

Browsers and AJ Smith Federal Savings Bank Internet Banking Suggested Settings

Updated 7/9/2009

Supported Browsers

This list refers to production versions of publicly released browsers as of July 2010. Beta versions of the individual browsers listed below are not supported. This list may be updated as new versions of individual browsers become available and are qualified with the Retail Internet Banking software. The versions listed below are the minimum required, but it is recommended that you update to the latest versions.

There may be slight cosmetic differences between the look of Retail Internet Banking across the various browser platforms that are supported. This is a function of the different methods and standards that each browser supports and / or how the individual browsers have been coded. It should be noted that the core functionality of Retail Internet Banking is consistent across all supported browsers, except for the ability to rotate a check images, which is only supported in Microsoft Internet Explorer (IE).

- Microsoft Internet Explorer (IE) for Windows version 7.0 or higher, including IE 8.0 and higher.
- Mozilla Firefox version 2.0 or higher, version 3.0 or higher.
- Opera version 9.0 or higher
- Mozilla Camino version 1.0.3 or higher
- Apple Safari version 1.2.1 or higher (Apple OSX only. iPhone not supported)
- Google Chrome, version 1.0 or higher

Operating System and Hardware Platforms

The end-user must meet the Operating System and Hardware requirements stated by the developers of each supported browser. Browsers are tested and qualified with Retail Internet Banking, not the Operating Systems or hardware platforms they run on. That said, only Microsoft and Apple operating systems are supported at this time. While we rely on the developers of the browsers to ensure uniform look, feel, and functionality across all supported hardware and software platforms for each specific browser, there are differences between each platform.

****Linux Specific**

Adobe Flash Player 10.0.22.87 is the current version as of this writing. To avoid incompatibilities with Mozilla Firefox based browsers on Linux and previous versions of Flash, ensure that you have the most current version of Flash is installed.

Adobe Flash Player Requirements

Adobe Flash Player does not support 64-bit Operating Systems at the time of this writing, and attempting to install a 32-bit version of Adobe Flash Player on a 64-bit Operating System with a wrapper is not supported.

Internet Service Providers

Internet Service Providers, ISPs, simply provide access to the Internet for their clients and are not differentiated as far as support for Retail Internet Banking is concerned. Examples include: cable companies such as Time Warner or ComCast, phone companies such as AT&T or TDS, and traditional ISPs such as AOL and NetZero.

Unsupported Browsers

Any browser that is not in the Supported Browser list is unsupported. That does not mean that it will not work with Retail Internet Banking, just that it is not specifically tested to ensure that it does fully function with Retail Internet Banking.

- America Online, AOL. It is worthy to note that AOL as an Internet Service Provider, ISP, is no different than any other ISP, which is to say that they provide Internet access to end-users. However, even though AOL is one of the largest ISPs, the fact that the application has a built in browser is why it is specifically mentioned in the Unsupported Browser list.
 - AOL for the PC uses a version of the IE engine as its internal browser. If the end-user is using the most current version of AOL, the internal AOL browser should work but is still not directly supported. Ideally, an AOL user should use a browser external to AOL which is in the Supported Browsers list to access Retail Internet Banking. This means the end user would utilize the AOL application to gain access, i.e. 'sign on', to the Internet, but then launch another browser to surf the Internet.
 - AOL for the Mac is based on an early version of the Netscape Gecko engine. However, as of AOL version 10.3.6 the Gecko engine was quite old. The user should use a browser external to AOL which is in the Supported bBrowsers list to access Retail Internet Banking. This means the end user would utilize the AOL application to gain access, i.e. 'sign on', to the Internet, but then launch another browser to surf the Internet.

Browser Settings

The following list contains the minimum settings for a browser to access Retail Internet Banking.

