



COI-SMART
Desktop Troubleshooting Guide

September 1, 2016

Table of Contents

DOCUMENT PURPOSE	3
1. BROWSER REQUIREMENTS	4
2. POP-UP BLOCKERS.....	4
3. TLS 1.0.....	5
4. JAVASCRIPT	5
5. ACROBAT READER.....	6
6. STORED PAGES.....	6
7. URL RE-WRITING.....	7
8. SINGLE SIGN ON.....	7
9. FORGOTTEN PASSWORD.....	8
10. SESSION TIMEOUT	8
11. VIRUS SCAN	9
12. PROXY SERVERS	9

Document Purpose

COI-SMART is offered as an ASP-hosted, web-based Internet solution. The Administrator, Reviewer, and Respondent interfaces are accessed via a web browser on the same URL / site.

The purpose of this document is to assist the COI-SMART Administrator and client IT teams in troubleshooting desktop- and browser- related issues. Some of the potential issues include, but not limited to:

- Browser errors
- System latency
- Inability to log into COI-SMART
- Forgotten password



The system does not require any non-standard or proprietary software in order to run. All client access is thin using a supported web browser. The application content is delivered to the desktop browser as HTML and client-side JavaScript.

1. Browser Requirements

COI-SMART supports the following browsers:

- Microsoft Internet Explorer version 11
- Apple Safari
- Google Chrome
- Mozilla Firefox

To check your version, proceed as follows:

Internet Explorer	<ol style="list-style-type: none"> 1. On the menu bar, click on Help. 2. Click on About Internet Explorer.
Apple Safari	<ol style="list-style-type: none"> 1. Click on Safari in your Safari menu, located at the top of your screen. 2. A drop-down menu will appear. Choose the option labeled About Safari.
Google Chrome	On the address bar, type: chrome://chrome
Mozilla Firefox	<ol style="list-style-type: none"> 1. Click the menu button  2. Click help  and select About Firefox.

2. Pop-up Blockers

COI-SMART recommends that pop-up blockers are disabled. The application may be launched from another website by clicking on a link, which open another window or tab. Within the application, the user may click links to documents, which opens another window or tab.

To check pop-up blockers, proceed as follows:

Internet Explorer	<ol style="list-style-type: none"> 1. Click on the Tools button, point to Pop-up Blocker. 2. If Turn on Pop-up Blocker is bolded, then it is off. Click Close. 3. If Pop-up Blocker Settings is bolded, then lick it. Add *.coi-smart.com to the list of websites allowed. Note: If you arrive at *.coi-smart.com from another website, add that website to the list as well.
Apple Safari	<ol style="list-style-type: none"> 1. Click on Safari in your Safari menu, located at the top of your screen. 2. A drop-down menu will appear. Choose the option labeled Preferences. 3. Click on the Security tab 4. If Block pop-up windows is enabled, uncheck it
Google Chrome	1. On the address bar, type in the following: chrome://settings/content

	<ol style="list-style-type: none"> 2. Go to the section Pop-ups. 3. If Allow all sites to show pop-ups is checked, click Done. 4. Otherwise, click Manage exceptions. Add *.coi-smart.com to the allowed list, then click Done. Note: if you arrive at *.coi-smart.com from another website, add that website to the list as well.
Mozilla Firefox	<ol style="list-style-type: none"> 1. On the address bar, type about:preferences 2. Select Content from the navigation bar 3. If Block pop-up windows is selected, close the browser 4. Otherwise, click Exceptions. Add *.coi-smart.com to the allowed list. Note: if you arrive at *.coi-smart.com from another website, add that website to the list as well.

3. TLS 1.0

COI-SMART negotiates HTTPS connections using TLS 1.1 and TLS 1.2. It does not support the weaker SSL 3.0 and TLS 1.0 protocols.

Unless the user changed the browser defaults, TLS 1.1 and/or TLS 1.2 should be enabled. Otherwise, the message displays (in IE): “Internet Explorer cannot display the webpage”.

