achbusiness.com™
Processor

QUICK START GUIDE

CONFIDENTIAL: **For Financial Institution use only. Do NOT make information available to clients.**

Last Modified: Monday, May 06, 2019

11 Racetrack Road NE, Suite F-3
Fort Walton Beach, FL 32547 USA
850-315-4944
www.sbtinc.com

Welcome to achbusiness.com

System Requirements

achbusiness.com Processor (Browser):

1. Internet Explorer 11, Firefox 38+, Google Chrome 39+, or Microsoft Edge
2. Frames, scripts, and cookies enabled
3. 256 Bit Encryption
4. Secure user name and password

Browser Configuration

As browsers strive to become more and more "secure", they also become more restrictive by default. Some of these restrictions can conflict with the way that online systems must communicate with end-users. These settings are not required but will ensure a pleasant user experience. Here are some things you can do to ensure printing, prompts, and other features work properly for you:

1. Go to your browser options menu. Click "Tools" -> "Internet Options"
2. Click on "Security" tab -> click on "Trusted Sites" -> click on "Sites"
3. Add the following site to the list: https://hosted.achbusiness.com
4. Click "Close" -> click "Custom Level"
5. Ensure that "Automatic prompting for file downloads" is ***enabled***
6. Ensure that "Allow websites to prompt for information using scripted windows" is ***enabled***
7. Click "Close" -> Click "Advanced" tab -> ***uncheck*** "Do not save encrypted pages to disk"

***Please be sure that all Microsoft Recommended Updates have been applied to your machine**

Obtaining a Certificate

***Please be advised that the Certificate must be renewed annually. For seamless operation, be sure to renew in advance of expiration.**

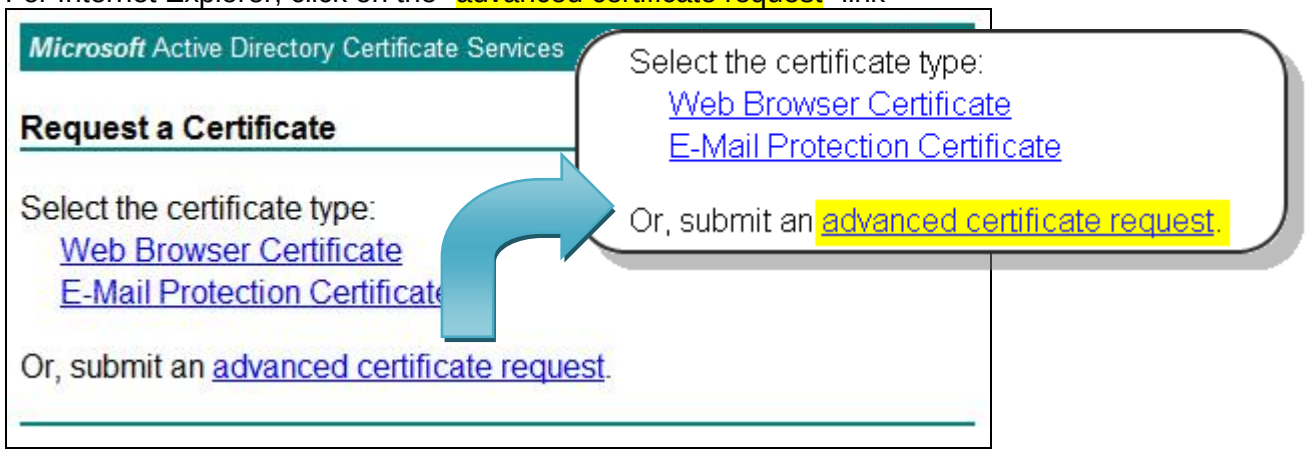
This will seem like a lot to digest at first, but it goes quickly once you get the hang of it. Microsoft makes installing a certificate especially difficult in an effort to ensure the most secure experience. It is also a requirement of banking regulations to have three levels of encryption security when dealing with sensitive, end-user data. Secure certificates fulfill that requirement.

