



Department of Treasury and Finance
Government of Western Australia

Client Agency Desktop System Guideline

DTF Information Systems (DTF IS)

Version 4.0 (July 2009)

Table of Contents

| | | |
|-----|---|----------|
| 1 | Introduction | 1 |
| 1.1 | Document Purpose | 1 |
| 2 | System Requirements..... | 1 |
| 2.1 | Desktop Client Requirements..... | 1 |
| 2.2 | Client Browser Requirements after 29 September 2009 following release 6.1 go-live | 2 |
| | 2.2.1 Certification Matrix for OS/Browser combinations..... | 2 |
| | 2.2.2 Java Runtime requirements..... | 2 |
| 3 | System Recommendations | 3 |
| 3.1 | Recommended Client Configuration | 3 |
| | 3.1.1 Processor | 3 |
| | 3.1.2 Memory | 3 |
| | 3.1.3 Other Software Requirements | 3 |
| 3.2 | Recommended Web Browser Settings | 3 |
| | 3.2.1 Internet Explorer | 3 |
| | Non-HTTP Based Access by Agencies..... | 8 |
| 3.3 | Use of OFA at Agencies..... | 8 |
| 3.4 | Recommended Solution..... | 8 |
| | 3.4.1 Site to Site VPN..... | 8 |
| 4 | Key Contacts..... | 8 |

DOCUMENT CONTROL

Document Approval:

| Name | Title | Initials | Date |
|---------------|---------------------|----------|-----------|
| Faranak Lillo | Shared Services SDM | | 9/11/2007 |
| Stephen Yii | Shared Services SDM | | 2/9/2008 |

Distribution list:

| Name | Title | Date |
|---------------|--|-----------|
| Faranak Lillo | Shared Services Technical Delivery Manager | 9/11/2007 |
| Terence Shim | Project Services Manager | 9/11/2007 |
| Stephen Yii | Shared Services Service Delivery Manager | 10/8/2008 |
| Dick Berry | Shared Services Technical Delivery Manager | 27/8/2009 |

Document history:

| Version | Revision Date | Prepared by | Reviewer | Review Date |
|---------|---------------|----------------|--|-------------|
| 0.1 | 8/3/2007 | Nimmi Carlose | Darren Smith (Oracle) | 12/12/2005 |
| 1.0 | | | Darin Davis (Oracle) | 9/6/2006 |
| 1.1 | 12/10/2007 | Terence Shim | Faranak Lillo (SS) Bill Laidlaw (SS) Simon Reeves (SS) | 12/10/2007 |
| 2.0 | 15/10/2007 | Terence Shim | Faranak Lillo (SS) Bill Laidlaw (SS) Simon Reeves (SS) | 15/10/2007 |
| 2.1 | 8/11/2007 | Simon Reeves | Faranak Lillo (SS) Terence Shim (SS) | 9/11/2007 |
| 2.2 | 15/6/2008 | Michael Wong | Terence Shim (SS) | 18/06/2008 |
| 2.3 | 8/8/2008 | Michael Wong | Stephen Yii (SS) Terence Shim (SS) | 10/08/2008 |
| 3.0 | 25/8/2008 | Michael Wong | Stephen Yii (SS) Terence Shim (SS) | 28/08/2008 |
| 3.1 | 20/11/2008 | Mustafa Basher | Stephen Yii (SS) Terence Shim (SS) | 20/11/2008 |
| 4.0 | 27/07/2009 | Vincent Law | Dick Berry | 27/07/2009 |

1 Introduction

1.1 Document Purpose

The intended audience of this document are for IT Managers / Helpdesk staff within Agencies that will be able to compare these Shared Services (SS) client desktop specification recommendations against their agency desktop environments in relation to compatibility information with the current and future SS Oracle E-Business Application – specifically supported Operating Systems/browser combinations and Java runtime engines.

This document does not necessarily cover all the requirements of agency client systems, as certain elements of the SS solution are still being built. The majority of Agency users access will occur using standard HTML browser access and assuming that they currently can run web applications to a satisfactory level of performance their current configuration should be sufficient for this type of HTML with no Java runtime engines required on the client desktop.

