

Configuring your Web Browser and Using WebISO

This document contains the following sections:

- [Overview](#)
- [WebISO](#)
- [Configure Internet Explorer](#)
- [Configure Firefox](#)
- [Configure Safari](#)
- [Troubleshooting WebISO Problems](#)

For information related to this topic refer to:

- [WebISO \(http://www.cmu.edu/computing/web/webiso.html\)](http://www.cmu.edu/computing/web/webiso.html)
- [Web Browsers: Statement of Support \(http://www.cmu.edu/computing/doc/software/browser-support/index.html\)](http://www.cmu.edu/computing/doc/software/browser-support/index.html)

Last Updated: 8/26/09

Overview

To be compatible with the Carnegie Mellon Web Portal and services provided by Administrative Computing, Computing Services and the Office of Technology for Education, your web browser must meet the following requirements:

- The browser must be configured to accept cookies.
- The browser must be configured to run JavaScript.
- The browser must be capable of 128-bit encryption.

Even if you are using a supported browser, you will not be able to access ALL of the services above if you have disabled JavaScript or cookies, or if you are using less than 40-bit encryption. See the appropriate steps for configuring your web browser.

Last Updated: 8/27/09

About WebISO

WebISO is the means by which Carnegie Mellon web services securely verify the identity of Carnegie Mellon users. WebISO does not require installation of a plug-in or any other software. However, your browser must:

- be configured to accept cookies
- have the Carnegie Mellon server certificates installed (see [Server Certificates \(http://www.cmu.edu/computing/software/all/certs/download.html\)](http://www.cmu.edu/computing/software/all/certs/download.html))

The first time you visit a WebISO-enabled service, you will be redirected to the login server at <http://webiso.andrew.cmu.edu> (<http://webiso.andrew.cmu.edu/>).

Carnegie Mellon

WebISO Secure Login

The resource you requested requires you to authenticate.

User ID @

Password

Warning: This web page, served through <https://webiso.andrew.cmu.edu/> is requesting your UserID and password. If you have any doubts as to the legitimacy of this page doing so, please **look for <https://webiso.andrew.cmu.edu/> in the URL** before you enter your user ID and password. If you think that this page should not be requesting your User ID and password, report it to advisor@andrew.cmu.edu and be sure to include the URL.

Carnegie Mellon Certificates: Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, you should [install the Carnegie Mellon Root Certificates in your browser.](#)

About this service. WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [\[more\]](#)

Your browser will be automatically returned to your original destination once you establish your credentials by entering your userID and password. Andrew, CS, and ECE accounts are supported, though some services only accept **Andrew** userIDs.

IMPORTANT! Until you close your browser OR twelve (12) hours have passed, your browser will have access to all WebISO-protected resources without the need to answer the user/password challenge. Please keep this in mind when you are using WebISO - especially when using a computer other than your own! Note that with some web browsers (e.g., Internet Explorer) you must close *all* web browsers to end your WebISO session.

Last Updated: 8/5/08

Configure Internet Explorer

Follow these steps to properly configure Internet Explorer:

Internet Explorer 7.0+ for Windows

Install the Server Certificate

1. If you haven't already done so, visit the [Server Certificate](http://www.cmu.edu/computing/software/all/certs/download.html) (<http://www.cmu.edu/computing/software/all/certs/download.html>) web page and download the appropriate certificate. Follow the [Certificate Installation instructions](http://www.cmu.edu/computing/software/all/certs/installation.html) (<http://www.cmu.edu/computing/software/all/certs/installation.html>) for Internet Explorer.
2. Launch Internet Explorer.
3. Select **Tools > Internet Options**.
4. The Internet Options window appears; select the **General** tab.
5. In the Browsing history section, click **Settings**.
6. The Temporary Internet Files and History Settings dialog box appears. Under **Check for newer versions of stored pages**, select the radio button for **Every time I visit the web page**. Click **OK** to close the tab.
7. Select the **Privacy** tab and set the slider bar to **Medium** to enable cookies.
8. Continue with the [Configure Active Scripting](#) steps below.