- You must use either the Microsoft Internet Explorer or the Mozilla Firefox browser to request and install your certificate. If you are a Google Chrome or Microsoft Edge user, use Internet Explorer just to request and install your certificate.

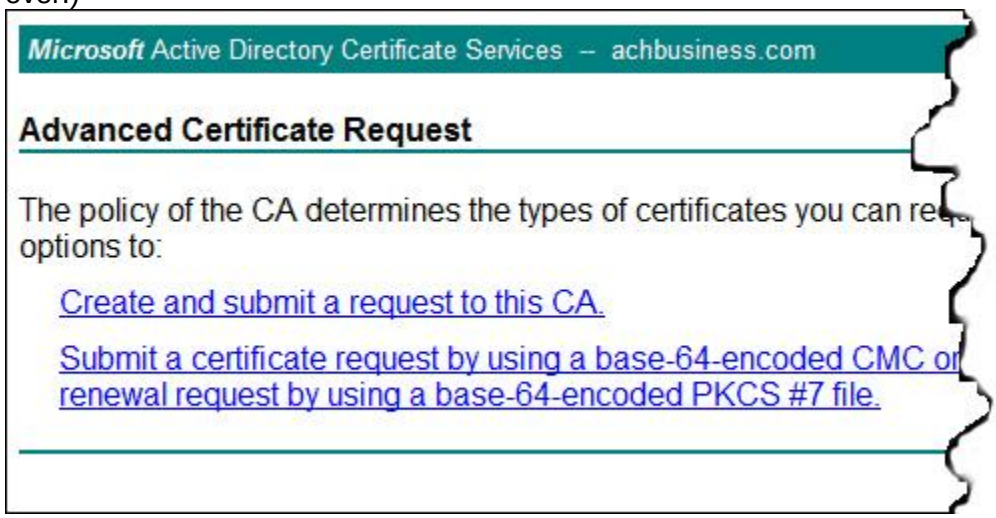
- Go to https://hosted.achbusiness.com/certsrv

- Choose "Request a Certificate"

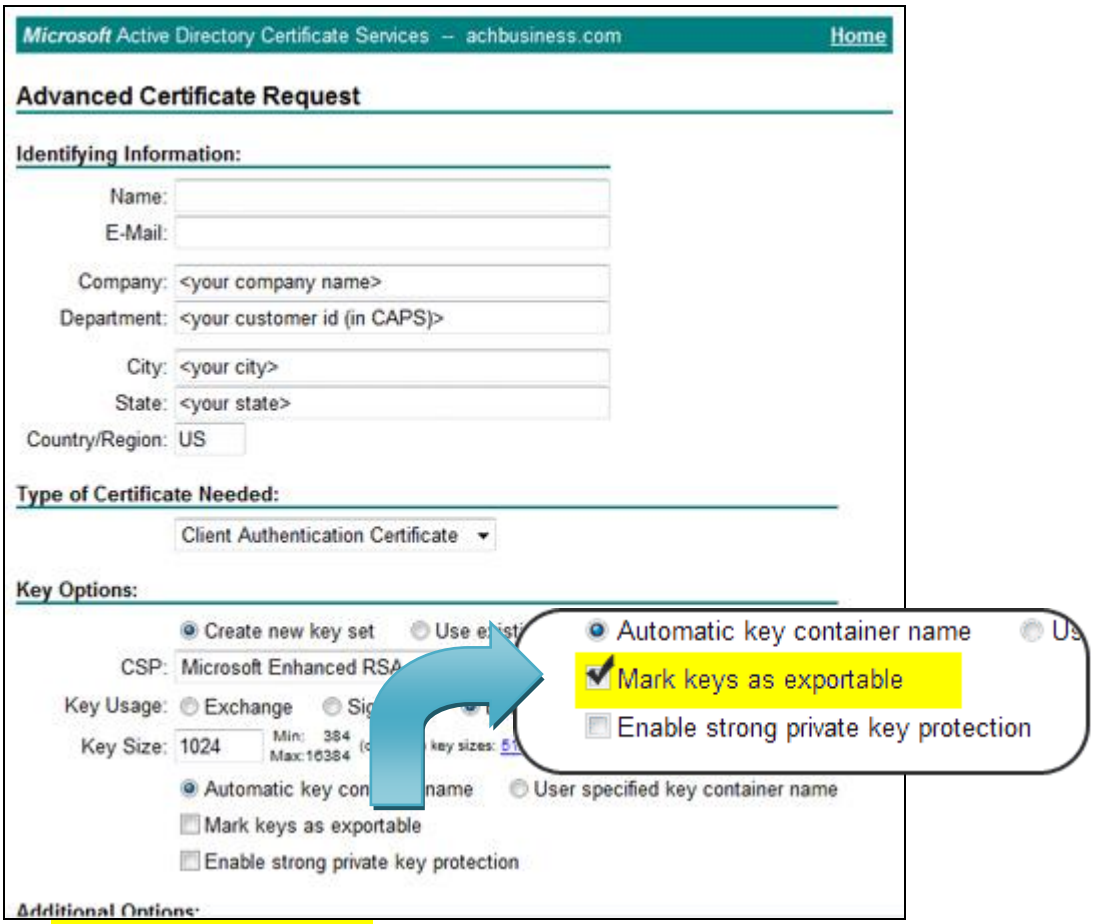
- For Firefox, click on the "Web Browser Certificate" link
- For Internet Explorer, click on the "advanced certificate request" link



