



# Client Readiness Checklist for RODE on VW301

Client Level Recommendations & IE 9.0 Settings

**©2012 Ramco Systems Ltd. All rights reserved. All trademarks acknowledged.**

This document is published by **Ramco Systems Ltd.** without any warranty.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose without the written permission of **Ramco Systems Limited.**

Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to software programs and/or equipment, may be made by Ramco Systems Limited, at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Any hard copies of this document are to be regarded as temporary reference copies only.

**Table of Contents**

**1.0 RECOMMENDED SETTINGS .....4**

**1.1 Add the Ramco application URL to Trusted Sites Zone.....4**

**1.2 Security Settings to be made.....5**

**1.3 Recommended settings in Internet Explorer 9.0 at the Client, which runs  
Ramco Application Runtime ..... 8**

**1.4 Clearing Cookies and Temporary Internet files .....8**

**2.0 OTHER RECOMMENDATIONS.....10**

## Client Level Recommendations

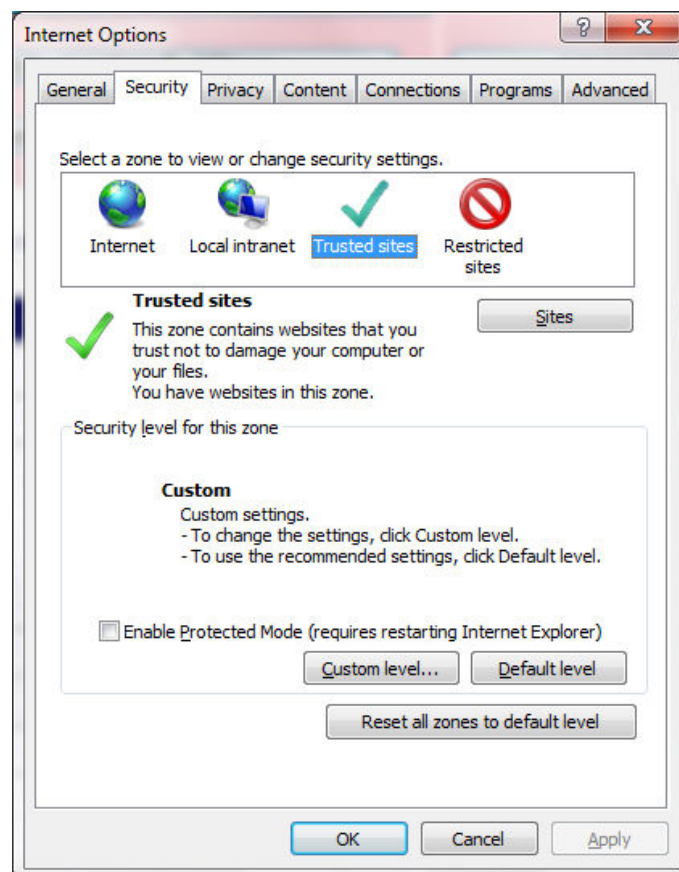
### 1.0 Recommended Settings

---

**Internet Explorer Settings that need to be set in all the local clients for smooth working of Ramco Application**

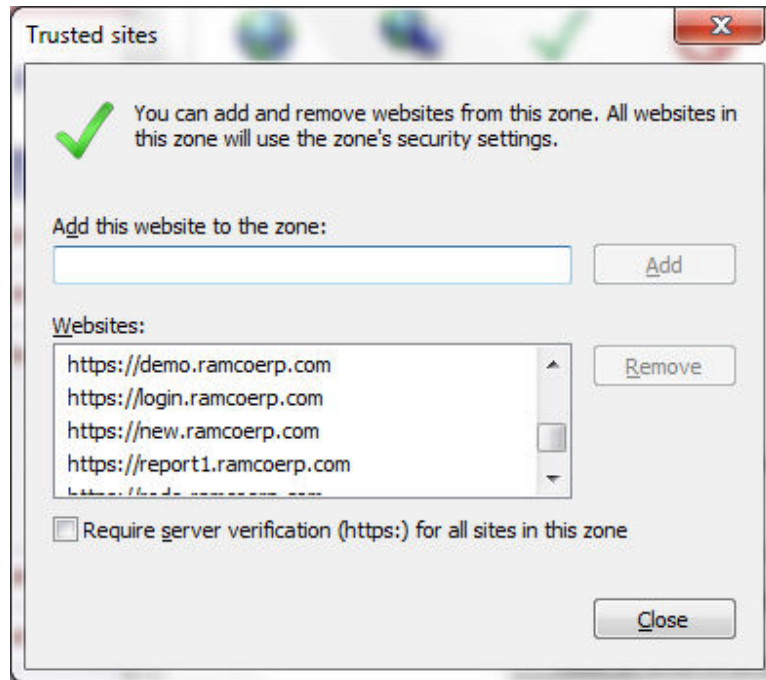
#### 1.1 Add the Ramco application URL to Trusted Sites Zone

- ❖ Open Internet Explorer
- ❖ Go to Tools -> Internet Options -> Security Tab.



