achbusiness.com™
Processor

QUICK START GUIDE

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

Last Modified: Wednesday, July 26, 2023

100 Gulf Shore Dr #301
Destin, FL 32541 USA
850-368-8421
www.sbtinc.com

Welcome to achbusiness.com

General Information

Once configured, the Processor portal is used for two things:

1. Adding and maintaining clients
2. Processing ACH files submitted by clients

System Requirements

achbusiness.com Processor (Browser):

1. Internet Explorer 11, 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. Failure to make these setting changes will cause problems later. Here are some things you can do to ensure printing, prompts, and other features work properly for you:

- Open Control panel and click on Internet Options.
- Click on the "Security" tab -> click on "Trusted Sites" -> click on "Sites"
- Add the following site to the list: https://hosted.achbusiness.com
- Click "Close" -> click "Custom Level"
- Scroll down to Scripting. Ensure that “Active scripting” is ***enabled.***
- Ensure that “Allow websites to prompt for information using scripted windows” is ***enabled***
- Click "OK" -> Click “Advanced” tab. Scroll down to “Security”. ***uncheck*** "Do not save encrypted pages to disk”

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

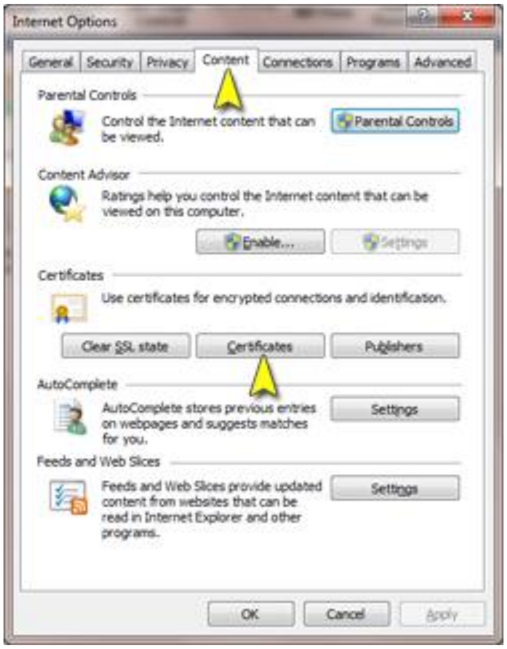
Obtaining a Certificate

- **PLEASE BE AWARE THAT ALL CERTIFICATES ARE GOOD FOR TWO YEARS**
-
- Each client will be warned upon login, as the expiration date approaches.
- **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 (browser) user. If there will be multiple users accessing this service, each one must request a certificate from the computer while logged on as that user on the network.

- Installing a certificate is made difficult by browser developers on purpose. They do it that way to make it tougher for hackers/criminals to steal access to secure sites. However, that means a little more work is required to get it working. We will help you through it, though, with the following steps:

- New users may skip this step and proceed to “To use Microsoft Edge” or ”To Use IE 11”

- If you have an existing certificate, let's be sure to clean up first:
  - Open Control Panel and click on "Internet Options"
  - Click the "Content" tab -> Click the "Certificates" button



Control the Internet content that can be viewed.

Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

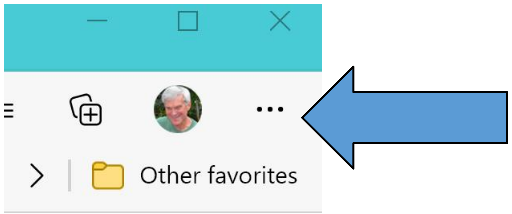
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

  - Highlight any expired certificates and click "Remove"

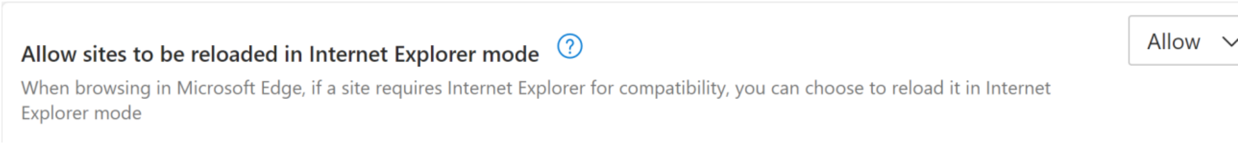
- Click on the "Intermediate Certificate Authorities" tab
    - Look at the top of the list for "achbusiness.com CA" and remove (if exists)
- Click "Close" -> Click "OK"