Internet Explorer 6.0 for Windows

Install the Server Certificate

1. If you haven't already done so, visit the [Server Certificate](http://www.cmu.edu/computing/software/all/certs/download.html) (<http://www.cmu.edu/computing/software/all/certs/download.html>) web page to download the appropriate certificate. Follow the [Certificate Installation instructions](http://www.cmu.edu/computing/software/all/certs/installation.html) (<http://www.cmu.edu/computing/software/all/certs/installation.html>) for Internet Explorer.
2. Launch Internet Explorer.
3. Select **Tools > Internet Options** and then select the **General** tab.
4. In the Temporary Internet Files section, click **Settings**.
5. Under **Check for newer versions of stored pages**, select the radio button for **Every visit to the page**.
6. Click **OK** to close the Settings tab.
7. Select the **Privacy** tab, then set the slider bar to **medium** to enable cookies.
8. Continue with the [Configure Active Scripting](#) steps below.

Configure Active Scripting (IE 6, 7 and 8)

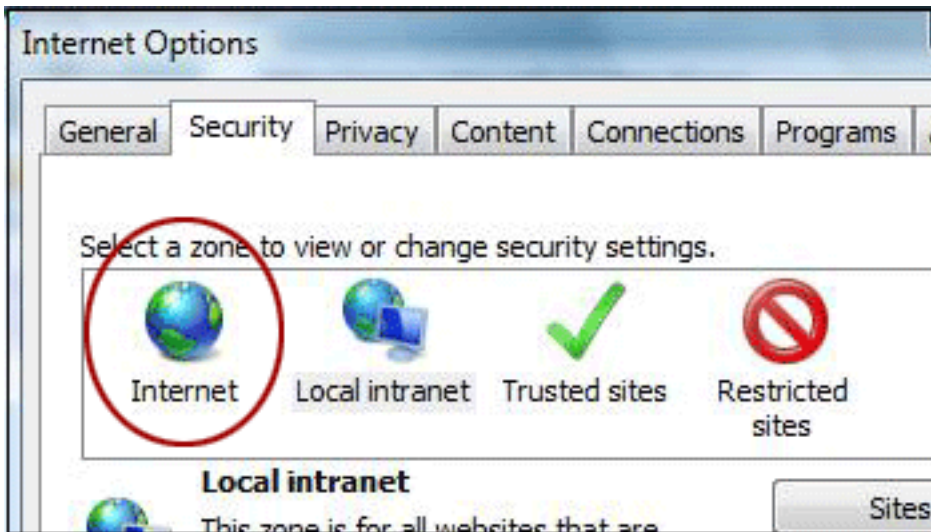
Many web sites (e.g., e-commerce or banking sites) use Active Scripting to provide additional functionality; however, you may need to protect yourself from some malicious sites that include Active X Exploits.

Follow the steps below to configure Internet Explorer to prompt you ANYTIME you visit a web page that uses Active Scripting. You may be prompted multiple times per web page if multiple scripts are used. Each time you are prompted:

- Answer Yes if you trust the site; this will allow the Active Scripting to run.
- Answer No if you don't trust the site; the page content will display without the scripting.

Follow these steps to configure Internet Explorer to prompt before allowing Active Scripting:

1. Select **Tools > Internet Options** (or **Options** on IE 6.0).
2. Select the **Security** tab.
3. Click **Internet** and then select **Custom Level...**



