Centricity* RIS-IC and Centricity OneView 10.x and Centricity ConnectR 5.x

Microsoft Internet Explorer (IE) Settings

December 2009, Revision 2
2048299-001, DOC0629804

Do not duplicate.
Copyright © 2009 by General Electric Co.
* Trademark of General Electric Co.
**Confidentiality and Proprietary Rights**

This document is the confidential property of GE and/or its affiliated entities. It is furnished to, and may only be used by, customers and their employees under a written agreement with GE and may only be used in accordance with the terms of that agreement. The access and use of this document is restricted to customers and their employees. The user of this document agrees to protect the confidentiality of the information contained herein and GE’s proprietary rights as expressed herein and not permit access to this document by any person for any purpose other than as an aid in the use of the GE software. In no case may this document or any portion hereof be accessed, made available, examined, or copied for the purpose of developing, marketing, or supporting any system or computer program similar to the GE software. No part of this document may be copied without the prior written permission of GE. The information in this document is subject to change by GE without notice.

Inquiries regarding permission for use of material contained in this document should be addressed to:

GE Healthcare

ATTN: General Counsel, 540 West Northwest Highway, Barrington, IL 60010

**Trademarks**

GE, the GE Monogram, and Centricity are trademarks of the General Electric Company. All third-party trademarks are the property of their respective owners.

**Copyright Notice**

Copyright © 2009 The General Electric Company. All rights reserved.

**Illustrations**

All illustrations in this document are provided as examples only. Screens shown in this document do not necessarily reflect or emulate your exact patient data or the precise appearance of your screen.

In this document, all names appearing in examples and illustrations are fictitious. The use of any real person's name is purely coincidental.
Contents

Contacting GE Healthcare Support ............................................. 4

About This Guide ........................................................................ 5
  Purpose of This Guide .............................................................. 6
  Document Revision History ....................................................... 7

Internet Explorer Settings ......................................................... 8
  Internet Explorer (IE) 6 Settings ............................................... 9
    Defining Browser Settings for IE 6 ...................................... 9
    Defining Security Settings for IE 6.................................... 10
  Internet Explorer (IE) 7 Settings ........................................... 12
    Defining Browser Settings for IE 7 .................................... 12
    Defining Security Settings in IE 7 .................................... 13
  Internet Explorer (IE) 8 Settings ........................................... 16
    Defining Browser Settings for IE 8 .................................... 16
    Defining Security Settings in IE 8 .................................... 17
You can report issues to the GE Healthcare National Service Center 7 x 24 either by telephone or eService.

**Telephone**
1. Call GE Healthcare National Service Center at 1-800-437-1171.
2. Select option 3, and then follow the menu.

**eService**
About This Guide

Purpose of This Guide ......................................................................... 6
Document Revision History .................................................................. 7
Purpose of This Guide

This guide contains information on defining Microsoft Internet Explorer (IE) settings for client PCs. GE Healthcare recommends using the Internet Explorer Administration Kit (IEAK) to allow administrators to set the IE settings without having to log in to each client PC. For more information about IEAK, refer to the following web page: https://www.microsoft.com/technet/prodtechnol/ie/ieak/default.mspx

The system uses signed ActiveX controls that must be installed on a client PC. The controls can be downloaded or pushed to the client.

Note Only users defined in Windows as an “Administrator” or “Power User” are allowed to install controls.

What Is Installed on Client PCs and Why?

<table>
<thead>
<tr>
<th>Control</th>
<th>Installed for working with...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crystal Reports Viewer</td>
<td>Reports</td>
</tr>
<tr>
<td>Doc Imaging Client</td>
<td>Document Management Solution</td>
</tr>
<tr>
<td>Doc Imaging Viewer</td>
<td>Document Management Solution</td>
</tr>
<tr>
<td>ICAPI</td>
<td>Integrated third-party products</td>
</tr>
<tr>
<td>MAM Breast Image Editor</td>
<td>MAM</td>
</tr>
<tr>
<td>WebWord</td>
<td>Results Reporting/Transcription</td>
</tr>
<tr>
<td>Window Handler</td>
<td>Centricity RIS-IC, in general</td>
</tr>
<tr>
<td>Centricity Edit Control</td>
<td>Precision Reporting</td>
</tr>
<tr>
<td>wSpell (Spell Checker)</td>
<td>Precision Reporting</td>
</tr>
<tr>
<td>AnyModalFootPedal</td>
<td>Precision Reporting</td>
</tr>
<tr>
<td>Centricity Capture</td>
<td>Precision Reporting</td>
</tr>
<tr>
<td>Centricity Capture Control</td>
<td>Precision Reporting</td>
</tr>
<tr>
<td>ICAPI Listener</td>
<td>eForms</td>
</tr>
<tr>
<td>Signature pad drivers</td>
<td>eForms</td>
</tr>
<tr>
<td>.NET 2.0</td>
<td>eForms</td>
</tr>
</tbody>
</table>
## Document Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>July 2009</td>
<td>Draft version for customer partners.</td>
</tr>
<tr>
<td>2</td>
<td>December 2009</td>
<td>First version for commercial release.</td>
</tr>
</tbody>
</table>
Internet Explorer (IE) 6 Settings

Defining Browser Settings for IE 6

The following settings are required. All other settings not specified in this document are optional.

