CalREDIE System Requirements

Contents

Section 1: Browser Settings

The following browser settings are **required** for access to CalREDIE:

Please note: If you are unable to access or change any of these settings please contact your system administrator or IT personnel.

1. **You will need to have Internet Explorer 7.0 or higher installed on your computer**
2. **Clear Internet Explorer Browser cache**

a. Select "Tools"
b. Select "Internet Options"
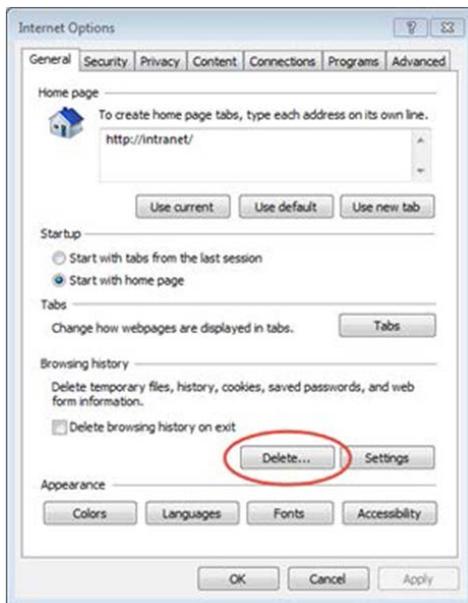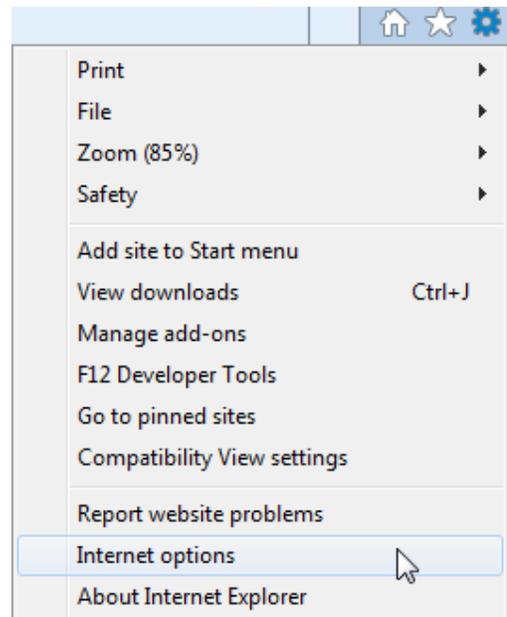
c. Click the "General" tab
d. Click "Delete" under "Browsing history"

e. Mark the Checkbox for at least "Temporary Internet files and website files" and "Cookies and website data"
f. Click "Delete"

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
Public Health
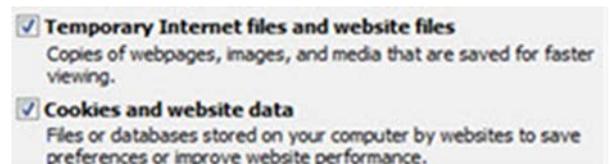
3. **Set Internet Explorer to "Check for newer versions of stored pages":**

a. Select "Tools"
b. Select "Internet Options"
c. Click the "General" tab
d. Click "Settings" under "Browsing history"
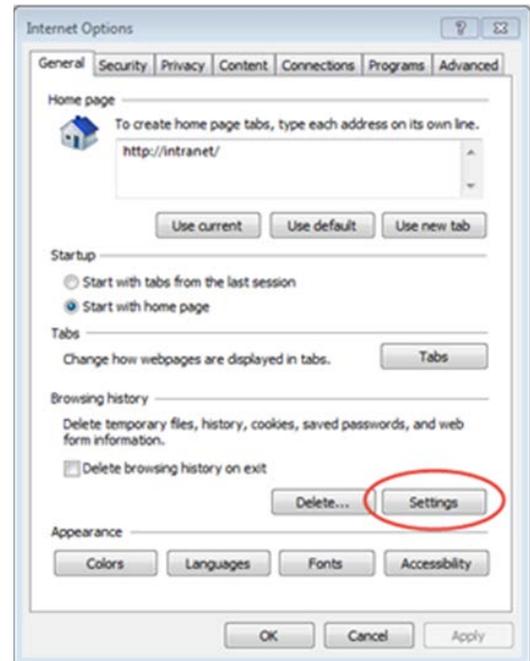
e. Mark the radio button for "Every time I start Internet Explorer"
f. Click "OK"
g. Click "Apply"