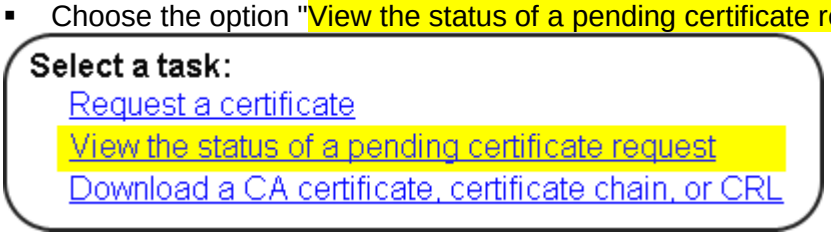
- Select 'Create and submit a request to this CA' (NOTE: if you see a different screen at this point, click on Tools, then "Compatibility View Settings", then click the Add button. Use the browser's back button to return to the "Welcome page and start over.)



Complete the certificate request screen (shown below) by following instructions that follow.



- Fill in the form as follows:
  - Name – User's Full Name
  - Email – Enter an email for further validation by server
  - Company – Your Company Name
  - Customer ID – Your Customer ID (must be in CAPS)
  - Enter your City / State, as desired
- CSP should be “Microsoft Enhanced RSA and AES Cryptographic Provider”
- Key size should be 2048
- Be sure to check ‘Mark keys as exportable’ but do not change anything else in that section
- Scroll down, click "SUBMIT" *
- Click “Yes” to the message: “This Web site is requesting a new certificate on your behalf.”
- Notify your financial institution of your request and ask them to verify & issue it for you
- Once the request is granted, click on the "Home" link in upper right corner to continue
- Choose the option "View the status of a pending certificate request"