1. Access the Microsoft Internet Explorer properties using one of the following methods:
   - Start Internet Explorer then click **Tools > Internet Options** from the main menu.
   - Right-click the Internet Explorer icon (ē) on your desktop, and then select **Properties**.
   The Internet Options window appears.

2. To define the application as your web browser home page, enter the address (URL) for the application in the **Address** field in the Home page panel of the Internet Options window. You must include “default.htm” in the URL. For example: http://server name/Centricity/default.htm, where server name is the name of the Web Server.

3. In the Temporary Internet files panel, click **Settings**.
   The Settings window appears.

4. At the Check for newer versions of stored pages prompt, click **Every time you start Internet Explorer**.
5. In the **Amount of disk space to use** field, enter 70 MB or more.

6. Click **OK**.

7. On the Internet Options window, click the **Advanced** tab.

8. Scroll to the HTTP 1.1 settings section and ensure that **Use HTTP 1.1** is checked.

### Defining Security Settings for IE 6

The following settings are required. All other settings not specified are optional.

1. Click the **Security** tab.

2. In the **Select a Web content zone to specify its security settings** field, click **Trusted sites**.

Windows 2000 and XP Service Pack 1 users may instead define the security settings for the Local intranet zone. However, Windows XP Service Pack 2 users must define the security settings for the Trusted sites zone.

3. Click **Sites**.

4. If your site uses server verification (https:) make sure the **Require server verification (https:) for all sites in this zone** check box is selected, otherwise, make sure it is cleared.

5. In the **Add this Web site to the zone** field, enter the URL of the Web Server. For example: http://server name

6. Click **Add**.

7. Click **OK**.

8. In the **Security level for this zone** field, click **Custom Level**.

   The Security Settings window appears.
9. To be able to download controls, in the ActiveX controls and plug-ins section, locate the Download signed ActiveX controls setting and select Prompt or Enable.

10. In the Miscellaneous section, locate the Userdata persistence setting and select Enable.

| Note | If this setting is set to Disable, users will be unable to acquire documents into the Document Management Solution. |

11. On the Security Settings Window, click OK.

12. At the Are you sure you want to change the security settings for this zone? prompt, click Yes.

13. Click the Privacy tab.

14. Move the slider and select the medium privacy setting.

15. Click OK.
Internet Explorer (IE) 7 Settings

The use of IE 7’s Zoom feature and IE 7 add-ons is not supported. When using IE 7 over an encrypted secure sockets layer (SSL), the security certificate presented by the website must match the website’s address. A certificate alert error will display if they do not match.

Defining Browser Settings for IE 7

The following settings are required. All other settings not specified in this document are optional.

1. Access the Microsoft Internet Explorer properties using one of the following methods:
   - Start Internet Explorer then click **Tools > Internet Options** from the Menu Bar.
   - Right-click the Internet Explorer icon ( ) on your desktop, and then select **Properties**.

   The Internet Options window appears.

2. To define the application as your web browser home page, enter the address (URL) for the application in the Home page section of the Internet Options window. You must include “default.htm” in the URL. For example:
http://server name/imagecast/default.htm, where server name is the name of the Web Server.

3. In the Browsing history section, click Settings.
The Settings window appears.

4. At the Check for newer versions of stored pages prompt, click Every time I start Internet Explorer.

5. In the Disk space to use field, enter 70 MB or more.

6. Click OK.

7. On the Internet Options window, click the Advanced tab.

8. Scroll to the HTTP 1.1 settings section and ensure that Use HTTP 1.1 is checked.

Defining Security Settings in IE 7

The following settings are required. All other settings not specified are optional.

1. Click the Security tab.

2. In the Select a zone to view or change security settings panel, click Trusted sites.

3. Click Sites.

4. If your site uses server verification (https:) make sure the Require server verification (https:) for all sites in this zone check box is selected, otherwise, make sure it is cleared.

5. In the Add this Website to the zone field, enter the URL of the web server and the ConnectR server. For example: http://server name

6. Click Add.

7. Click Close.

8. In the Security level for this zone panel, click Custom level.
9. In the ActiveX controls and plug-ins section, Locate the **Allow Scriptlets** setting and select **Enable**.

   **Note**  
   If disabled, ConnectR’s calendar control will not function properly.

10. To be able to download controls, do the following:
    - In the ActiveX controls and plug-ins section, locate the **Automatic prompting for ActiveX controls** setting and select **Enable**.