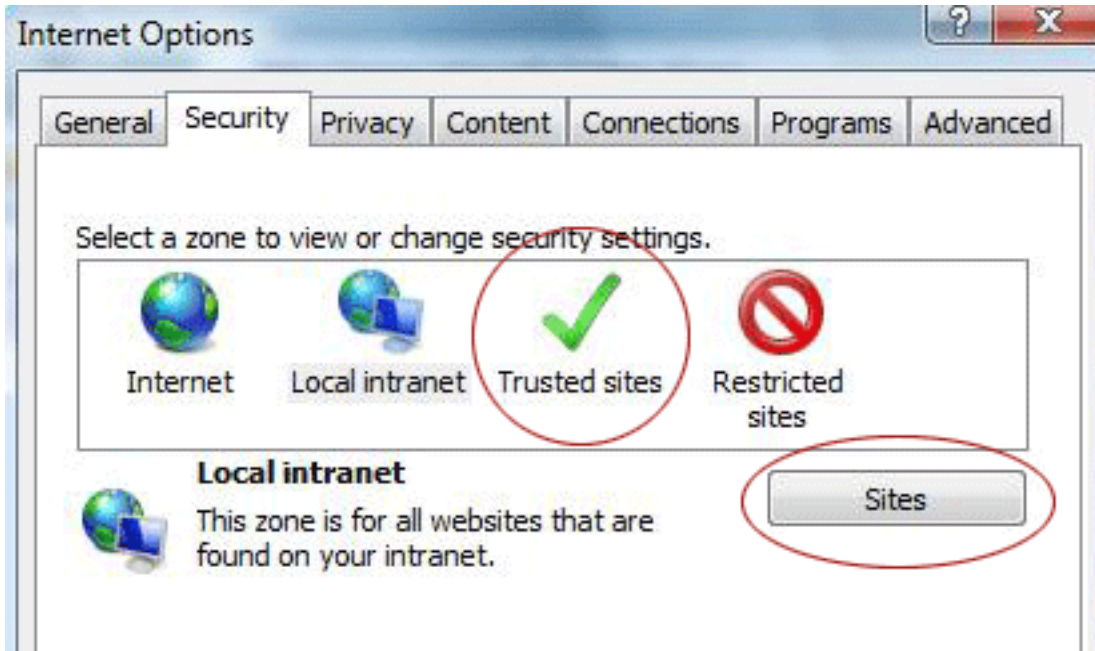
4. Scroll down to **Active Scripting** (below the *Scripting* heading) near the bottom of the list.
5. Select the radio button to **Prompt**. Click **OK**.
6. Click **Yes** to accept the warning message.
7. Select **Local Intranet**, and then select **Custom Level**.



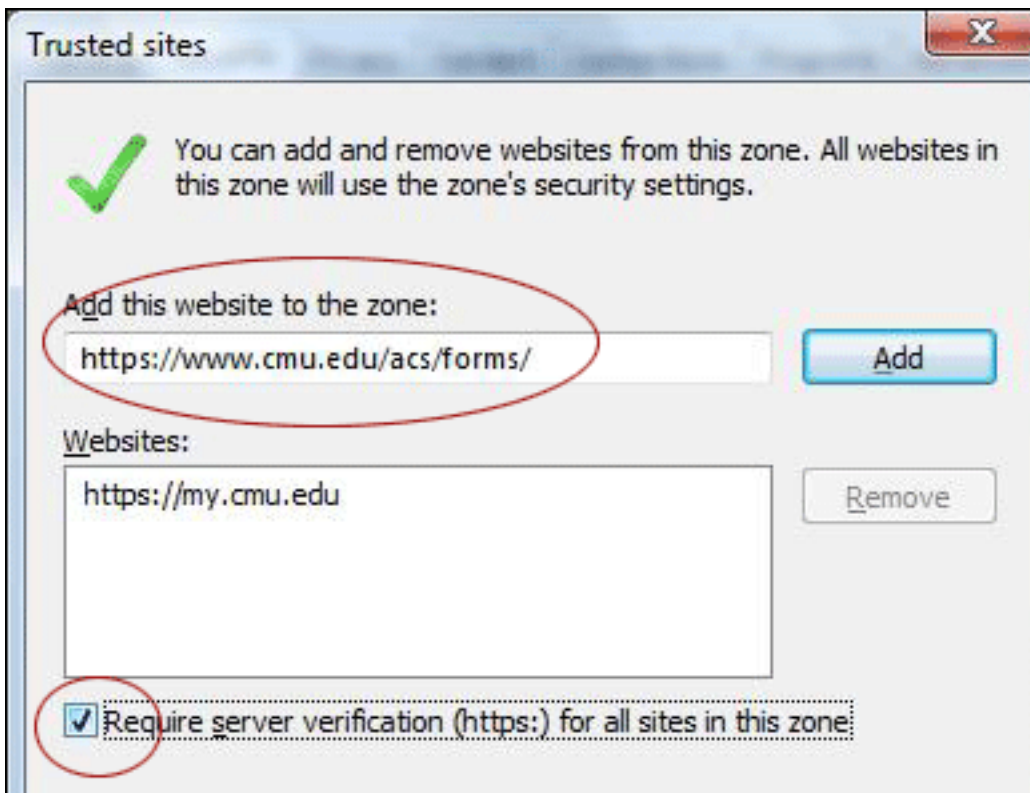
8. Scroll down to **Active Scripting** (below the *Scripting* heading) near the bottom of the list.
9. Select the radio button to **Prompt**. Click **OK**.
10. Click **OK** close.