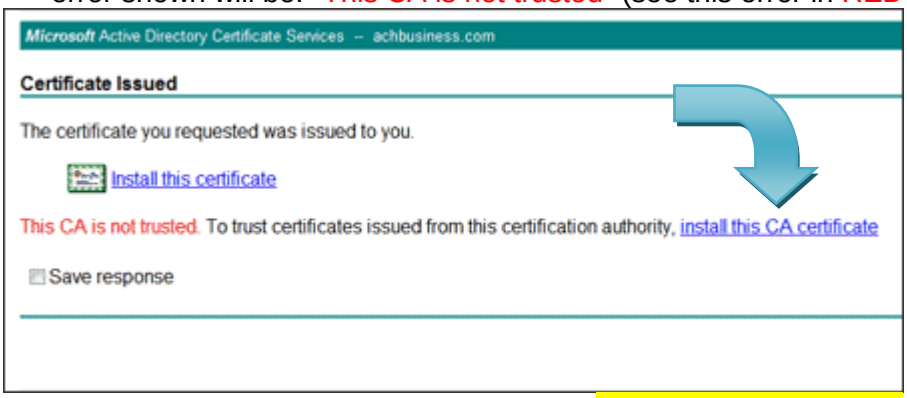
- Choose the certificate applied for –by date- by clicking it

If the certificate was issued, it will download to the client

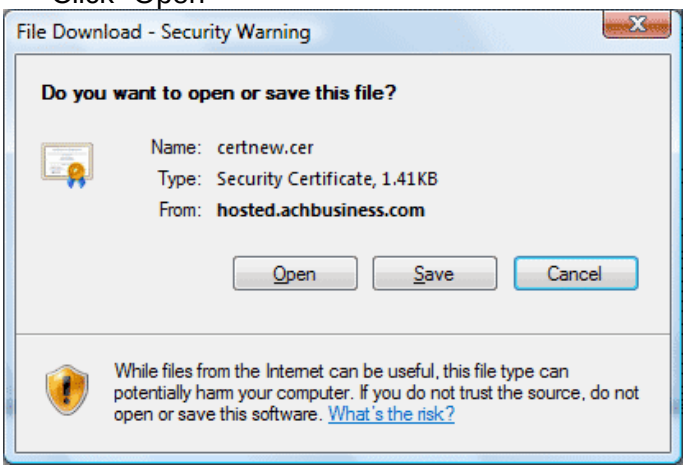
**BE SURE TO WAIT FOR THE CERTIFICATE TO COMPLETELY DOWNLOAD*

(i.e. make sure that the 'blue' indicator bar at the bottom of the browser is finished loading)

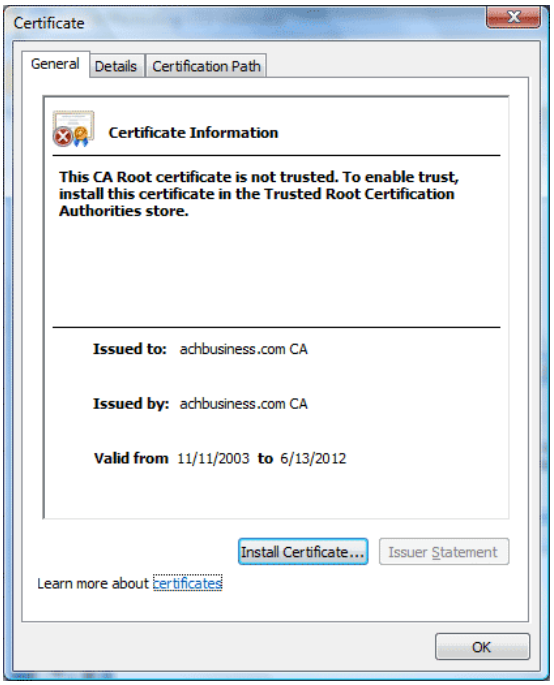
- For VISTA / Windows7 users, clicking "Install this certificate" ***WILL FAIL.*** The error shown will be: "This CA is not trusted" (see this error in RED below).