2 System Requirements

2.1 Desktop Client Requirements

Release 6.1 of the SS Oracle E-business Application will make a number of changes to the Desktop Client Operating Systems that is certified to be used against it. The table below shows what will be supported up to 25 September 2009 and what will be supported following the upgrade of the system over the weekend of 26-28 September.

| Supported OSs up to 25 September 2009 | Supported OSs on 29 September 2009 |
|--|---|
| Windows 2000 SP1+ | Windows 2000 SP1+ |
| Windows XP Professional + SP1, SP2, SP3 | Windows XP Professional SP2, SP3 |
| Macintosh 10.2 | Mac OS Xv 10.3.9 or higher |
| | Vista and Vista SP1 |

Therefore, if your current SOE OS is working with the existing application then it will work after release 6.1 is implemented on 29 September 2009 and Agencies have to do no modifications to their OS. However, please refer to the next section below as to the OS/browser combinations that are supported by Oracle.

Notes:

- E-Business Suite 11i is certified on Pentium 4, for Desktops/Client Tier use.

- Service Pack Requirements for Microsoft Windows platforms may change in the future

2.2 Client Browser Requirements after 29 September 2009 following release 6.1 go-live

2.2.1 Certification Matrix for OS/Brower combinations

The table below outlines the currently Oracle certified Browsers, Operating System combinations after release 6.1 go-live.

| OS/Browser | IE6 | IE7 | Firefox 3.0.x | Safari |
|---|-----|-----|---------------|--------|
| Windows 2000 SP1+ | ✓ | x | x | x |
| XP SP1 | x | x | x | x |
| XP SP2 and SP3 | ✓ | ✓ | ✓ | x |
| Mac OS X 10.3.9 or higher | x | x | x | ✓ |
| Vista and Vista SP1 (JRE now provides support for Vista) ¹ | x | ✓ | ✓ | x |

The significant change is that there is no longer any support for XP SP1 with any browser combination and Vista is now supported.

Please note that as XP SP2 and SP3 and IE6 and IE7 make up the majority of the operating systems and browsers used by Agencies, these will be supported by DTF SS. Agencies using any other Oracle supported OS and browser combinations do so at their own risk. If Agencies have issues with the system then DTF SS will only be obligated to open up a support request with Oracle.

2.2.2 Java Runtime requirements

The current Java Runtime engine to access functionality that requires Oracle Forms is Oracle's Jinitiator 1.3.1.29. However, this will be out of support 31 July 2009. The replacement for this will Sun's Java Runtime, JRE 1.6.0_14 or any higher version of this (e.g. 1.6.0_15).

We strongly recommend that you install JRE 1.6.0_14 to all your Agency's PCs before the release 6.1 go-live in preparation for it. Failure to do this will mean that users will not be able to access the Forms pages of the application.

To download this, please go to the Java download site and download JRE 6 Update 14 via this URL - <http://java.sun.com/javase/downloads/index.jsp>

¹ Vista SP2 not supported yet but certification in progress.

3 System Recommendations

3.1 Recommended Client Configuration

The following are the minimum recommendations for configuring your desktop client assuming that you are using J-Initiator on the desktop.

3.1.1 Processor

Release 11i performance is sensitive to the CPU speed. We recommend using PCs with at least Pentium Pro 200MHz processors, or Apple Macintoshes with at least 200MHz PowerPC G3 processors. You will realise significant performance improvement with faster (1.4GHz +) processors. Note: Users with client machines running dual core AMD processors may encounter browser hangs and crashes when running Shared Service eBusiness portal, therefore we currently do not support Dual core AMD processors.

3.1.2 Memory

We recommend at least 256 MB of RAM for Microsoft Windows operating systems. Windows 2000 or Windows XP users, or users who are concurrently running Oracle Applications with other desktop applications, will experience better performance with at least 512 MB of RAM. Apple Mac OS clients require a minimum of 256 MB of RAM.

3.1.3 Other Software Requirements

Adobe Reader (PDF) Version 7 only.

3.2 Recommended Web Browser Settings

3.2.1 Internet Explorer

3.2.1.1 Security Zones

Microsoft Internet Explorer offers four different security zones to run your application. How you access your site (Internet or Local Intranet) dictates what security zone to use (Trusted sites & Restricted sites).

It is advisable to have the security setting at Medium for run-time use.