To avoid being prompted for sites that you trust, you can add them to the Trusted Sites zone. Follow these steps:

1. Select **Tools > Internet Options** (or **Options** on IE 6.0) and then select the **Security** tab.
2. Select **Trusted Sites** and then click **Sites**.



3. If you want to add sites that do not require an encrypted channel (i.e., https:), **deselect** the checkbox for "**Require server verification (https:) for all sites in this zone**".
4. Enter the URL of a site that you trust in the "**Add this Web site to the zone**" text box, and then click **Add**. The URL appears in the **Websites** list.



5. Repeat these **steps 2-4** for each site that you want to add to the zone.
6. Click **OK** to accept the changes and close any open dialog boxes.

Last Updated: 8/26/09

Configure Mozilla Firefox 3.0+

Follow these steps to properly configure Firefox:

1. Visit the [Server Certificate](http://www.cmu.edu/computing/software/all/certs/download.html) (<http://www.cmu.edu/computing/software/all/certs/download.html>) web page and download the appropriate certificate. Follow the [Certificate Installation instructions](http://www.cmu.edu/computing/software/all/certs/installation.html) (<http://www.cmu.edu/computing/software/all/certs/installation.html>) for Firefox.
2. By default Firefox is configured correctly as downloaded. If you have disabled cookies or JavaScript, you will need to re-enable them; to do so perform the steps below:

Enable JavaScript and Cookies

Windows

1. Launch Firefox.
2. Select **Tools > Options** and click **Privacy**.
3. Make sure that the **Accept cookies from sites** checkbox is selected.
4. Select **Content**. Make sure that **Enable JavaScript** is selected.
5. Close the Options window.

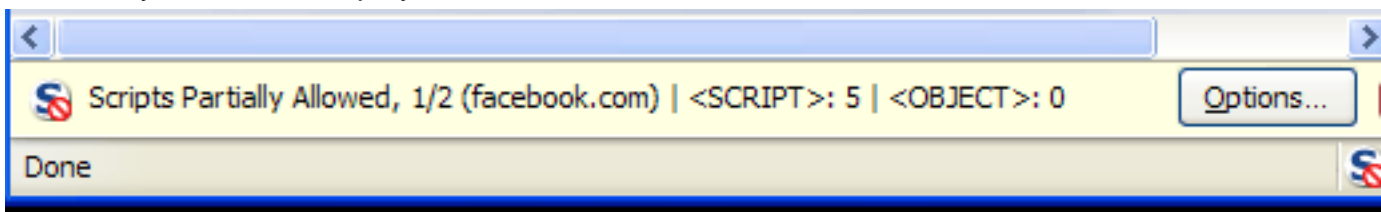
Mac

1. Launch Firefox.
2. Select **Firefox > Preferences** and click **Privacy**.
3. In the Cookies section. Make sure that **Accept cookies from sites** is selected.
4. Select **Content**. Make sure that **Enable JavaScript** is selected.
5. Close the Options window.