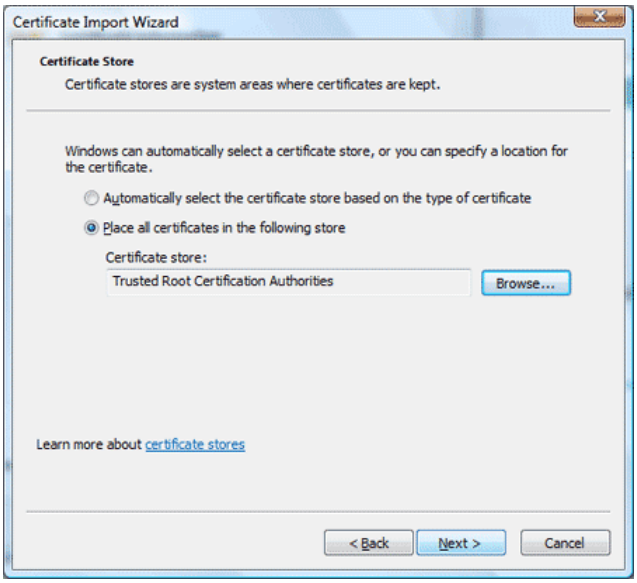
- Go all the way over to the right and click "install this **CA** certificate"
- Click "Open"

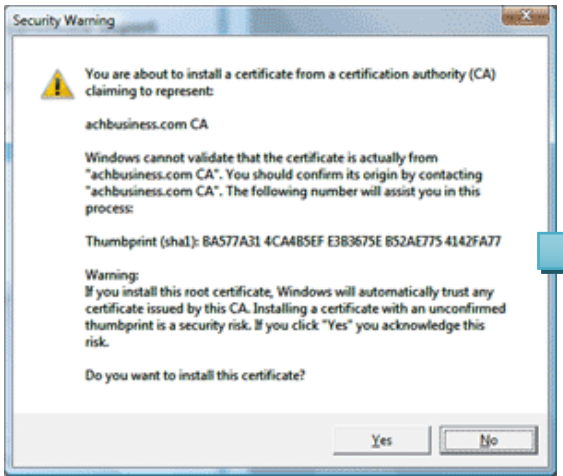


- Click 'Install Certificate…'

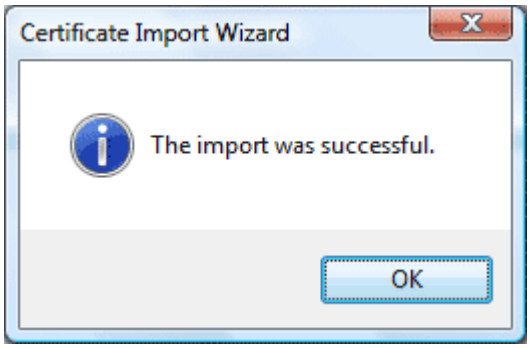


- Click ‘Next’ on the certificate import wizard screen to begin
- On this screen, it is ***VERY IMPORTANT*** to click "Place all certificates in the following store"
    - Click "Browse", select "Trusted Root Certification Authorities"
    - You should see: Certificate store - Trusted Root Certification Authorities