To check if the browser is enabled for TLS 1.1 and/or TLS 1.2, go to (from that browser): <https://www.ssllabs.com/ssltest/viewMyClient.html>. In the section Protocol Features, make sure TLS 1.1 and/or TLS 1.2 is Yes.

4. Javascript

COI-SMART uses JavaScript for browser controls. By default, all browsers enable scripting upon installation. To check if the settings were changed, proceed as follows:

Internet Explorer	<ol style="list-style-type: none"> 1. Click on the Tool bar, and select Internet Options 2. Click on the Security tab and select Internet. 3. Select Custom Level, and scroll down to the Scripting section. 4. Under Active scripting, check Enable.
Apple Safari	<ol style="list-style-type: none"> 1. Click on Safari in your Safari menu, located at the top of your screen. 2. A drop-down menu will appear. Choose the option labeled Preferences. 3. Click on the Security tab 4. Check Enable JavaScript
Google Chrome	<ol style="list-style-type: none"> 1. On the address bar, type: chrome://settings 2. At the bottom of the page, click on "Show advanced settings" 3. Under the Privacy section, click on Content Settings. Under the Javascript section, check Allow all sites to run JavaScript (recommended).
Mozilla Firefox	<ol style="list-style-type: none"> 1. On the address bar, type about:config 2. On the search bar, type javascript.enabled 3. If javascript.enabled is false, double-click to set to true

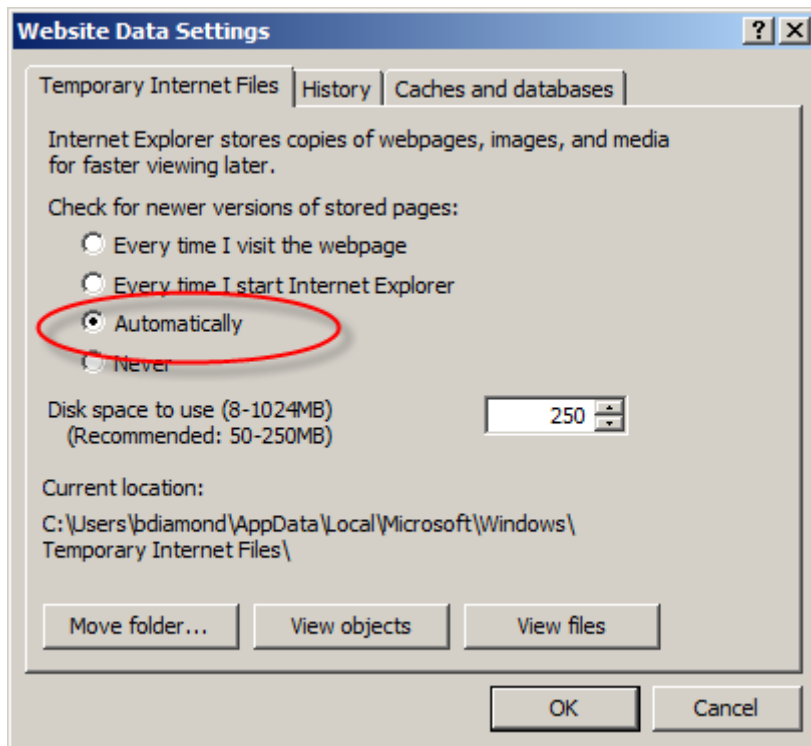
5. Acrobat Reader

COI-SMART generates transcripts of disclosures in PDF format. Check if Adobe Acrobat Reader is installed and properly configured as a plug-in for the browser.

6. Stored Pages

In Internet Explorer, COI-SMART runs exponentially faster if web pages and associated resources are not downloaded every time a new page is opened. (Note: page *data* is downloaded every time regardless of the setting).

In Internet Explorer, click Tools from the menu bar and select Internet Options. In the General Tab, go to the section for "Browsing history" and click Settings. Ensure that the "Check for newer versions of stored pages" section is set to "Automatically".