- You can use either the Microsoft Edge or Microsoft Internet Explorer 11 browsers to request and install your certificate. Google Chrome cannot be used to request and install your certificate, although once your certificate is installed, you can use Google Chrome to access the achbusiness.com site.

- To use Microsoft Edge:
    - Open Microsoft Edge.
    - In the top right corner, click on the "Settings and more" icon (ellipsis or 3 dots).



    - Click on "Settings".
    - In the "Settings" menu in the left pane, click on "Default browser".
    - Under "Internet Explorer compatibility", set the following option to "Allow":
    -



Allow sites to be reloaded in Internet Explorer mode ?

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Allow

    - Restart Edge if prompted.
    - Navigate to https://hosted.achbusiness.com/certsrv

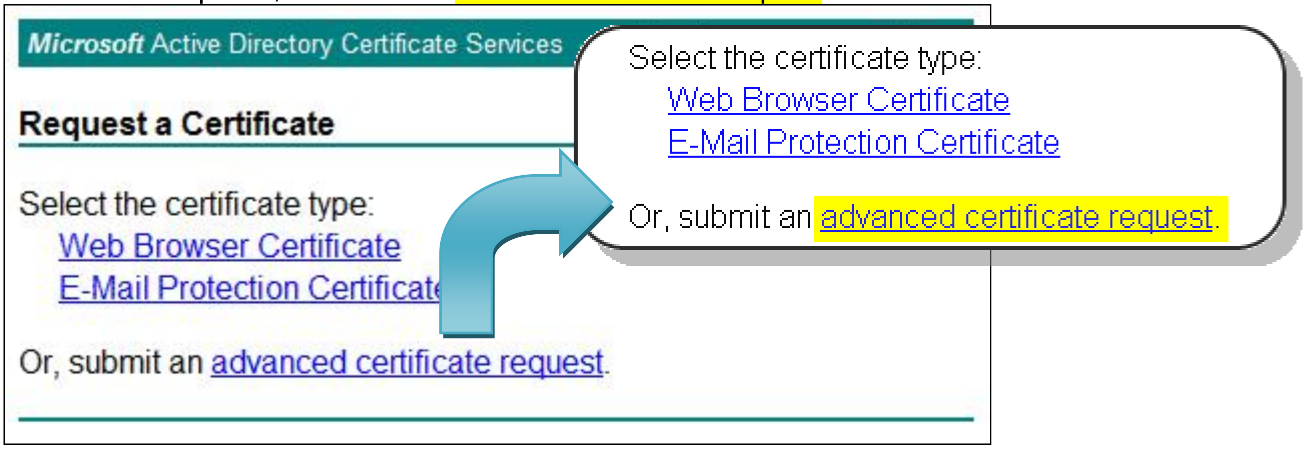
- Once you reach the “Welcome” page, click on the ellipsis in the top right corner again.

- Click on the menu item “Reload in Internet Explorer mode”. This loads the IE rendering engine in Edge for the certsrv site.

- Proceed to the instructions for using Internet Explorer below but skip to the “Request a certificate” step bypassing opening of IE 11 (it’s already running in Edge).