- ❖ Click on Trusted Sites and click on the Sites button

- ❖ Type the URL **"https://login.ramcoerp.com"**, **"https://new.ramcoerp.com"** and **"https://rode.ramcoerp.com"** to be added in the "Add this Web site to the zone" edit control and click on the Add button.
















- ❖ Click on the OK button. (This takes the user back to the "Internet Options" dialog.)


## **1.2 Custom Level Security Settings to be made.**







- ❖ Open Internet Explorer.
- ❖ Go to Tools -> Internet Options -> Security Tab
- ❖ Click on the button "Custom Level" in the "Security Level for this Zone" frame.
- ❖ Security Settings window will open.
- ❖ Go down to the following sections and set the following options
  - ❖ ActiveX Controls and Plug-ins
  - ❖ Scripting
  - ❖ User Authentication.

❖ **ActiveX Controls and Plug-ins**


-  ActiveX controls and plug-ins
  -  Allow ActiveX Filtering
    - Disable
    - Enable
  -  Allow previously unused ActiveX controls to run without prompt
    - Disable
    - Enable
  -  Allow Scriptlets
    - Disable
    - Enable
    - Prompt
  -  Automatic prompting for ActiveX controls
    - Disable
    - Enable
  -  Binary and script behaviors
    - Administrator approved
    - Disable
    - Enable
  -  Display video and animation on a webpage that does not use ActiveX
    - Disable
    - Enable
  -  Download signed ActiveX controls
    - Disable
    - Enable
    - Prompt
  -  Download unsigned ActiveX controls
    - Disable
    - Enable
    - Prompt
  -  Initialize and script ActiveX controls not marked as safe for scripting
    - Disable
    - Enable
    - Prompt
  -  Only allow approved domains to use ActiveX without prompt
    - Disable
    - Enable
  -  Run ActiveX controls and plug-ins
    - Administrator approved
    - Disable
    - Enable
    - Prompt
  -  Script ActiveX controls marked safe for scripting\*
    - Disable
    - Enable


❖ **Scripting**

 Scripting

-  Active scripting
  - Disable
  - Enable
  - Prompt
-  Allow Programmatic clipboard access
  - Disable
  - Enable
  - Prompt
-  Allow status bar updates via script
  - Disable
  - Enable
-  Allow websites to prompt for information using scripted windows
  - Disable
  - Enable
-  Enable XSS filter
  - Disable
  - Enable
-  Scripting of Java applets
  - Disable
  - Enable
  - Prompt