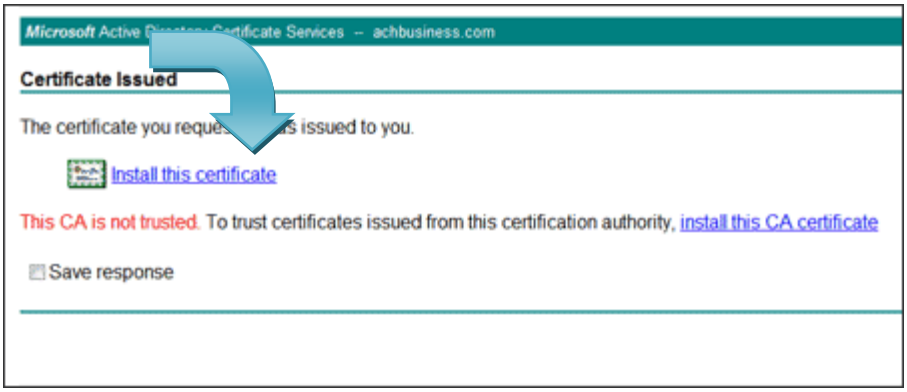




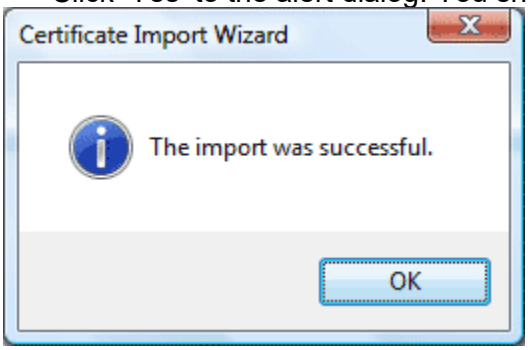
- Click "Next", then click "Finish"
- You will see a "Security Warning" (similar to below). Simply click "Yes" to continue.



- Once you see "The import was successful" dialog prompt, you can click "OK"
- Then click on the original "Install this certificate" link to install the personal certificate



- Click 'Yes' to the alert dialog. You should then see the following message:



- [DONE!] At this point, you must close ALL browsers, reopen a browser, and then you may proceed to the "Logging on to achbusiness.com" section.

Requesting a Certificate

1. **Note**: If this is a network environment be sure to be logged on as the user that will be accessing the service. This is necessary because each certificate specifically identifies with one user. If there will be multiple users accessing this service each must request a certificate from the computer while logged on as that user on the network.

***Please be advised that the Certificate must be renewed annually. For seamless operation, be sure to renew in advance of expiration.**

How to issue a Clients Certificate

*Your customers should notify you that they have requested a certificate.

1. Go to Files – Certificate Management or choose the Certificate Management icon.

2. Select the certificate and click on the 'Issue' button to issue the certificate (You may also deny or revoke a certificate from this screen)

*If your customer has not requested the certificate correctly, it will not appear on this screen

Using your iPhone

You can access achbusiness.com as a web app using the Safari app. It needs certificates just as the PC does. Apple refers to them as Profiles. Complete instructions for importing the certs into your iPhone can be found in the Client QuickStart Guide.

Logging on to achbusiness.com

URL: https://hosted.achbusiness.com/scripts/webcas/asp/processor.asp?id=___

*****Be sure when logging off of achbusiness.com to use the Logoff button on your toolbar instead of closing the browser.

*****If prompted for a Master Password at any time, the password is "MASTER". The master password may be changed by, going to Config-System-Password Preferences and selecting Master PW.

*****If you would like your company logo displayed, please email the logo to sbtsales@sbtinc.com

Configurations

Provider information must be filled out in the Provider Profile screen.

- Fill in the form as follows:

  Provider Identification
  - Provider Name – Your Institution or Company name
  - Provider Address – Your Institutions address
  - Telex Name – Your Institutions abbreviated name
  - Reply to Email-Email to receive notification once client has sent their ACH File(s).

  ACH Configuration
  - Immediate Destination- Enter the ABA number and name of the FRB or ACH Processor which processes ACH files originated by your institution
  - Transmitter- Enter the ABA number and name of your institution
  - ACH Ident No.- Optional Field (Leave Blank)
  - Enable Risk Management- when checked, activates optional ACH risk management functionality

ONUS ABA's- Enter ABA numbers which make up your institutions enterprise ACH Payroll Prefunding (where applicable)

*If you do not want to use this feature simply leave all fields blank.

- RT/ABA- Enter the routing transit number for the common prefunding account
- Account Number-Enter the account number of the account that the payroll prefunding will use
- Prefund Days- Select the number of days to subtract from the customer specified effective date.