Oracle E-Business Suite can be set to run through the 'Trusted Sites' zone, with a 'Medium' security setting as follows;

1. Select Tools -> Internet Options -> Security tab -> Trusted Sites icon.
2. Set the 'Security Level for this Zone' to 'Medium' if it is not set already.
3. Select Tools -> Internet Options -> Security tab -> Trusted Sites icon -> Sites button .

4. In the 'Add this Web site to the zone:' field, enter the 'hostname and domain' of the environment you are running Oracle E-Business Suite from, i.e. https://*.oss.wa.gov.au then click the 'Add' button.

(If you are entering an 'http://...' or '*. ' domain address, you must ensure that the 'Require server verification (https:) for all sites in this zone' is *not* checked).

3.2.1.2 JRE Plug-in (Supported For MSIE 6 & 7)

The JRE plug-in will download and install from the webserver on a medium security setting. After clicking on a 'forms link', a message similar to the following will appear at the top of the browser window:

```
'The website wants to install the following add-on: 'J2SE Runtime Environment 6 Update 3' from 'Sun Microsystems, Inc.'. If you trust this website and the add-on and want to install it, click here...'
```

To install the plug-in:-

1. Click on the message above and select 'Install ActiveX Control...'
2. Once the browser has stopped processing, click on the 'forms link' again, and the oaj2se.exe file should start to download
3. Once the download has completed, a security warning pop-up window will ask, 'Do you want to install this software?'
4. Click on the 'Install' button and follow the on screen instructions

Alternatively, you can avoid this message by temporarily altering the security settings for the initial install, using one of the two methods below. Once the plug-in has been installed on the desktop, the browser security settings should be reset to 'medium'.

3.2.1.3 Method A: Change Security Setting to Medium-low

1. Select 'Tools' -> 'Internet Options -> 'Security' (Tab) from the browser menu.
2. Select 'Trusted Sites' -> 'Custom Level' (button)
3. From the 'Reset custom settings' drop down select 'Medium-low'
4. Click the 'Reset...' button and accept the changes.
5. Press the 'okay' buttons to close the window.
6. Close the browser and start a new browser session for the settings to take effect.
7. After launching Oracle E-Business Suite and downloading the oaj2se.exe file onto your desktop, please reset the security setting back to 'Medium'.

3.2.1.4 Method B: Change Individual Parameter Settings

1. Select 'Tools' -> 'Internet Options -> 'Security' (Tab) from the browser menu.
2. Select 'Trusted Sites' -> 'Custom Level' (button)
3. Under 'Settings' -> 'ActiveX controls and Plug-ins'
4. Change 'Automatic prompting for ActiveX controls' to 'Enable'
5. Change 'Download unsigned ActiveX controls' to 'Prompt'
6. Click the 'OK' button and accept the changes and click the 'OK' buttons to close the window
7. Close the browser and start a new browser session for the settings to take effect.
8. After launching Oracle E-Business Suite and downloading the oaj2se.exe file onto your desktop, please reset 'Automatic prompting for ActiveX controls' to 'Disable' and 'Download unsigned ActiveX controls' to 'Disable'.

3.2.1.5 Use of Excel with WebADI (Applicable To MSIE 6 & 7)

To create an excel spreadsheet on your desktop through WebADI, the 'Initialize and script Active X controls not marked as safe' setting must be set to 'Prompt'. This is only defaulted to this value on a 'Low' security setting', therefore you will probably need to alter this setting through Internet Explorers Custom Settings option as follows; Select Tools -> Internet Options -> Security *tab* from the Internet Explorer Menu Bar. Select the zone that you are running Oracle E-Business Suite through and click the 'Custom Level' button. You can then set the value as recommended above.

3.2.1.6 Page Refresh (Applicable To MSIE 6 & 7)

When using Oracle Self-Service products it is important to ensure that the most current data is being viewed. You may check if the page has been updated since your last visit by manually refreshing the page, however it is desirable for this to be done automatically through MSIE by setting the following parameter;

To set 'Page Refresh', select Tools -> Internet Options -> General 'tab' -> Settings 'button' from the MSIE menu bar. Under the 'Check for newer versions of stored pages:' heading, select 'Every visit to the page'. With this option set, Internet Explorer will check if the page has changed since it was last viewed.

