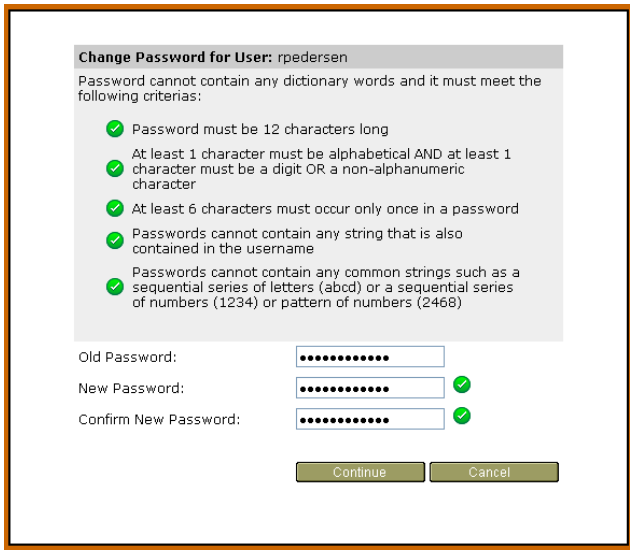


All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

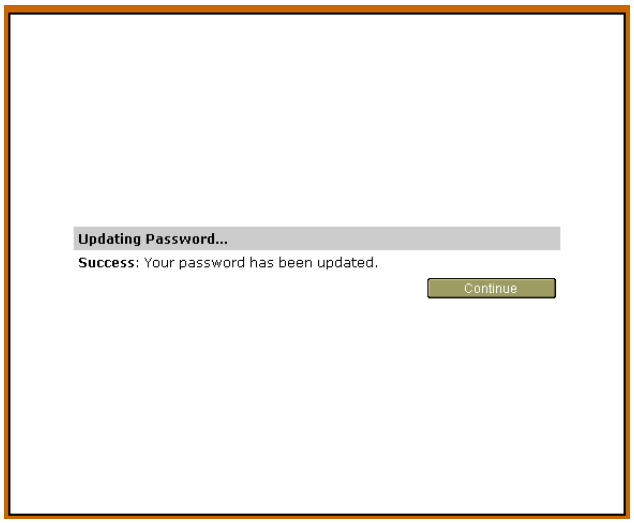
- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # $ %

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

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



AESDirect will validate the password as the User creates it.



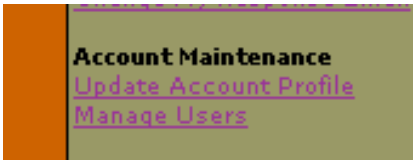
Once updated, the User will have access to your AESDirect Account.

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, your company must take additional measures identify a new Account Administrator in AES*Direct*, as they are the individual directly responsible for AES*Direct* maintenance.

To Change an Account Administrator...

