AES Branch,
Foreign Trade Division,
U.S. Census Bureau

AES*Direct* Account Maintenance Transition

Account Maintenance Transition to Begin Roll-Out October 1, 2008

Issue II
September, 2008

Transition Roll-Out October 1, 2008

On October 1, 2008, AES*Direct* will begin the roll out of Account Maintenance changes to AES*Direct* clients. Per the first newsletter[1], published in July 2008, changes will 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**
- **New Account Administration Functions**

AES*Direct*'s Increased Security Measures Benefits its Users!

Special points of interest:

- ✓ The Transition "At a Glance"
- ✓ A Closer Look
- ✓ AES*Direct* Usernames
- ✓ The Roles Defined
- ✓ A New Feature: "View Only"
- ✓ New Administrative Functions

Account changes will be phased in over a period of months, based on existing accounts pending Password expiration date. Once a password expires, the Account Administrator for that Account will be responsible for managing the transition. All users will be asked to make this change within the 90 days after October 1st and all changes must be completed by January 13, 2009. This newsletter will cover the specifics of the transition and will also answer many of the inquiries that have been fielded from our AES*Direct* client-base.

We have taken into great consideration our clients as a whole and have developed a plan that will provide the easiest transition across the board. We are aware of the drastic implementation change that this may impose upon some of our clients and are available to answer any questions or discuss possible issues that provide you with concern. Further direct communication, including the distribution of an Administrative User Guide, which will outline step-by-step instructions for the change, is pending. Please read this newsletter in its entirety, as well as the previous issue available online via the link listed below. If you still have questions/concerns please call 1-800-549-0595, option 1, or e-mail askaes@census.gov for further assistance or clarification.

Keep in mind, these changes will be phased in over a 90-day period beginning October 1, 2008.

[1] **The first issue of newsletter is available for download at:**
http://www.census.gov/foreign-trade/aes/documentlibrary/AESDirectAccountMaintenanceChanges.pdf

The Roles Defined…

Account Administrator is the highest level of authority in reference to a company's AES*Direct* Account and able to perform all of the administrative functions relative to that company account.

User Manager is the second highest level of authority in the hierarchy and assists the Account Administrator with user account maintenance functions only.

User is the account level designation for each filer within the company. Each user has a user account (individual username and password).

***Be mindful that there is an AESDirect company-level **"Account"** and there are individual user-level **"accounts"** assigned to each user on the system (note the distinction with the uppercase and lowercase "a"). If a user "account" is experiencing an issue, the Account Administrator should be contacted. If an Account Administrator is locked out of the company "Account," AES*Direct* Technical Support must be contacted.

The Transition "At a Glance"

The transition to the upgraded Account Maintenance features will be driven by the 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, your expiration date will remain the same.

Once an Account Password expires, the Administrator will be required to upgrade their AES*Direct* Account to include the new features. Account Administrators, however, may choose to do this before their expiration date, but after October 1st. 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 AES*Direct* can still be used for 15 days following the upgrade. This username will not be subject to any of the new AES*Direct* security restrictions during this time.

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 AES*Direct* username. The password will expire and must be reset. At this time, all filers should file with their own, unique username and password.

*****Accounts can be upgraded at Administrator's discretion prior to scheduled transition period.**

The Specifics…

After October 1, 2008, when the password for a company account has expired, the user that makes the upgrade from the current "Admin Code" structured account will be designated as the Account Administrator. This person will have to have both the "Admin Code" and the administrative password to upgrade the account. This newly created Account Administrator will have the ability to designate two User Managers that will be able to assist with the administrative duties. The User Managers will be able to create, disable, and unlock user accounts. The Account Administrator will be able to perform all of these functions as well, in addition to viewing/updating account profile information, adding/removing User Managers, and nominating a new Account Administrator.

Making Your Move

***Under the new structure, Account Administrators are now able to nominate a new Account Administrator to assume the administrator responsibilities without communication via fax with AES*Direct* Technical Support. In the event that an Administrator leaves the company without nominating a new Administrator, a fax on company letterhead will be required to designate a new administrator.

AESDirect 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. Alternate suggestions for failed usernames will be given.

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 (at which time the Administrator should disable the user account.)

Reminder - The previous company-wide username/password will be available for 15 days after account is upgraded.

*****Usernames and Passwords are not to be shared.**

A New Feature: "View Only"

Account Administrators will now be able to set-up user accounts and provide them with the permission to **"View Only."** This will be extremely beneficial for Compliance Managers and Quality Assurance personnel because it allows them the functionality to review all Electronic Export Information (EEI) without having the authorization to create, edit or delete shipments.

***Accounts with solely the "View Only" designation will be able to view and/or print EEI associated with their company's Account.

AES Branch,
Foreign Trade Division,
U.S. Census Bureau

www.census.gov/aes

Phone: 800-549-0595
Option 1 - AES Branch
Option 2 - Commodity Analysis Branch
Option 3 - Regulations Outreach & Education Branch

We're here to help you!!!

Our Pledge to You...

We understand that these new security enhancements have the capacity to impact your work environment drastically and we are here to assist you in any way possible to provide for a smooth transition. If you have any concerns or encounter any issues that we are able to assist your company with as we migrate to the new security platform, do not hesitate to contact us via the information provided to the left.

Keep in mind, user security, confidentiality and data integrity are our top priorities and we are here to serve you. Change can be overwhelming and we are aware of the effect this will have on your processes. The utmost concern for you, our clients, was taken into consideration as we developed and employed this new standard.

New Account Administration Functions

The following functionalities will be provided to the **Account Administrator** and **User Managers** when the new security measures are phased in beginning **October 1, 2008**:

- **Create New User**
- **Search/View Users by:**
  - Name
  - Username
  - E-mail Address
  - Group (user level)
- **Edit User**
  - Change groups
  - Update profile (name, e-mail address, etc.)
- **Disable User**
- **Reactivate User**
  - This function will be used for manually disabled users and users that have been locked out. It will issue a reset code for the Account Administrator to give to user
- **Reset Password**
  - This function will issue a reset code that the Account Administrator will give to the user

The Account Administrator has the power and can create 2 User Managers to assist with user account-level maintenance.

****The Account Administrator has other privileges that are not afforded to User Managers (detailed on page 2).*