

IAD Enhancements

IAD Enhancements

- Previous User Pays User Group agreed the following:
 - Single User – Forced Logout Functionality
 - Password Reset Functionality
 - ‘LSO Managed’ or ‘User Managed’ IAD Account Organisations
 - 3 Questions
 - Your / LSO Name
 - Your / LSO User Id
 - Your Security question / LSO IAD Admin Password
 - Idle Time set to 30 minutes
 - Period of 10 days provided for representations
 - No representations received within period
 - Design Finalised

Single User Log On – Forced Logout

- This solution allows a ‘secondary’ session to force the ‘primary’ session to close, in instances of
 - Network Failure
 - Unclean logout
- This solution will be developed in the Application Code and will be a universal solution regardless of which type or version of web browser is used to access the IAD Service
- Introduction of a ‘Logout’ button to record logout times

Idle Time

- User inactive in IAD for duration of idle time
 - Duration set at 30 minutes at implementation
 - Can vary this but has to be set for entire User Group
- When logged out after a period of inactivity the User will be directed to the front screen

Modify Password Functionality

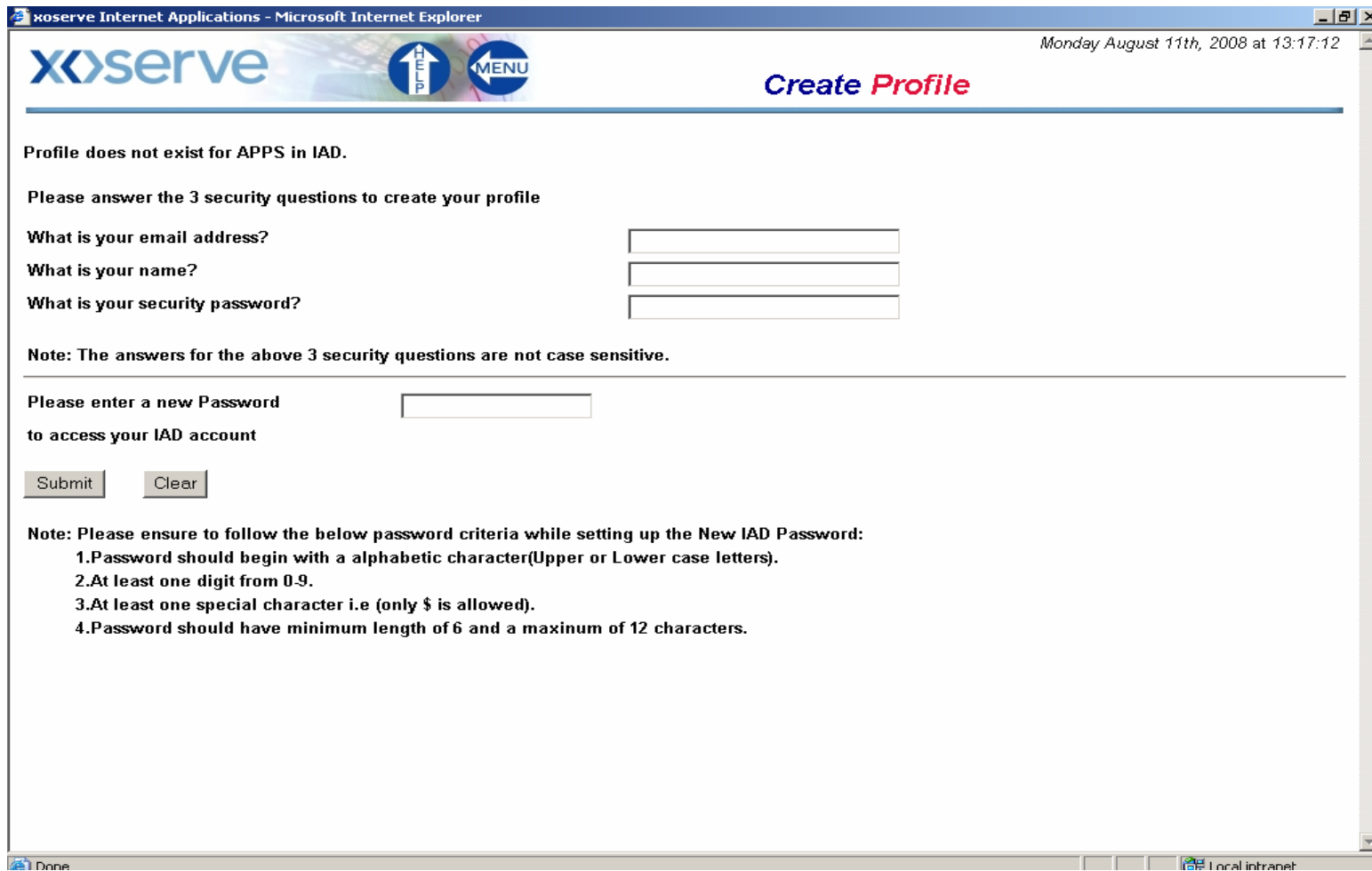
- Users / LSOs will be able to modify account passwords
 - Input answers to 3 Security Profile Questions
 - Input new password
- Users / LSOs will be to retrieve password
 - Input answers to 3 Security Profile Questions
- Password Reset Functionality at set frequency (e.g. 28 days) will not be enabled