- First party cookies must be allowed.
- First party images must be allowed.
- Pop-up blockers inherent to each supported browser are allowed. Some links within Retail Internet Banking spawn a new browser window and could be blocked by a 3rd party pop-up blocker. Thus, 3rd party pop-up blockers are not supported.
- SSL connections must be allowed (HTTPS://) for a minimum of 128bit strength.
- JavaScript enabled and the running of active scripts allowed.
- Iframes allowed.
- Minimum browser resolution of 800x600

Troubleshooting Add-ons and Toolbars

Occasionally, when normal troubleshooting steps fail to uncover the root cause of a particular problem with Retail Internet Banking or a component thereof, it becomes necessary to disable add-ons and toolbars. The functions of these add-ons, such as pop-up blocking, blacklisting, cookie management, and the like, may compound, obscure, or be the cause of the particular problem a user is having. One easy way to prove or disprove that a particular browser is the cause of the problem is to use another supported browser to determine if the problem occurs in that browser as well. If it does not, and after normal troubleshooting steps have been exhausted, follow the steps below to disable add-ons:

Internet Explorer 7.0, Internet Explorer 8.0, and later:

Method 1, if an Internet Explorer icon is present on the desktop:

1. Right-click on the icon, and select “Start without add-ons”
2. Ensure that you see a “Internet Explorer is currently running with add-ons” message

Method 2, if there is not an Internet Explorer icon on the desktop or the “Start without add-ons” option is not present.

1. Press Windows Key-R
2. In the textbox, type the following (including quotes):
"C:\Program Files\Internet Explorer\iexplore.exe" -extoff
3. Ensure that you see a “Internet Explorer is currently running with add-ons” message

Note: This will start a 64-bit version of IE in 64-bit Vista or XP, and a 32-bit version of IE in 32-bit Vista or XP.

Method 3, to selectively disable Add-ons

1. Start Internet Explorer as normal
2. Select Tools->Manage Add-ons->Enable or Disable Add-ons
3. Make sure the “Show” dropdown is set to “Add-ons that have been used by Internet Explorer”
4. Select each Add-on to modify and click “Disable” below
5. Click “OK” on the warning box
6. Repeat for each Add-on to be disabled
7. Click “OK”
8. Restart Internet Explorer

Firefox 2.0 and later:

1. Start Firefox
2. Go to Tools->Add-ons
3. Click “Disable” on each Add-on to modify
4. Close the window

5. Restart Firefox

Once all add-ons and toolbars have been disabled, attempt the steps within Retail Internet Banking that caused the issue to determine if the outcome changes. If the problem is resolved, restore each add-on one at a time and repeat the test until the problem add-on is identified.

Layered Authentication Support

If an end-user is Layered Authentication enabled, this section supersedes the requirements of Retail Internet Banking.

Browser Support

The browser requirements are the same for Layered Authentication and Retail Internet Banking.

- While Internet Explorer for the Mac may have worked with Retail Internet Banking in the past, even though it was unsupported, it will not function with Layered Authentication. The end-user must use one of the other mentioned supported browsers.
- While multiple browsers may be supported for any given computer; generally, only one browser may be used to register a computer as a personal computer within Layered Authentication. That is to say, the initial browser that an end-user uses to register a computer will be the only browser on the computer that Layered Authentication will actually register. Using a different browser will require successfully completing the Layered Authentication challenge upon every login.

Setting a Trusted Site (Internet Explorer)

Trusted sites generally have lessened security restrictions because it involves a user interaction to make a site trusted, and should allow a user to log into Layered Authentication by default. Also, by logically grouping the Retail Internet Banking site into the Trusted Sites zone, it is easier to adjust security settings without impacting the browsing experience or adjusting security for all other web sites in the Internet zone.

To set a trusted site to Retail Internet Banking, perform the following:

1. Go to Tools -> Internet Options -> Security
2. Under “Select a Web content zone to specify its security settings:”, click on the Trusted Sites icon
3. Check the “Security level for this zone”
 - For IE 7 and later, **Medium-High** is the highest security level that will still allow the user to log into Layered Authentication.
4. Click on the “Sites” button
5. Enter **https://*.secureinternetbank.com** into “Add this Web site to the zone:”, and ensure the “Require server verification (https:) for all sites in this zone” is checked, then click “Add”, then “OK”

To ensure you have properly added the site to the Trusted Sites zone, look in the IE status bar at the bottom of the browser window after you have navigated to the Retail Internet Banking site. On the right side of the status bar you should find a green circle with a check in it (or simply a green check if IE 7) followed by the text "Trusted Sites". If you see a small world on the right side of the status bar followed by the text "Internet", the site was not correctly added to the Trust Sites zone. Please verify the previous procedures for Setting a Trusted Site.