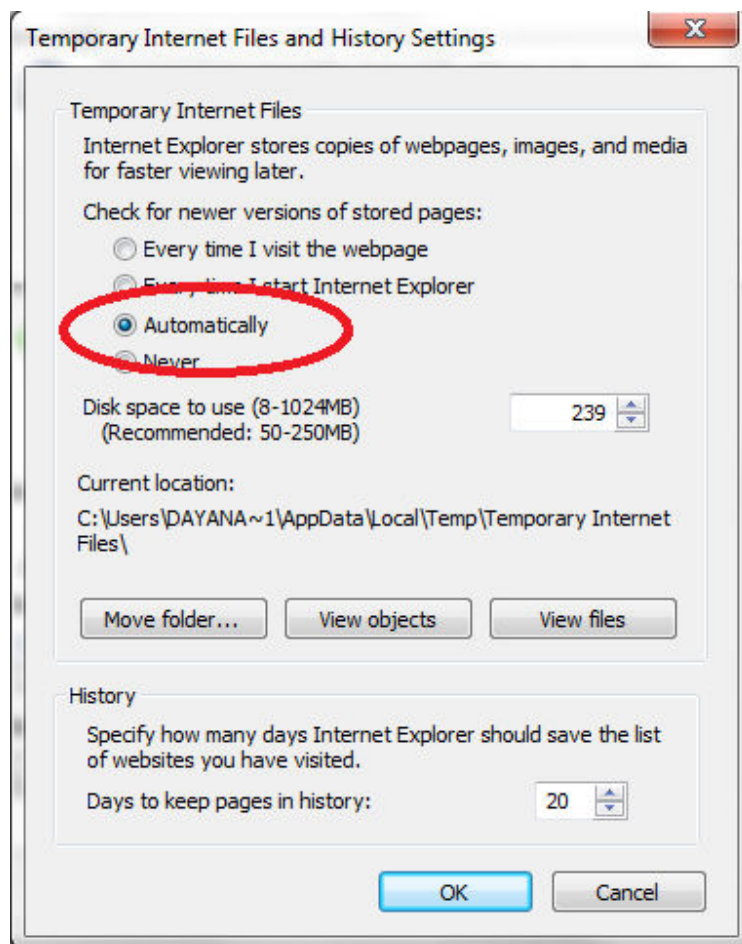
❖ **User Authentication.**

 User Authentication

-  Logon
  - Anonymous logon
  - Automatic logon only in Intranet zone
  - Automatic logon with current user name and password
  - Prompt for user name and password

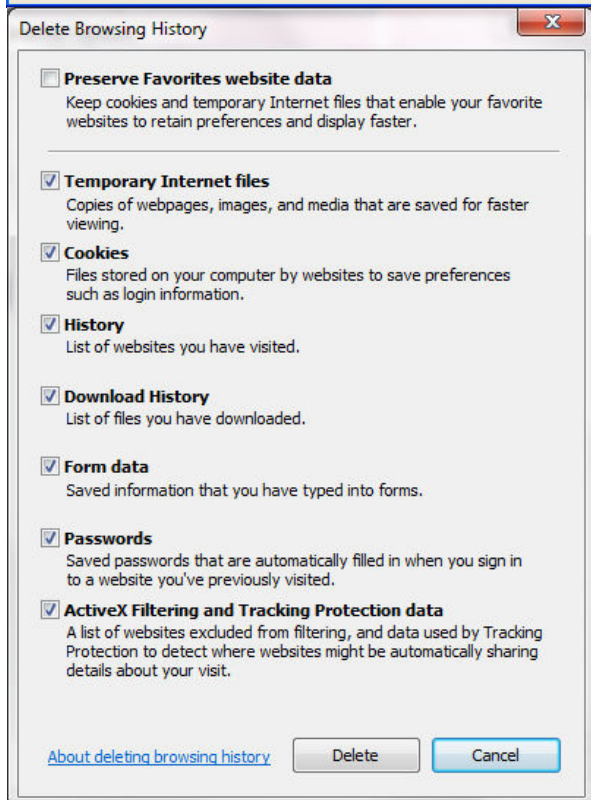
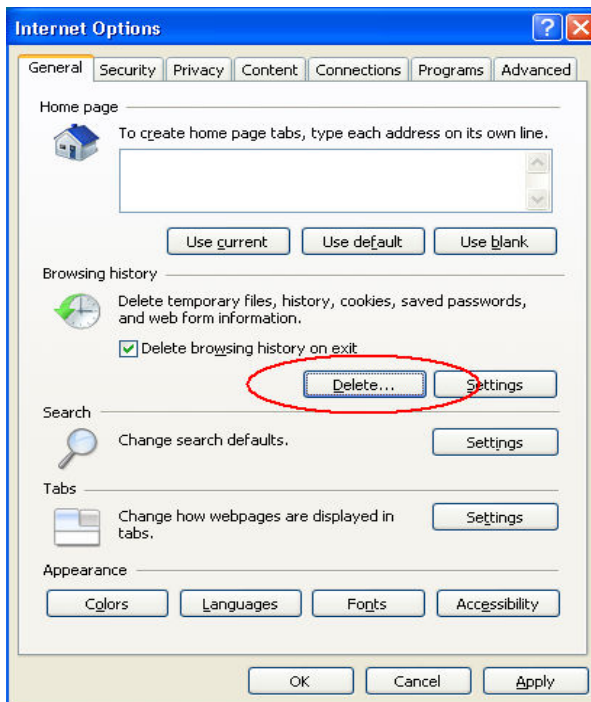
### 1.3 Recommended settings in Internet Explorer at the Client, which runs Ramco Application Runtime.

- ❖ Go to Internet Explorer
- ❖ Click on Tools-> Internet Option-> General->
- ❖ Click on Settings button in Temporary Internet files, choose "**Automatically**" under Check for Newer version of Stored pages