To use IE 11:

- Open IE11.
- 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



Microsoft Active Directory Certificate Services

Request a Certificate

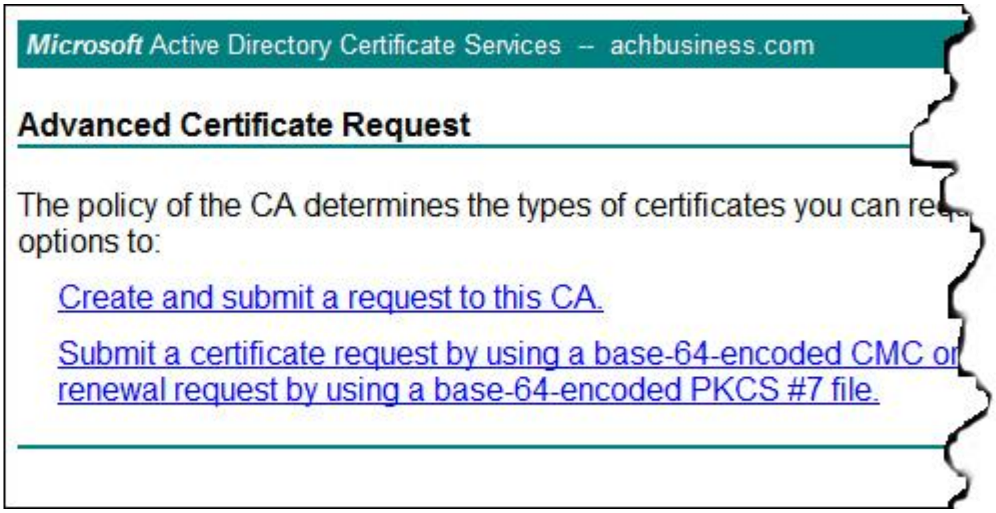
Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

- 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.)



Microsoft Active Directory Certificate Services -- achbusiness.com

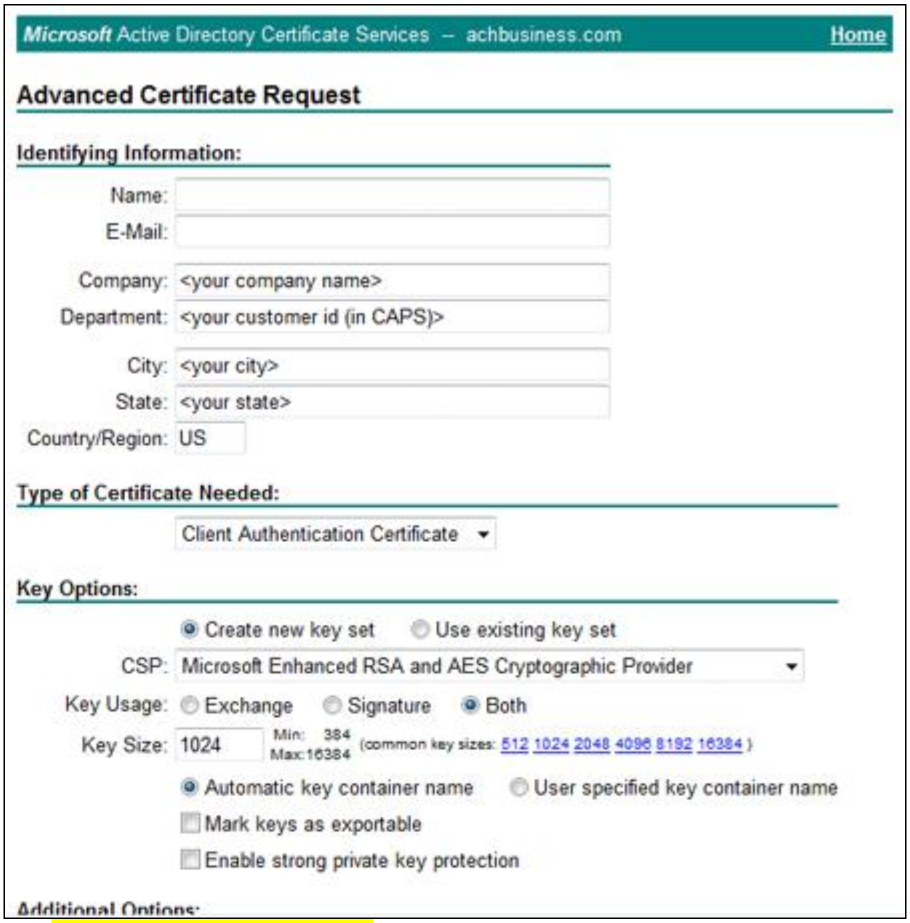
Advanced Certificate Request

The policy of the CA determines the types of certificates you can re
options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or
renewal request by using a base-64-encoded PKCS #7 file.