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
Public Health
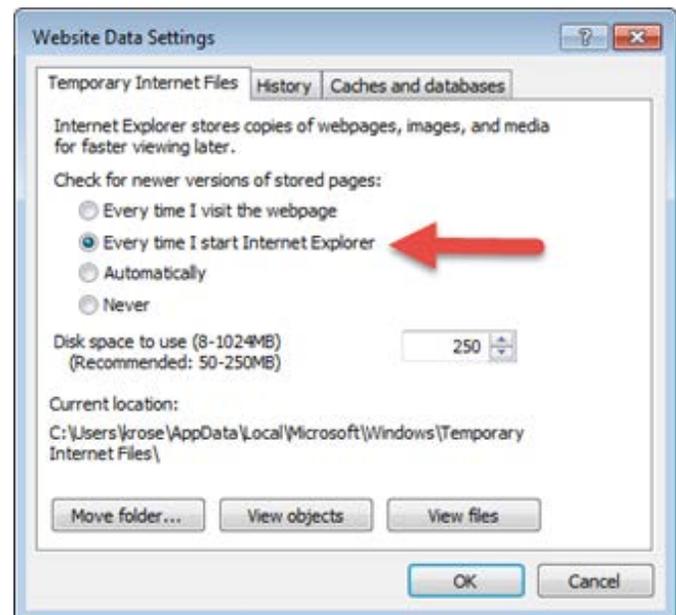
4. **Add the CalREDIE URLs as trusted sites:**

a. Select "Tools"
b. Select "Internet Options"
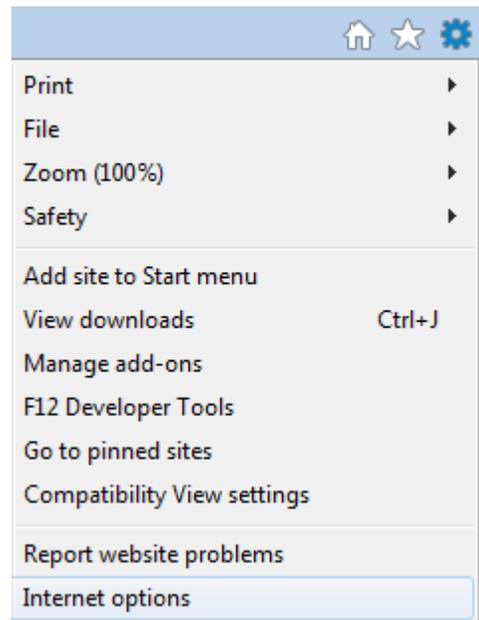
c. Click the "Security" tab
d. Select "Trusted Sites"
e. Click "Sites"

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
PublicHealth
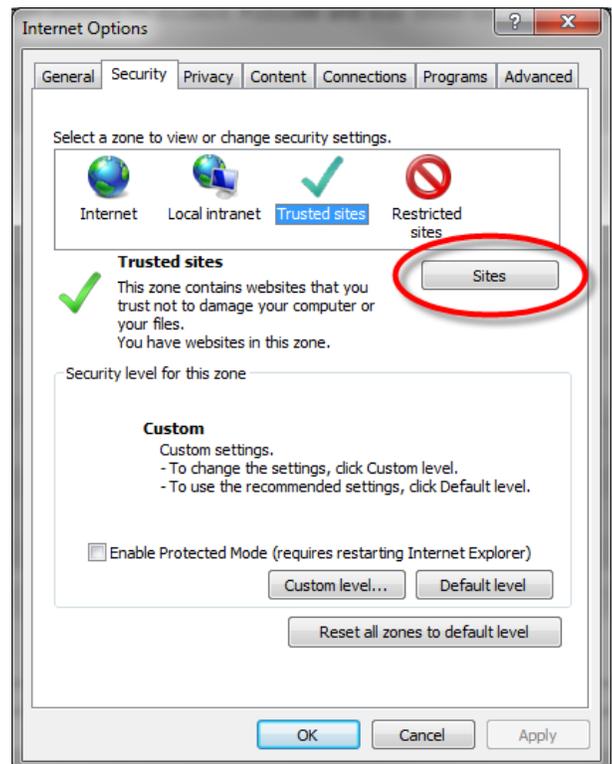
f. Enter the following CalREDIE
    URLs in the "Add this website to
    the zone" box:
        https://calredie.cdph.ca.gov
        https://calrediestaging.cdph.ca.gov

g. Click "Add"
h. Click "Close"

Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:
[   ] [Add]

Websites:
https://calredie.cdph.ca.gov
https://calrediestaging.cdph.ca.gov [Remove]

☑ Require server verification (https:) for all sites in this zone

[Close]
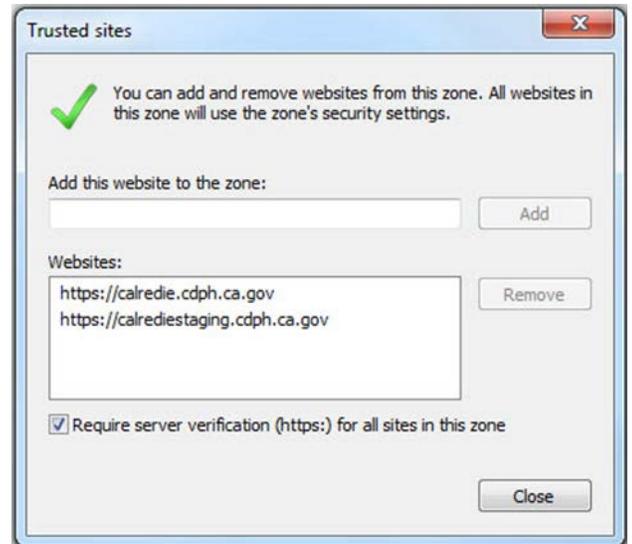
5.   **Enable Active X and Javascript for the trusted sites**

(Please note: The following security
settings will only apply to secure
websites listed as Trusted Sites)

a. From the security tab used above,
    click "Trusted Sites"
b. Click "Custom Level"

Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites   [Sites]
This zone contains websites that you
trust not to damage your computer or
your files.
You have websites in this zone.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

[Custom level...] [Default level]

[Reset all zones to default level]

[OK] [Cancel] [Apply]

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
PublicHealth

c. Select "Low" from the drop-down
d. Click "Reset"

Security Settings - Trusted Sites Zone

Settings

- .NET Framework
  - Loose XAML
    - ○ Disable
    - ◉ Enable
    - ○ Prompt
  - XAML browser applications
    - ○ Disable
    - ◉ Enable
    - ○ Prompt
  - XPS documents
    - ○ Disable
    - ◉ Enable
    - ○ Prompt
- .NET Framework-reliant components
  - Permissions for components with manifests
    - ○ Disable

*Takes effect after you restart your computer

Reset custom settings

Reset to: Low ▾   Reset...

OK   Cancel

e. Set the following:

   i. ActiveX controls and plug-ins → Automatic prompting for ActiveX controls: **ENABLE**

Automatic prompting for ActiveX controls
- ○ Disable
- ◉ Enable
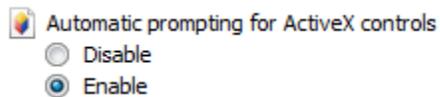
   ii. ActiveX controls and plug-ins → Download unsigned ActiveX controls: **PROMPT**

Download unsigned ActiveX controls
- ○ Disable
- ○ Enable
- ◉ Prompt
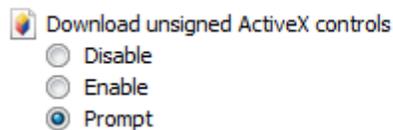
   iii. ActiveX controls and plug-ins → Initialize and script ActiveX controls not marked as safe for scripting: **PROMPT**