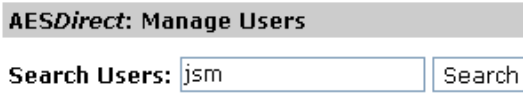
1) Login to AES*Direct*



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

The **AES*Direct*: Manage Users** screen will open

3) Search for the User

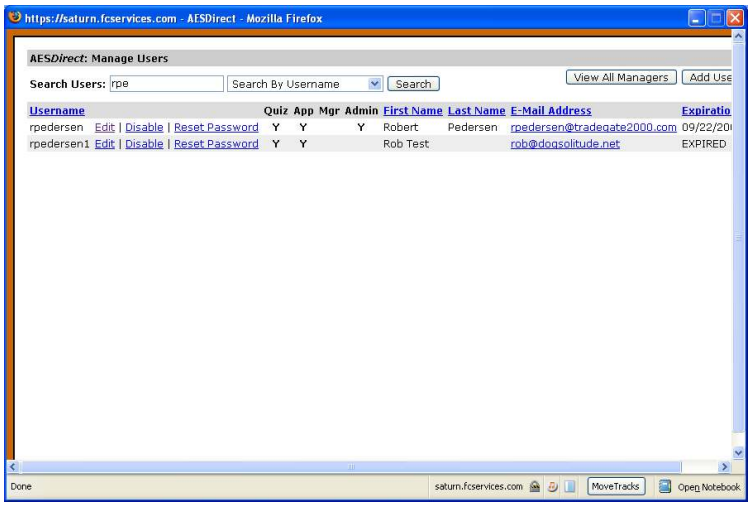


a) Enter at least one character of a search string

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

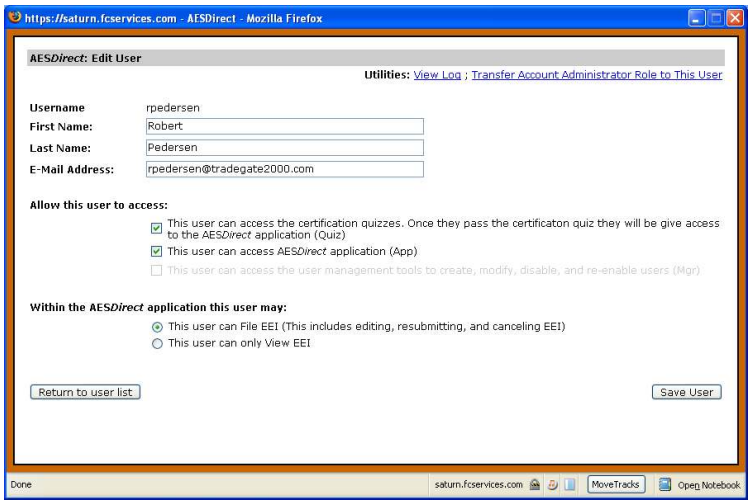
- Username
- E-Mail Address
- First Name
- Last Name

c) Click 'Search'

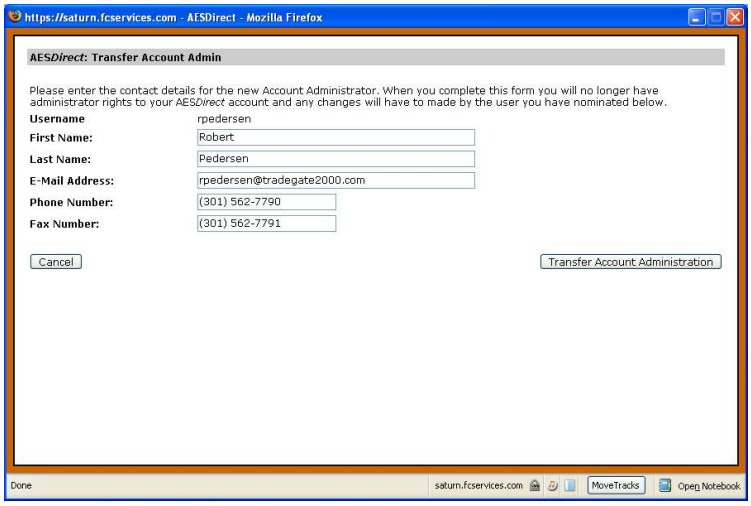


A list of matches will be returned.

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



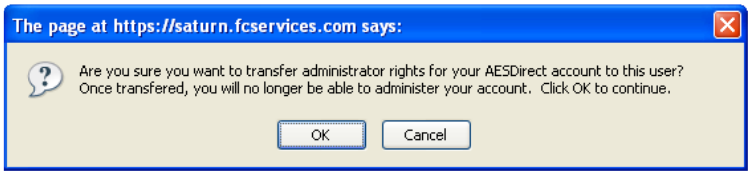
5) Click ‘Transfer Account Administrator Role to This User’



The **AES*Direct*: 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'

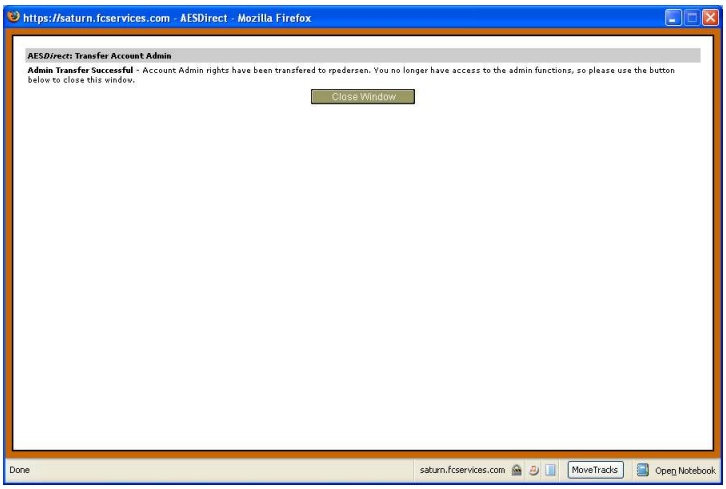


You will be asked to confirm the change of Account Administrator a first time

8) Click 'OK'

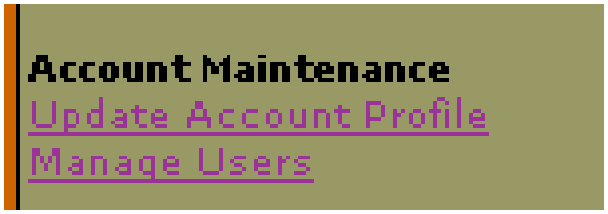
You will be asked to confirm the change of Account Administrator a second time

9) Click 'OK'



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

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)
- AES*Direct* 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 12 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.