3.2.1.7 AutoComplete in Internet Explorer (Applicable To MSIE 6 & 7)

IE can automatically show previous values entered in the same form field. For privacy and security reasons this feature should be *disabled* as follows;

Go to Tools - > Internet Options -> Content
Click the AutoComplete button
Uncheck the 'Forms' and 'User names and passwords on forms' boxes.

3.2.1.8 Internet Explorer 7 - Web Based LOV's (Tabbed Browsing)

If the 'Always Open Pop-Ups in a New Tab' option within MSIE7 is selected, Web based LOV's can lose focus. To regain focus within the pop-up window press 'Ctrl & Tab'. This option is set in MSIE7 through Tools -> Internet Options -> Tabs -> Settings -> Always Open Pop-Ups in a New Tab.

3.2.1.9 Exporting Data and Opening Attachments

The file type that you wish to export from Shared Services E-Business Suite must be associated with the browser. If the file type is not associated, the Window will not open or will briefly open and then close immediately. This may occur for example, when using 'File -> Export' to an excel spreadsheet or when opening an attachment from E-Business Suite.

To fix this issue, using the 'Trusted Sites' zone as an example, (which is recommended for running Oracle E-Business Suite through);

Select 'Tools' -> 'Internet Options' -> 'Security' (tab) -> 'Trusted Sites' -> 'Custom Level' (button) -> 'Downloads' from the browser menu.

Set 'Automatic prompting for file downloads' to 'Enable'.

Save the setting and close the browser window.

Start a new browser session and login to Oracle E-Business Suite.

This time, when trying to open the attachment or export data you should see a pop up windows titled 'File Download'.

Uncheck the checkbox labelled, 'Always ask before opening this type of file' and click the 'open' button.

The file should now display correctly.

After this has been done, the file extension type is registered and you may set the 'Automatic prompting for file downloads' back to 'disable', accessing such files in future will now work correctly with that setting.

3.2.1.10 Microsoft Internet Explorer 'Live Toolbar'

Enabling Microsoft Internet Explorer Live Toolbar within the browser, may cause the browser to crash, whilst trying to login to Shared Services Oracle E-Business. This function is not supported by Shared Services. Therefore it is advised to remove the toolbar from the browser as follows;

On the Start menu > Control Panel > Double-click Add or Remove Programs > Click Windows Live Toolbar > Click the Remove button

NOTE: 'Browser Helpers' such as this, may also cause the browser to crash when trying to Launch Shared Services Oracle E-Business Suite.

3.2.1.11 Microsoft Internet Explorer ActiveX Update 912945 and Oracle Applications

The Microsoft Internet Explorer ActiveX update 912945 changes the way Active X controls work for Microsoft XP SP2 users. In some cases, users will no longer be able to directly interact with ActiveX controls loaded by the APPLET, EMBED or OBJECT elements. This change will also impact some areas of Oracle Applications as outlined in this document.

When accessing a screen affected by this issue, the controls will not function and moving the mouse on it will display the message 'Click to activate and use this control'. However once you mouse click in the screen, the form becomes 'activated' and users may interact with all controls normally within that session.

To work around this: Once user mouse-clicks in the screen, the form becomes 'activated' and the user may interact with all controls normally within that session.

3.2.1.12 Shared PC Security (Applicable To MSIE 6 & 7)

For security reasons, if a PC is shared by multiple users it is advisable *not* to save encrypted pages onto the drive. To set this option, go to Tools -> Internet Options -> Advanced *tab* -> Security settings and tick 'Do not save encrypted pages to Disk'

3.2.1.13 Auto Complete in Internet Explorer

IE can automatically show previous values entered in the same form field. For privacy and security reasons this feature should be disabled as follows:

Go to Tools > Internet Options > Content. Click the AutoComplete button. Uncheck the 'Forms' and 'User names and passwords on forms' boxes

3.2.1.14 HTTP 1.1 / Keep Alive Settings

Customers using Applications 11.5.9 or later should have HTTP 1.1/Keep Alive enabled.