Click 'Save' upon completion

Adding a New Customer

1. Go to Config – Customer – Customer Profiles.
2. Select 'Add new customer'.
3. Enter the specified information into each field.
    - Customer ID: This field is only available for modification during the initial entry of customer identification information. When the Add New Customer button is pushed, you may enter a Customer ID in this field. Otherwise, the field is for display only.
    - Company Name: This field is the name of the company.
    - Company Address1, 2 and City, State, Zip: These fields are the mailing address of the company.
    - Customer Type: Select C for corporate/small business or F for financial institution customer.
    - Active Customer: Select Y(yes) or N(no) from the drop down menu.
    - Sender ABA: Enter the ABA number of the bank originating electronic funds transfers for this customer (accommodates holding companies and service bureaus).
    - Upgrade: Use default setting.
    - ACH Validation: Enter one of the following codes to determine if account numbers are validated against this customer's predefined accounts when originating

        B - validate both debits and credits

        C - only credited accounts validated

        D - only debited accounts

        N - no accounts are validated

        T - validate both debits and credits and require balanced files

        Z- Do not validate accounts, but require balanced files
    - Prohibit OFAC: Processor must subscribe to the OFAC scanning service in order to allow customers to scan files.
    - Prohibit ACH TEL: Y or N; Do you want this customer to be able to originate ACH TEL transactions

- Disable ACH Warehousing: Keep default setting of N (No)

- Prohibit ACH WEB: Y or N; Do you want this customer to be able to originate ACH WEB transactions
- Prefund Payrolls: When set to Y ACH payroll files submitted by this customer will automatically credit your payroll prefunding account 1-9 (configuration option) days earlier than the customer-specified effective date. The employee deposits will then be debited from your payroll prefunding account.

4. Click 'Save'
5. Click the 'ACH Orig' Button
6. Select the SEC code(s) that the customer will be authorized for
7. Click the 'Applications' Button
8. Activate the appropriate applications for the selected customer.
    - Options: Y or N - Does the customer have access to this application
    - Mon. Rate, File Rate, and Entry Rate: (Optional) To setup billing for this customer – Monthly Rate, Per File Rate, and Per Entry Rate
9. Click 'Save'.
10. Click the 'Security' Button.

Backdoor Name: This field displays the backdoor name for this account. The backdoor name is a five-character code that may be disclosed to a customer to gain access to an admin logon when no name/password combination will work. **For security purposes, once this code is disclosed, be sure to change it**.

Security PIN: The Security PIN for this account is an optional personal identification number (PIN) assigned to this customer.

Security PIN Owner: Enter the name of the person to which the PIN number has been assigned.

Exposure Limit: (If wire transfer creation is an option for this customer) Enter a dollar figure for wire transfer exposure limit (daylight overdraft limit).

ACH Daily Limit: Enter the maximum dollar amount that this customer can originate in a single day. If ACH files are processed more than once per day, the system will keep track of all ACH activity for the day by customer. The dollar amount that you enter here will be checked against both debits and credits. A value of zero disables daily limit checking.

ACH Orig. Deviation: Enter the deviation percentage for originated items associtated with Risk Management.
ACH Ret. Deviation: Enter the deviation percentage for Returns associated with Risk Management.

1. Click 'Save'
2. Click 'Save' Again
3. Click 'Exit'

View Customer Logons/ Reset Passwords

1. Go to Config-Customer-Customer Profiles- Select User by ID- Select the 'User' button
2. To view your customer's passwords, select the appropriate session ID and select 'View Password'. You will be asked to enter in the master password, which is 'MASTER' by default.
3. To reset your customer's password, select the 'reset password' button.
4. Your customer's new password will be 'TEMP'.

*IMPORTANT, PLEASE DO NOT SKIP THIS STEP
Processing Incoming ACH Files

Go to Files - Applications - Normal Processing – ACH Appls – ACH Combined.

Select the file(s) that are to be processed.

Click the Process button. A list of the output files generated is shown.

View the reports and verify that the correct file(s) were processed and that the totals are correct.

If there is a problem then click Close. This will clean up all temporary files and leave the selected files in pending status.

If there are no problems, click 'Commit'. This will move all selected files to the backup directory and allow for the data files to be exported.

After Committal, export any data files. Select the files to be exported and click the "Export" button.

A FRB file and an Onus file can be created.
The FRB file is to be imported into FedLine
The ONUS file is to be imported into the DDA system.