7. URL Re-writing

In some offices, users access the Internet on remote desktop farms. If using Citrix Netscaler Access Gateway, for example, the built-in URL re-writing function masks the COI-SMART URLs to re-direct incorrectly or not at all.

If your institution uses remote desktop (i.e. Citrix) and the pages are not properly redirecting, add an exception to prevent the URL from being re-written automatically. For example, from the password page, *.coi-smart.com/login.php should automatically redirect to the home page, *.coi-smart.com/main.php. If this does not work, you may need to add a re-write exception rule.

8. Single Sign On

COI-SMART supports Single Sign On (SSO) over Shibboleth/SAML2, in addition to a custom solution. With Shibboleth/SAML2, the client starts with clicking on a link to COI-SMART, e.g. <client>.coi-smart.com. COI-SMART re-directs the user to the organization's IDP. Upon

successful authentication, the user is re-directed back to <client>.coi-smart.com, bypassing the COI-SMART Login Page.

Non-registered users

SSO will fail if the User ID is inactive or does not exist in COI-SMART. When this happens, the application will display an error:

“Your account is inactive or does not exist in COI-SMART. Please close this browser and contact your local manager.”

Registered users

If the COI-SMART page does not load on the local network(s), check if COI-SMART is required to be added to internal DNS and/or the proxy.pac configuration. Some clients may be restricting redirection from their IDP to a DOT COM.

9. Forgotten Password

For non-Single Sign On (SSO) access to COI-SMART, the application provides authentication via a Login page. If a user forgets their password any time after they set it, the user or Administrator can send a link to the user’s email so they can reset it. On the Login page, select the “Forgot Login ID or Password” link and type in the user’s email address.

Passwords must:

- Have between 6-18 characters
- Contain at least 1 letter
- Contain at least 1 number
- Contain at least 1 special character (examples: ! @ # \$ % ^ & * () ~ _ + - =)

10. Session Timeout

Reports

COI-SMART reports feature a web front-end for execution and download. When initiated, the reports run in the background while the application waits for results. In the meantime, the application is locked and the session is inactive.

For voluminous reports, the session may time out (typically after 15 minutes) before the report completes:

- In IE, the following message appears: “This page can’t be displayed”.
- In Chrome, the following message appears: “No data received”.

To allow for long wait times, increase the timeout setting(s) on the network user’s firewall. Contact the IT Department for assistance.

Single Sign On

With SSO using SAML2, the client is the Identify Provider (IDP) whereas COI-SMART is the Service Provider (SP). Once the authentication is made, the SSO connection sits idle. The session is alive until the user logs out of COI-SMART and redirected back to the IDP.

The SP timeout is 7,200 seconds or 120 minutes. Users who experience AJAX errors after a shorter period (e.g. 5 minutes) may have been timed out by the IDP sooner. In this case, the IDP should keep the login session active until the user closes the browser or redirected back to a logout page.

11. Virus Scan

On occasion, real-time virus scans on web pages will cause some latency issues when there is special handling. For example, when virus-scans are enabled and there exists an exception for the COI-SMART website or domain, the browser may actually load pages slower.

Sometimes, the anti-virus software performs URL filtering. For example, *McAfee* Web Gateway blocks web pages if the content of the page (e.g. email address, hyperlinks) includes unauthorized URLs or domains. The filter is usually based on categorization, e.g. Parked Domain, or Reputation, e.g. Unverified.

To check the URL or domain, go to *McAfee’s* Real-Time Database: www.trustedsource.org.

12. Proxy Servers

On occasion, a user is set up to use a different configuration script than other users depending on the Group policy. If the configuration script routes the user to a different network that restricts internet sites, the following message displays:

In Firefox: “Unable to connect... If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.”

The Compliance Department should work with IT to add an exemption to COI-SMART and/or reconcile the Group policy of all COI-SMART users.

<This page intentionally left blank>