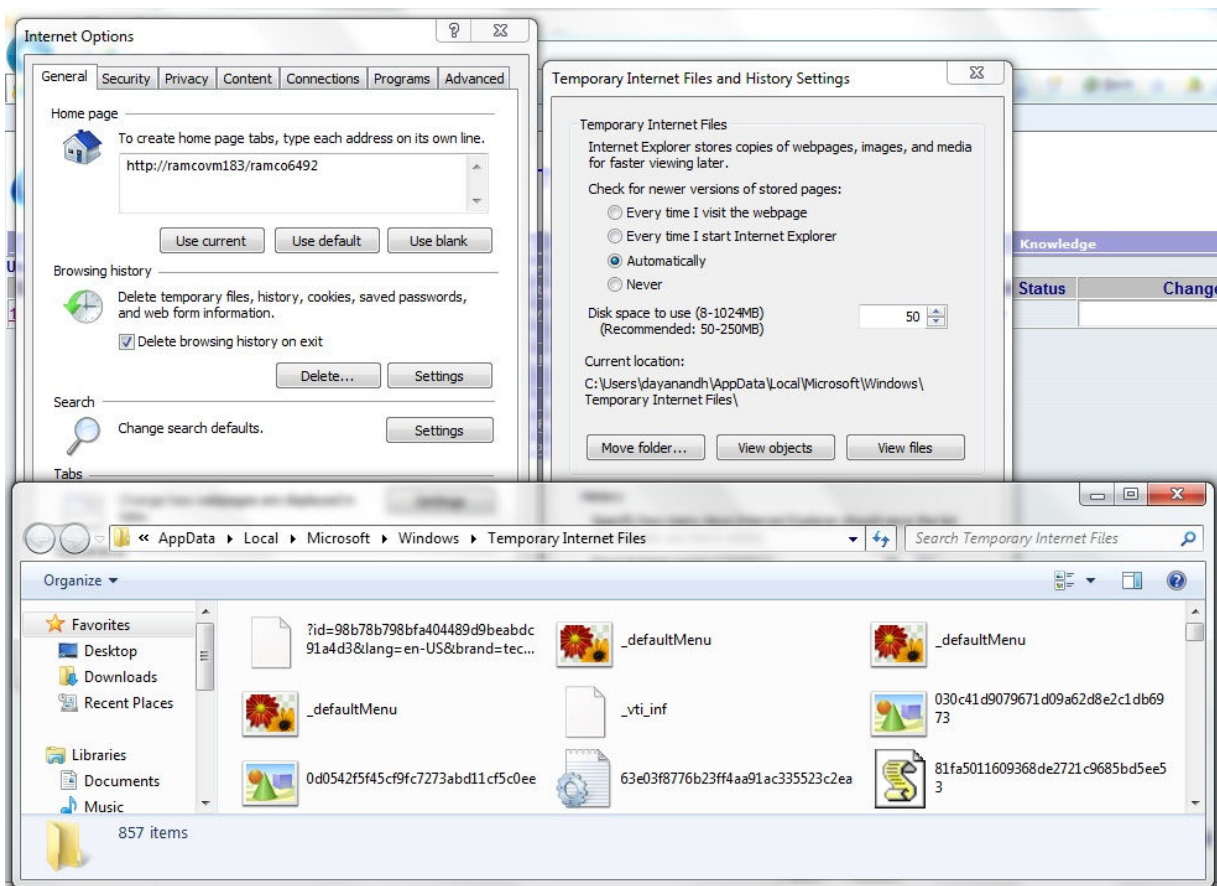


### 1.4 Clearing Cookies and Temporary Internet Files.

- ❖ Go to Internet Explorer
- ❖ Click on Tools-> Internet Option-> Delete ->



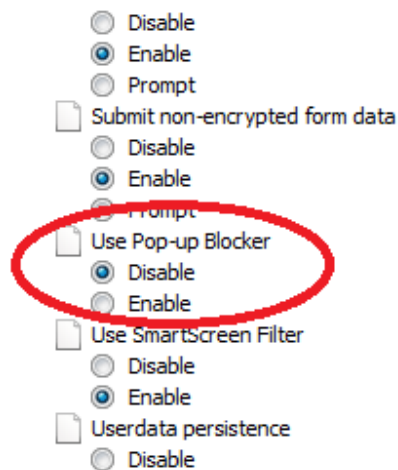
- ❖ Select all Check boxes including Preserve Favorites website data and Temporary Internet files, Cookies, History, Form Data, Passwords and InPrivate Filtering data. Select "**Delete**" button to delete all temporary files.
- ❖ Delete all the Temp Files available in the **Temporary Internet Files** which loads in a separate folder when you click the View files button.



## 2.0 Other Recommendations

---

- ❖ Remove Yahoo Toolbar, Google toolbar if installed.
- ❖ **Turn off popup blocker** for the Trusted Sites security zone on which the site is being launched.



---

### Corporate Office and R&D Center

Ramco Systems Limited, 64, Sardar Patel Road, Taramani Chennai – 600 113, India

Tel: +91 (44) 2235 4510. Fax +91 (44) 2235 2884

[www.ramcoondemand.com](http://www.ramcoondemand.com)

Confidential