Initialize and script ActiveX controls not marked as safe for script
- ○ Disable
- ○ Enable
- ◉ Prompt
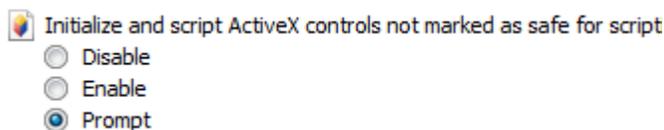
iv. Downloads → File downloads: **ENABLE**

v. Miscellaneous → Allow scripting of Microsoft web browser control: **ENABLE**

vi. Miscellaneous → Allow script-initiated windows without size or position constraints: **ENABLE**
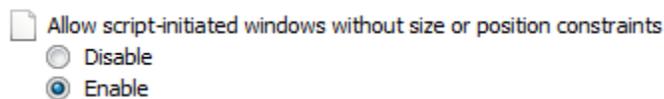
vii. Miscellaneous → Display mixed content: **ENABLE**
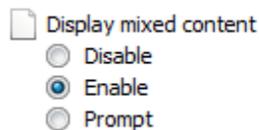
viii. Miscellaneous → Use Pop-up Blocker: **DISABLE**
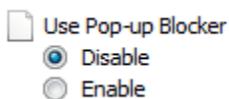
ix. Miscellaneous → Websites in less privileged web content zone can navigate into this zone: **ENABLE**

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
Public Health
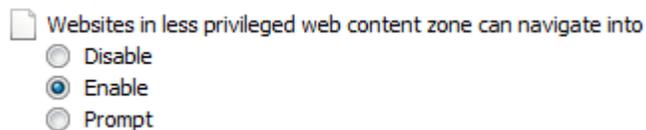
x. Scripting → Activate scripting: **ENABLE**


```
Scripting
    Active scripting
        ○ Disable
        ● Enable
        ○ Prompt
```
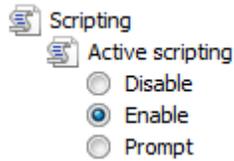
xi. Scripting → Allow Programmatic clipboard access: **PROMPT**


```
Allow Programmatic clipboard access
    ○ Disable
    ○ Enable
    ● Prompt
```
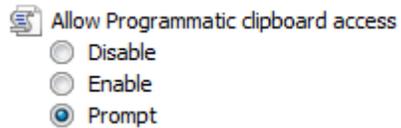
xii. Scripting → Allow websites to prompt for information using scripted windows: **ENABLE**


```
Allow websites to prompt for information using scripted windows
    ○ Disable
    ● Enable
```
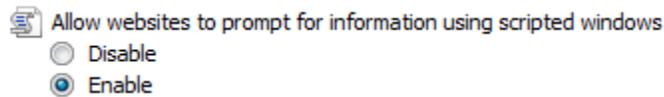
xiii. Scripting → Enable XSS filter: **ENABLE**


```
Enable XSS filter
    ○ Disable
    ● Enable
```

xiv. Scripting → Scripting of Java applets: **ENABLE**


```
Scripting of Java applets
    ○ Disable
    ● Enable
    ○ Prompt
```

f. Disable Security Setting:
    i. Click the "Advanced" tab
    ii. Under "Security" settings, un-check the "Do not save encrypted pages to disk" setting
    iii. Click "OK"
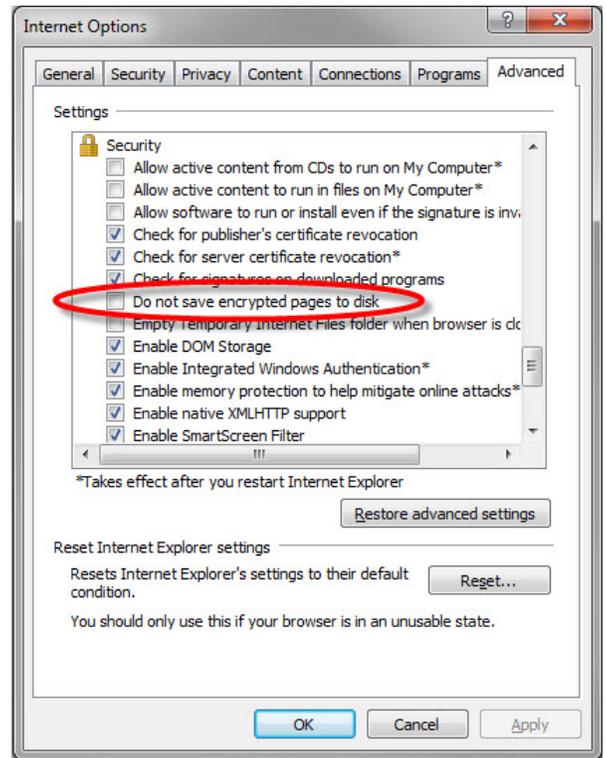
6. Install ActiveX Controls:

a. Navigate to the CalREDIE login page: https://calredie.cdph.ca.gov

b. Click on the "Install ActiveX Controls" link
c. Follow the instructions on the new page that will open