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



Microsoft Active Directory Certificate Services -- achbusiness.com — Home

Advanced Certificate Request

Identifying Information:

Name:	
E-Mail:	
Company:	<your company name>
Department:	<your customer id (in CAPS)>
City:	<your city>
State:	<your state>
Country/Region:	US

Type of Certificate Needed:

Client Authentication Certificate

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced RSA and AES Cryptographic Provider

Key Usage: ○ Exchange ○ Signature ● Both

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

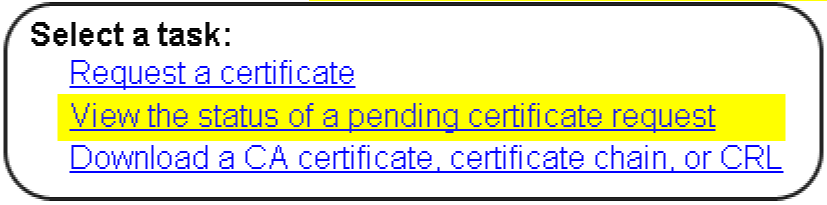
□ Mark keys as exportable

□ Enable strong private key protection

Additional Options:

- 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 SBT 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"



Select a task:

Request a certificate

View the status of a pending certificate request

Download a CA certificate, certificate chain, or CRL

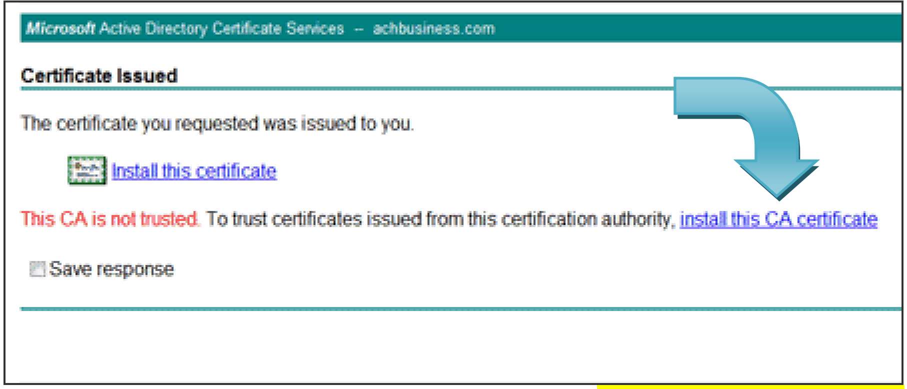
- Choose the certificate applied for –by date- by clicking it

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)

- If this is your first certificate, you will see an error message. The error shown will be: "This CA is not trusted" (see this error in RED below).



Microsoft Active Directory Certificate Services -- achbusiness.com

Certificate Issued

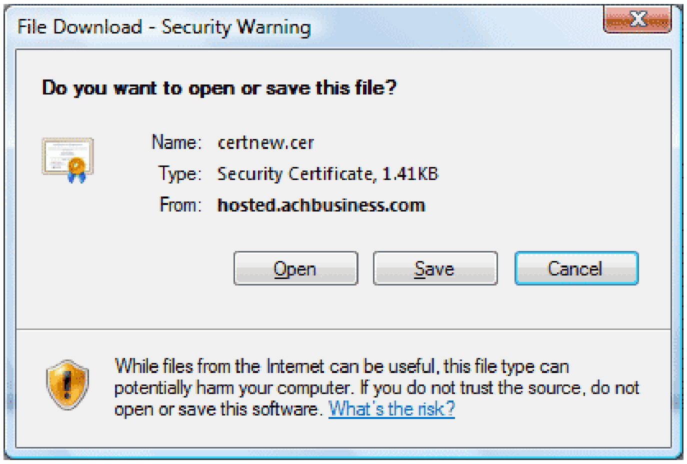
The certificate you requested was issued to you.