If you continue to experience problems with Layered Authentication after making these modifications, check the settings mentioned below. **After adding the website to the Trusted Sites zone, any Browser Setting mentioned below will now need to be made on the Trusted Sites zone, not the Internet zone.**

Browser Settings (Internet Explorer)

Within Internet Explorer, two settings must be enabled for Layered Authentication to function. These settings can be viewed and modified under Tools, in IE 7 and IE 8 it is on the far right of the screen, under the address bar by default.

Active Scripting:

1. Tools -> Internet Options -> Security
2. Select the desired zone, Trusted Sites if you have followed the steps in "Setting a Trusted Site", Internet if not
3. Next click Custom Level -> Scripting -> Active Scripting
 - This value must be **Enable**.

*This should already be true, otherwise the JavaScript menus will not render within Retail Internet Banking

Binary and script behaviors:

1. Tools -> Internet Options -> Security
2. Select the desired zone, Trusted Sites if you have followed the steps in "Setting a Trusted Site", Internet if not
3. Next click Custom Level -> ActiveX controls and plug-ins -> Binary and script behaviors
 - This value must be **Enable**.

If this is not enabled:

- A user will be able to enroll into Layered Authentication, and then login to Retail Internet Banking afterwards
- After logging out of Retail Internet Banking, when a Layered Authentication enabled user attempts to login to Retail Internet Banking again, they will receive a "Unable to process request" error message

In addition, if Security Level is set to High without making the fine-grained modifications mentioned above, Layered Authentication will not work because it turns off Active Scripting and Binary and script behaviors. A user may be able to modify their Internet Explorer security settings to Medium-High in IE7.0 and IE 8.0. These settings can be changed at:

1. Tools -> Internet Options -> Security

2. Select the desired zone, Trusted Sites if you have followed the steps in "Setting a Trusted Site", Internet if not
3. Next click Custom Level -> Reset Custom Settings, and then click Reset, OK, then Apply

-Or-

1. Tools -> Internet Options -> Security
2. Select the desired zone, Trusted Sites if you have followed the steps in "Setting a Trusted Site", Internet if not
3. Next click Default Level, then adjust the slider bar to the desired security level, then click Apply

Changing these settings will adjust more settings than just the two required, so this would be a suggestion for a home user who is not comfortable making fine-grained adjustments.

Security Objects

Layered Authentication will place a browser cookie and a Flash object (if Flash is installed) on the computer accessing Retail Internet Banking. Layered Authentication uses these objects, in part, in determining whether or not to challenge the end-user from a given computer.

- If Flash is installed on the computer
 - If both the cookie and flash object that were placed on a computer that has previously accessed Retail Internet Banking and has been registered are not available when a user next logs into Retail Internet Banking, the end-user will be challenged.
 - If the end-user access Retail Internet Banking from multiple browsers on the same computer the end-user may be challenged upon each login, regardless of computer registration within Layered Authentication.
- If Flash is NOT installed on the computer
 - If the cookie that was placed on a computer that has previously accessed Retail Internet Banking is not available when a user next logs into Retail Internet Banking the end-user will be challenged. The end-user may have a cookie manager program that regularly removes their cookies or the end-user may manually delete their cookies to cause this situation.

Clearing cookies and cache is a standard troubleshooting practice and can still be used with the understanding that the user may be challenged upon next login. Note, that clearing cookies and cache within IE does not delete the Flash object.

You can test for Flash functionality, and currently installed version and download the Flash player from: <http://www.adobe.com/products/flash/about/> Flash version 6.0 and greater is supported, although not required.

Deleting the Flash FSO Object

Occasionally, it becomes necessary to delete the Flash Shared Object (FSO), which is a separate function from deleting cookies within a browser. The most common situation for deleting the Flash object is when an end-user cannot register a computer or if an end-user is being challenged after a browser upgrade. To delete the FSO, perform the following:

Option 1 (Platform Independent):

1. Navigate to the Adobe Flash Player Settings Manager Website:
 - http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html
2. In the Table of Contents to the left, navigate to the “Website Privacy Settings Panel”
3. In the panel to the right there will be a list of “Visited Websites”. Search for “secureinternetbank.com”, select it, then click the “Delete Website” button, then click the “Confirm” button to remove the Flash Object.

After deleting the FSO object, the end user must delete all cookies in their browser(s). The end user will be challenged by Layered Authentication upon next login. After successfully completing the Layered Authentication challenge, the end-user can register the computer as a personal computer to avoid further Layered Authentication challenges.