Install Firefox's NoScript Add-on (Optional)

To add an extra level of protection to your browsing, follow these steps to install Firefox's NoScript Add-on:

1. Using Firefox as your browser, visit the [NoScript Add-on](https://addons.mozilla.org/en-US/firefox/addon/722) (<https://addons.mozilla.org/en-US/firefox/addon/722>) web page click the **Download Now** button.
2. The next time you run Firefox, you'll notice the NoScript icon in the lower right corner of your screen display:



3. To allow scripting on a page that you trust, click the **Options** button and select **Allow all this page** or **Temporarily allow all this page**.



Last Updated: 8/26/09

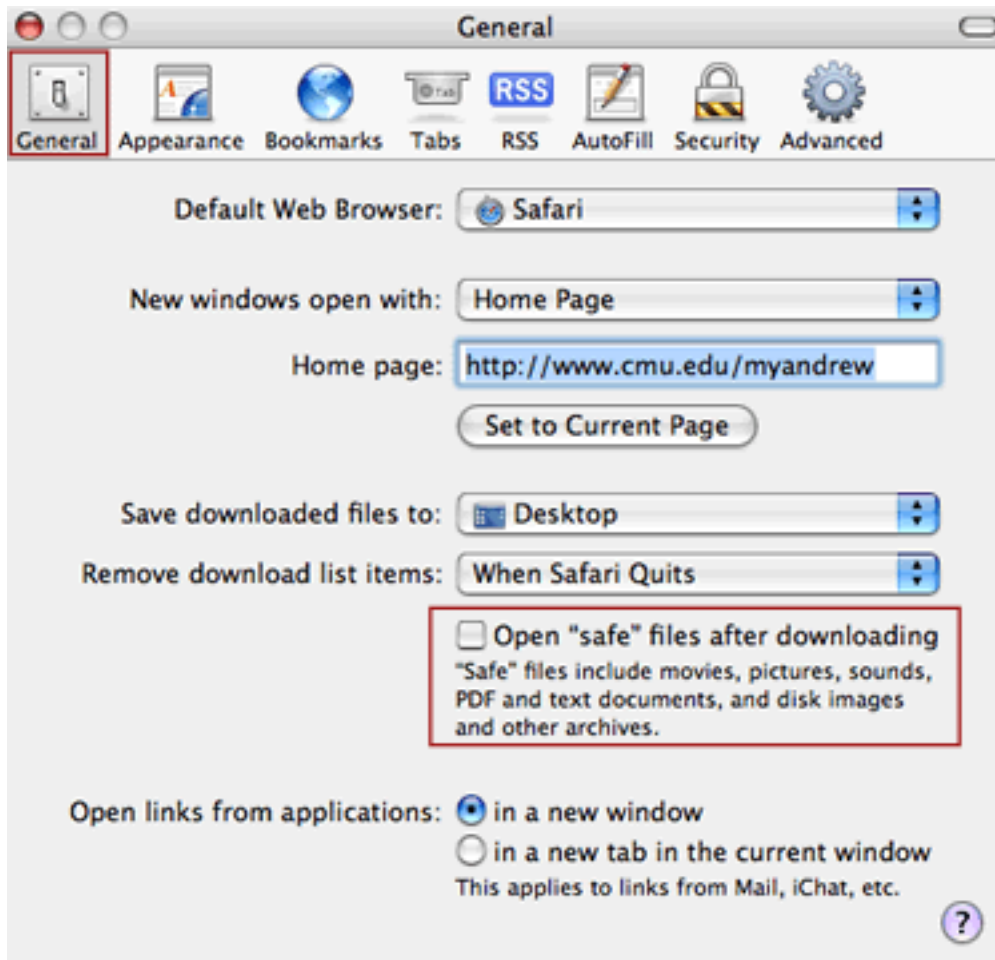
Configuring Safari 4.0+

The steps below will assist you in properly configuring Safari. First, you will need to install the Server Certificate for Safari and then ensure JavaScript is enabled.