Install this certificate

This CA is not trusted. To trust certificates issued from this certification authority, install this CA certificate

□ Save response

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


File Download - Security Warning

Do you want to open or save this file?

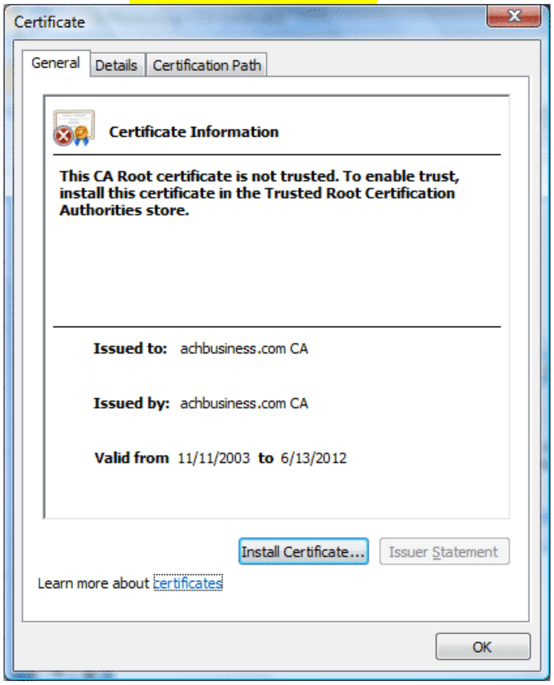
Name: certnew.cer

Type: Security Certificate, 1.41KB

From: hosted.achbusiness.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

- Click 'Install Certificate…'



Certificate Information

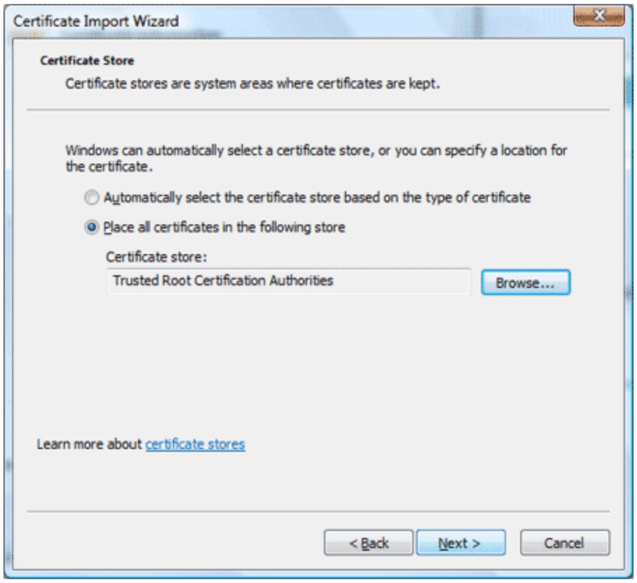
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: achbusiness.com CA

Issued by: achbusiness.com CA

Valid from 11/11/2003 to 6/13/2012

- 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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

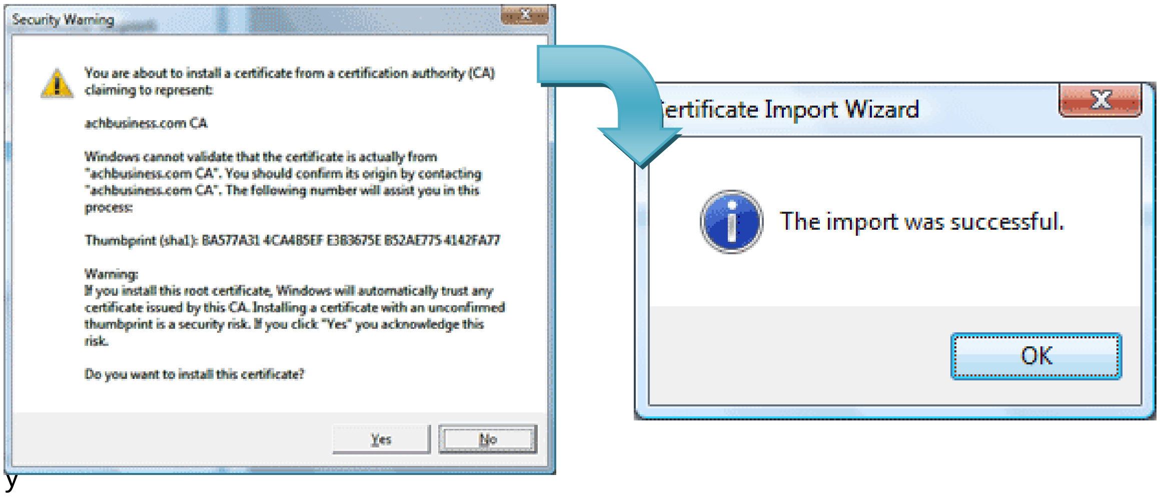
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