       **Note**  
       If disabled, users will not be able to download ActiveX controls from modal dialog windows.

       - In the ActiveX controls and plug-ins section, locate the **Download signed ActiveX controls** setting and select **Enable**.

       - In the Downloads section, locate the **Automatic prompting for file downloads** setting and select **Enable**.

11. In the Miscellaneous section, locate the **Userdata persistence** setting and select **Enable**.

    **Note**  
    If disabled, users will be unable to acquire documents into the Document Management Solution.

12. In the same section, locate the **Use Pop-up Blocker** and select **Disable** or add the site to the Pop-up Blocker settings located on the Privacy tab.

13. In the same section, locate the **Allow script-initiated windows without size or position constraints** and select **Enable**.

    **Note**  
    If disabled, the **Always on Top** user preference will not function causing windows such as the Help or the Document Management Solution to open behind other Centricity windows.

14. In the Scripting section, locate the **Allow Programmatic clipboard access** setting and select **Enable**.

    **Note**  
    If disabled, users will receive an additional prompt when accessing a context sensitive pop-up menu or window.

15. On the Security Settings window, click **OK**.

16. At the **Are you sure you want to change the security settings for this zone?** prompt, click **Yes**.
17. Click the **Privacy** tab.

![Internet Options settings](image)

18. Move the slider and select the **medium** privacy setting.

19. Click **OK**.
Internet Explorer (IE) 8 Settings

The use of IE 8's Zoom feature and IE 8 add-ons is not supported. When using IE 8 over an encrypted secure sockets layer (SSL), the security certificate presented by the website must match the website's address. A certificate alert error will display if they do not match.

Defining Browser Settings for IE 8

The following settings are required. All other settings not specified in this document are optional.

1. Access the Microsoft Internet Explorer properties using one of the following methods:
   - Start Internet Explorer then click **Tools > Internet Options** from the Menu Bar.
   - Right-click the Internet Explorer icon ( ) on your desktop, and then select **Properties**.

   The Internet Options window appears.

2. To define the application as your web browser home page, enter the address (URL) for the application in the Home page section of the Internet Options window. You must include “default.htm” in the URL. For example:
http://server name/imagecast/default.htm, where server name is the name of the Web Server.

3. In the Browsing history section, click **Settings**.
   The Temporary Internet Files and History Settings window appears.

4. At the Check for newer versions of stored pages prompt, click **Every time I start Internet Explorer**.

5. In the **Disk space to use** field, enter 70 MB or more.

6. Click **OK**.

7. On the Internet Options window, click the **Advanced** tab.

8. Scroll to the HTTP 1.1 settings section and ensure that **Use HTTP 1.1** and **Use HTTP 1.1 through proxy connections** is checked.

### Defining Security Settings in IE 8

The following settings are required. All other settings not specified are optional.

1. Click the **Security** tab.

2. In the **Select a zone to view or change security settings** panel, click **Trusted sites**.

3. Click **Sites**.

4. If your site uses server verification (https:) make sure the **Require server verification (https:) for all sites in this zone** check box is selected, otherwise, make sure it is cleared.

5. In the **Add this Website to the zone** field, enter the URL of the web server and the ConnectR server. For example: http://server name

6. Click **Add**.

7. Click **Close**.
8. In the **Security level for this zone** panel, click **Custom level**.

9. In the ActiveX controls and plug-ins section, Locate the **Allow Scriptlets** setting and select **Enable**.

   **Note**  
   If disabled, ConnectR's calendar control will not function properly.

10. To be able to download controls, do the following:

    - In the ActiveX controls and plug-ins section, locate the **Automatic prompting for ActiveX controls** setting and select **Enable**.

       **Note**  
       If disabled, users will not be able to download ActiveX controls from modal dialog windows.

    - In the ActiveX controls and plug-ins section, locate the **Download signed ActiveX controls** setting and select **Enable**.

    - In the Downloads section, locate the **Automatic prompting for file downloads** setting and select **Enable**.

11. In the Miscellaneous section, locate the **Allow script-initiated windows without size or position constraints** and select **Enable**.

   **Note**  
   If disabled, the **Always on Top** user preference will not function causing windows such as the Help or the Document Management Solution to open behind other Centricity windows.

12. In the same section, locate the **Use Pop-up Blocker** and select **Disable** or add the site to the Pop-up Blocker settings located on the Privacy tab.

13. In the same section, locate the **Userdata persistence** setting and select **Enable**.

   **Note**  
   If disabled, users will be unable to acquire documents into the Document Management Solution.

14. In the Scripting section, locate the **Allow Programmatic clipboard access** setting and select **Enable**.

   **Note**  
   If disabled, users will receive an additional prompt when accessing a context sensitive pop-up menu or window.

15. On the Security Settings window, click **OK**.

16. At the **Are you sure you want to change the security settings for this zone?** prompt, click **Yes**.
17. Click the **Privacy** tab.

18. Move the slider and select the **medium** privacy setting.

19. Click **OK**.