1. If you haven't already done so, visit the [Server Certificate](http://www.cmu.edu/computing/software/all/certs/download.html) (<http://www.cmu.edu/computing/software/all/certs/download.html>) web page and download the appropriate certificate. Follow the [Certificate Installation instructions](http://www.cmu.edu/computing/software/all/certs/installation.html) (<http://www.cmu.edu/computing/software/all/certs/installation.html>) for Safari.
2. Launch Safari.
3. Select **Safari > Preferences** and then select **Security**.
4. In the Web Content section, be sure that **Enable plug-ins**, **Enable Java** and **Enable JavaScript** are checked.
5. In the Accept Cookies section, select **Only from sites you navigate to**.
6. Select (check) **Ask before sending a non-secure form to a secure website**.



7. Select the **General** tab and UNCHECK **Open "safe" files after downloading**.



8. Close the General window to save changes.

Last Updated: 8/27/09

WebISO Troubleshooting

Follow steps in this section if you experience problems authenticating at the [WebISO login page \(http://webiso.andrew.cmu.edu\)](http://webiso.andrew.cmu.edu) .

1. Make sure you have configured your web browser properly.
2. If you never changed your [Andrew password \(http://www.cmu.edu/computing/doc/accounts/passwords/change.html\)](http://www.cmu.edu/computing/doc/accounts/passwords/change.html) OR have not changed it in a long time, change it now using the COMPUTING tab of the [Carnegie Mellon Web Portal \(https://my.cmu.edu\)](https://my.cmu.edu) .
3. Check your computer's clock to make sure your machine's time, time zone, and Daylight Savings Time (*if applicable*) are set properly for your geographic region.
4. Quit and restart your browser. Try logging in to WebISO again.

Following the four steps above solves the majority of WebISO problems. If you continue to have problems, read the following:

Problem:

I can't log in to WebISO with my Andrew account; however, I can read my email and do other things with my Andrew account.

Solution:

Your Andrew account password has either never changed or hasn't been changed in a very long time. Changing your password may resolve this problem. For help with changing your password, see the [Managing Your Andrew Account and Password \(http://www.cmu.edu/computing/doc/accounts/passwords/index.html\)](http://www.cmu.edu/computing/doc/accounts/passwords/index.html) document.

Problem:

I'm using a Linksys wireless AP router and can't get into WebISO.

Solution:

Make sure you have the latest router firmware installed.

Problem:

When I try logging into WebISO, I get the following error message:

```
Base64Decode error '800a0001'
```

```
Bad Base64 string.
```

```
/bin/n_libBase64.asp, line 45
```

Solution:

You may have a piece of spyware installed called "Commonname" which is interfering with your browser. Select **Start > Control Panel > Add/Remove** programs, remove "Commonname," and then restart your computer.

Problem:

I have two Andrew accounts and I can't access my Blackboard courses.

Solution: Contact the [Computing Services Help Center \(http://www.cmu.edu/computing/repair/help-center.html\)](http://www.cmu.edu/computing/repair/help-center.html) 412-268-HELP (4357). We can merge the two accounts together. Changes may take a couple of days to be reflected in the Student Information System and in Blackboard which may cause interruption of access to your Blackboard courses.

Problem:

I am accessing WebISO from behind a firewall.

Solution:

Since every Intranet and firewall configuration is different and beyond our control, we are unable to provide technical assistance to users accessing WebISO server from behind a firewall. We can, however, provide basic information about the resources used by WebISO. Minimally, in order to use these services, the following traffic must be permitted for machines that you will be using in your organization:

Ports 80 (HTTP) and 443 (HTTPS) should be permitted for all machines in the CMU.EDU domain. There are many machines being utilized within the WebISO system, and more will be added in the future. Allowing HTTP and HTTPS traffic to pass to all machines within CMU.EDU will greatly reduce the potential for problems.

Last Updated: 5/21/09