7. IE 11 Only – Update for Internet Explorer 11 (KB3025390):
   a. Have your system administrator install the following update for IE 11:
https://support.microsoft.com/en-us/kb/3025390

8. IE 8 Only – Disable AutoComplete:
   a. Click the "Content" tab
   b. Under the "AutoComplete" section, select "Settings"
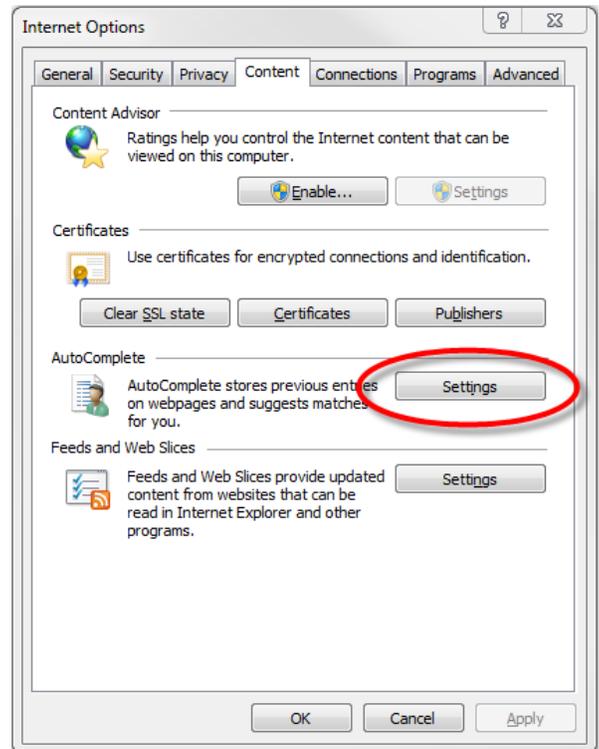
   c. Uncheck the "User names and passwords on forms" setting
   d. Click the "Delete AutoComplete history" button
   e. Click "OK"