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

  Security Warning

  You are about to install a certificate from a certification authority (CA) claiming to represent:

  achbusiness.com CA

  Windows cannot validate that the certificate is actually from "achbusiness.com CA". You should confirm its origin by contacting "achbusiness.com CA". The following number will assist you in this process:

  Thumbprint (sha1): BA577A31 4CA4B5EF E3B3675E B52AE775 4142FA77

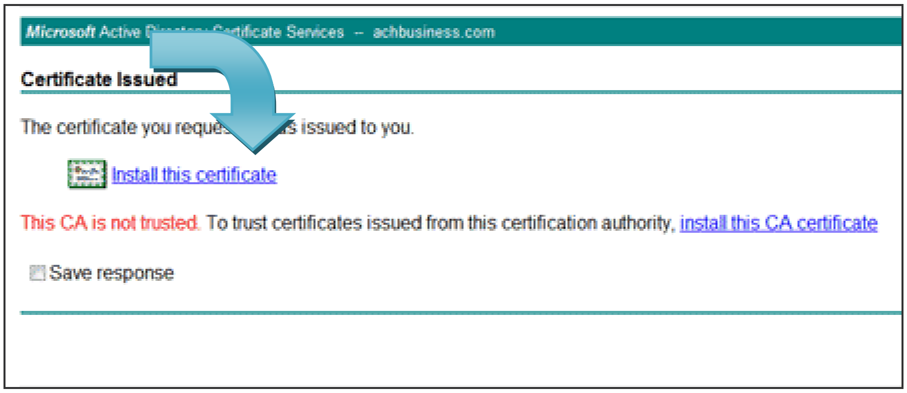
  Warning:
  If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

  Do you want to install this certificate?

  ertificate Import Wizard

  The import was successful.

  y
  ou 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



Microsoft Active Directory Certificate Services -- achbusiness.com

Certificate Issued

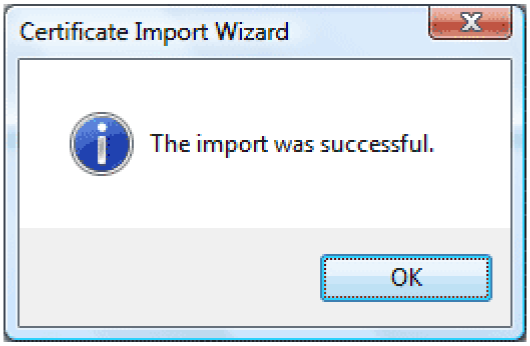
The certificate you reque s issued to you.

Install this certificate

This CA is not trusted. To trust certificates issued from this certification authority, install this CA certificate

□ Save response

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


Certificate Import Wizard

The import was successful.

- [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

Note 1: 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.

Note 2: Support for the Mozilla Firefox browser is being phased out. Current users that are using Firefox can continue to use it until your certificate expires. However, when you need a new certificate, you must switch to Internet Explorer 11 and say goodbye to Firefox (see previous section).

1.

***Please be advised that the Certificate must be renewed every 2 years. 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

<u>Using your iPhone</u>

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=___

When you first go to the site, you should be prompted to select a certificate. Click on your certificate for achbusiness.com to select it and click OK.

***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. In the Configuration icons, click on 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. In the Configuration icons, click on 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

In the Applications icons, click on 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.