IAD Enhancements – Users Day 1

- ‘User Managed’ IAD Account Organisations
 - Users will be prompted for answers to the Security Profile questions
 - 3 Questions
 - Your / LSO Name
 - Your / LSO User Id
 - Your Security question / LSO IAD Admin Password
 - Users will be asked to reset their Passwords
 - Note: A restriction will not allow Users to reset the password to previous password
 - Note: The Password is a combination of numeric and alpha and \$

Set Security Profile

- Users will be asked to populate the following screen:



The screenshot shows a web browser window titled "xserve Internet Applications - Microsoft Internet Explorer". The page header includes the "xserve" logo, a "MENU" button, and the text "Create Profile". The main content area contains the following text and form elements:

Profile does not exist for APPS in IAD.

Please answer the 3 security questions to create your profile

What is your email address?

What is your name?

What is your security password?

Note: The answers for the above 3 security questions are not case sensitive.

Please enter a new Password
to access your IAD account

Note: Please ensure to follow the below password criteria while setting up the New IAD Password:

- 1.Password should begin with a alphabetic character(Upper or Lower case letters).
- 2.At least one digit from 0-9.
- 3.At least one special character i.e (only \$ is allowed).
- 4.Password should have minimum length of 6 and a maximum of 12 characters.

The browser's status bar at the bottom shows "Done" and "Local intranet".

IAD Enhancements – Users Day 1

- 'LSO Managed' IAD Account Organisations
 - Users will NOT be prompted for answers to the Security Profile questions
 - Users will NOT be prompted to reset their Passwords
 - Above information will need to be populated prior to Day 1
 - Security Question answers
 - Passwords
 - Information can be provided at:
 - Organisation Level
 - Individual Account Level
- Confirmation to be provided by Monday 1st September if you are intending to be a LSO Managed Organisation

LSO Organisations – Provision of Information

- 1st September - Contract Manager to confirm intention to be an LSO Managed Organisation
 - To box account .Box.Xoserve.DataCentreServices
- 5th September – xoserve confirm all accounts by user id held by LSO Managed Organisation (may require a freeze on account deletions/creations/resets during that week)
- 15th September - Contract Manager to provide information for LSO Managed Accounts
 - To box account .Box.Xoserve.DataCentreServices
 - Where all accounts for an LSO Managed Organisation are not provided we will assume these are 'User Managed Accounts'
- 19th September - User Guide to be issued to Contract Managers

LSO / User Managed Organisation

- Things to consider in decision whether to be LSO Managed:
 - LSO maintaining central register
 - LSO Absence
 - Change of LSO – therefore bulk change of security profile
 - Out of hours support
 - Increased Administration on LSOs
 - Individual Users not knowing LSO Identity
 - Individuals not knowing whether part of LSO / User Managed Organisation
 - LSO issuing passwords to Users from implementation
 - New Accounts set up – LSOs to manually set profile and passwords

Proposed Next Steps

- Implementation of IAD Service changes – 11th October 2008
 - Proposed outage 22.00 10th Oct – 06.00 13th Oct
 - Contingency outage 17th Oct – 20th Oct
- LSO Managed Organisations
 - Indication of LSO Management – as soon as possible
 - Identify User Accounts
 - Provide Security Profile Answers
 - Provide Passwords
- Contract Managers to provide predicted volume of account creations / deletions / resets