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
PublicHealth
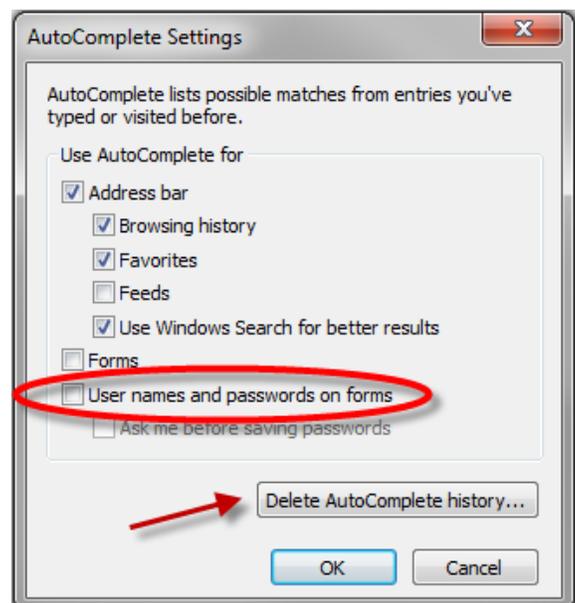
9. **IE 7 Only – Disable AutoComplete:**
   a. Click the "Content" tab
   b. Under the "AutoComplete" section, select "Settings"
   c. Uncheck the "User names and passwords on forms" setting
   d. Click "OK"
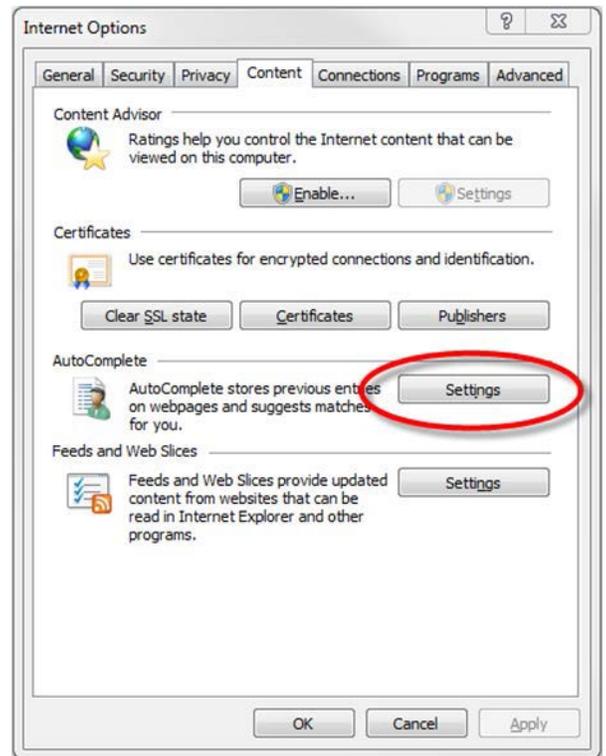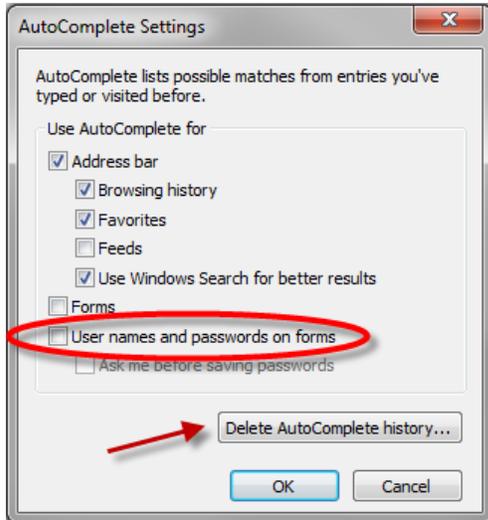
   e. Select the "General" tab
   f. Click "Delete…"
   g. Check the "Passwords" setting
   h. Click the "Delete"
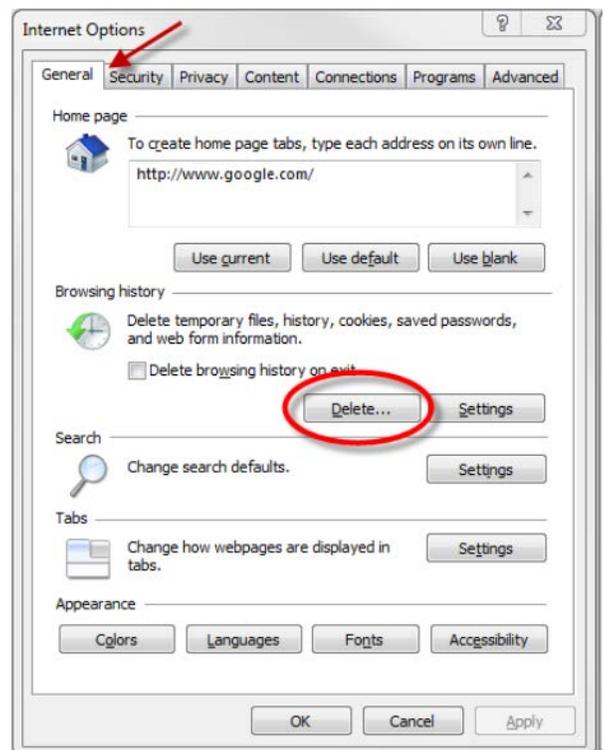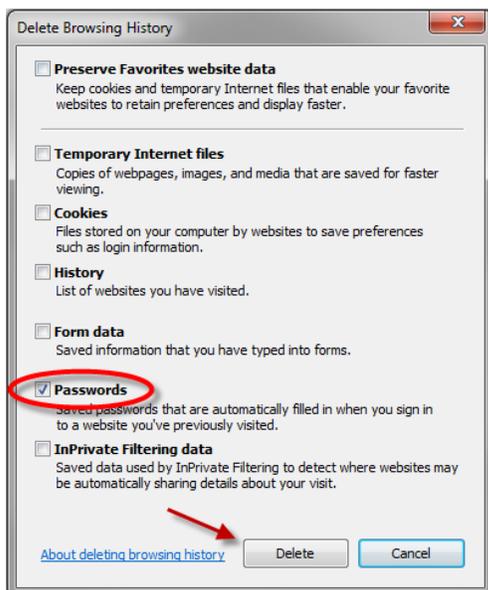
Section 2: Windows XP Requirements
The following settings are **required** to access
CalREDIE using **Windows XP**