To enable this in IE please go to Tools > Internet Options > Advanced tab > HTTP 1.1 Settings. Please ensure 'Use HTTP 1.1' and 'Use HTTP 1.1 through proxy connections' ensuring that both are ticked

3.2.1.15 Importing the SSL Certificate in MSIE7 on Windows Vista

Connecting to a Secure Socket Layer (SSL) enabled environment requires the certificate to be 'Trusted'. If the certificate is not from a trusted authority or has not previously been trusted on the client, it must be verified at runtime. When accessing such an environment it will return the following warning message: 'There is a problem with this website's security certificate'.

Using the the automatic default install button on Vista will not be sufficient and the error message will still display. Using the automatic default install button results in the addition of the certificate to the browser's 'Intermediate Certification Authorities' folder and not the 'Trusted Root Certification Authorities' folder.

Installing an SSL certificate into the Browsers Trusted Certificates folder requires the browser's security option 'Enable Protected Mode' to be off, which is the default setting in the 'Trusted Sites' zone. This is a new feature in IE7 for Vista. This feature does not exist in the IE7 XP version. (If required, 'Enable Protected Mode' may be turned on after the certificate has been installed, for runtime use).

To trust the certificate authority and to stop this error page appearing on future logins;

1. Enter the URL in the browser
2. From the browser menu select: Tools -> Internet Options -> Security -> Trusted Sites icon. Security setting should be 'Medium' by default
3. Make sure the 'Enable Protected Mode' option is off (not checked)
4. Click the 'Sites' button and add the URL if it is not there already (or add *.oracle.com to cover all Oracle environments, you must uncheck the 'Require Server Verification....' option first to allow you to add it)
5. Save the changes and close the browser window
6. Enter the URL in a new browser window
7. You will again see a message saying 'There is a problem with this website's security certificate'. Click on, 'Continue to this website (not recommended)
8. In the taskbar click on the Red certificate error
9. An Untrusted Certificate Window Pops, click on 'View Certificates'
10. Click on Certification Path 'Tab'
11. Highlight the Root certificate (will probably have a white cross in a red background next to it) and press 'View Certificate'
12. Click on Install Certificate 'button' and press next
13. Select 'Place all the certificates in the following store'
14. Click 'Browse' and tick the 'Show physical Stores' box.
15. Click the + next to 'Trusted Root Certification Authorities' folder
16. If a folder exists called 'Local Computer' Click on it and select 'Okay'
17. If that folder does not exist, highlight 'Trusted Root Certification Authorities' folder and select 'Okay'
18. Press 'Next' followed by 'Finish'
19. When the Security Window pops asking if you wish to install it, say 'Yes' then hit the 'Finish' button
20. Close the pop-up and the browser, when you next login, it should be fine.

If you still do not get the option to install the certificate (no install button) you may have installed the certificate previously using the automatic facility. This only puts it in the

'Intermediate Certification Authorities' zone. To remove the certificate you can do the following;

- Open the browser and go to Tools -> Internet Options -> Content -> Certificates -> Intermediate Certificate Authorities
- Highlight the appropriate certificate for the instance you are trying to access and press the 'Remove' button and close down the browser
- You can then open a new session and follow the steps above to install it in the 'Trusted Certificates' folder

Non-HTTP Based Access by Agencies

3.3 Use of OFA at Agencies

To enable the Budgeting process at Agencies, it is necessary for the Agency Budget Manager(s) to have access to the OFA software (thin client mode). The remaining Agency staff who participate within the budgeting process are able to use the Web based version of OFA as they do not require the additional administration functions that are only available in the OFA client software.

It is planned for the OFA desktop client to connect directly to the e-business suite database at Shared Services, rather than having a personal database installed on their machine (that is periodically replicated to the e-business suite database).

3.4 Recommended Solution

The OFA client makes use of the SNAPi protocol which is not able to be encrypted, and so we need to be made to ensure that it is properly secured. To minimize the security risk the use of VPN infrastructure is recommended for those users that require the OFA client.

3.4.1 Site to Site VPN

To minimize the security risk the use of VPN infrastructure is recommended for those users that require the OFA client. Please note that further information on this VPN solution can be found within the VPN Agency Pack document which is distributed by the Shared Services Transition Team to Agency during the roll-in phase.

4 Key Contacts

For enquiries, please contact the DTFIS SS Service Delivery Manager on 9258-0606 or Integration Analyst on 92580806.