1. **Set text DPI to 96 DPI**
   a. Right-Click your Desktop
   b. Select "Properties"
   c. Click the "Settings" tab
   d. Select "Advanced"

   e. Select "Normal size (96 DPI)"
   f. Click "OK"
   g. Click "Yes" on pop-up window to reboot your computer

CalREDIE
California Reportable Disease
Information Exchange

CDPH
California Department of
PublicHealth
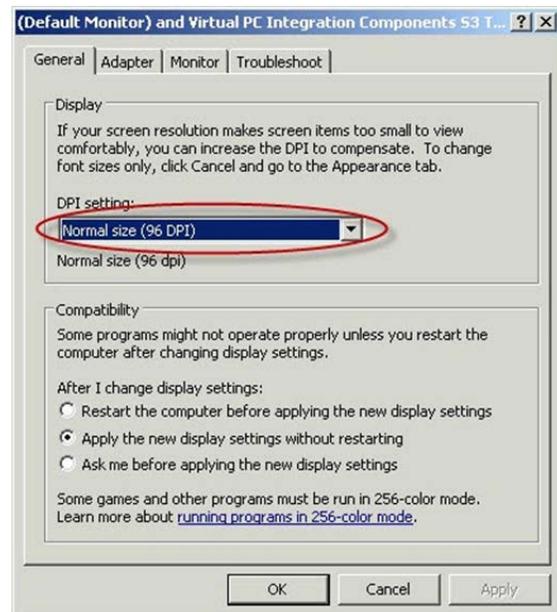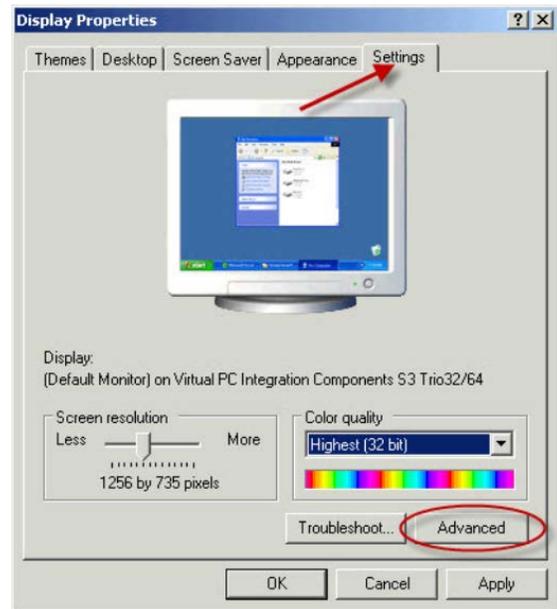
Section 3: Troubleshooting

The following can help resolve common issues:

Please note: If you are unable to access or change any of these settings please contact your system administrator.

1. **EFC upload feature is missing.**

   a. Verify that you see a blank box instead of the Data Source drop down menu

Acquire Files

Patient: Fake, Data
Record ID: 2377473

File Upload Method: ● Advanced (ActiveX) ○ TWAIN (ActiveX) ○ Simple (HTTP)

* Album Name: [   ]

Notes:

Due to limitations within your browser, a maximum of 5 MB of files can be saved to an album at a time. When scanning images, monitor the progress indicator to determine when you are approaching the maximum allowance. When you are at the limit, close the scanning interface and save data to the server

Internet Explorer Add-on Installer - Security Warning

Do you want to install this software?

   Name: CMRImageScan.cab
   Publisher: **Atlas Development Corporation**

☒ More options   [Install]   [Don't Install]

⚠ While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Files in the Album:

File   **Delete**

◂ PREV | NEXT ▸

   b. Have your system administrator log into your computer with their Windows account and then let you log into your CalREDIE account.
   c. Navigate through the EFC to the Upload window
   d. Update your browser settings to match those in this document
   e. You can now logoff CalREDIE and Windows
   f. Log back into the computer with your normal Windows account
   g. The EFC file upload/scanning will be present from now on