Single User Logon and Self User Password re-set proposals

As discussed at the User Pays User Committee (UPUC) meeting on 14th July, the following approach was agreed with regards functional changes to the IAD Service. The implementation date of 4th October 2008 was proposed for these changes and comments are specifically invited on this matter.

Single User Log on Restriction – Forced Logout Functionality:

Implementation of this functionality will enhance the current IAD system security to ensure that appropriate controls are applied to all live IAD accounts.

Whilst this change will restrict user access to a single user logon per IAD account, the solution will allow a user to open a 'secondary' session of their IAD account and force the 'primary' session to be logged out of the IAD Service.

This approach has been made following the previous discussion at the User Pays User Group as this will ensure that impact to user access to the IAD Service is minimised in instances where logout from a user account has not been captured in circumstances of a network failure or an unclean logout when closing down their previous session.

To further illustrate the functionality for the Single User Log on Restriction, example screen prints of the IAD Service that demonstrate the screens and messages that the user will see once the functionality has been deployed into the production environment are available for view on the Joiny Office website Industry information / user pays documentation / user group meetings 2008 / 14 July 2008 .

Self User Password Reset / Retrieval Functionality:

Implementation of the Self Password Retrieval and reset functionality removes the requirement for LSOs to raise calls to the xoserve helpdesk to retrieve or reset forgotten passwords. The deployment of this functionality will allow a user or Local Security Officer (LSO) the opportunity to retrieve a forgotten password by answering three predetermined security questions. The questions discussed and agreed at 14th July UPUC are listed below:

Q1: What is the LSO's email address?
Q2: What is the LSO's name?
Q3: What is the LSO's IAD Admin password?

User Organisations can restrict the user password retrieval and reset functionality to be used by their appointed LSO only. In order to facilitate this, organisations will be required to supply the answers to the above three questions to xoserve in a timely manner to ensure that xoserve have sufficient time to complete the updates in the security tables ahead of the 11th October implementation date. In such circumstance xoserve are assuming that the answers to the three questions will be applied across all user accounts for an organisation.

If an organisation chooses to allow individual users to update their security profile with their own security question answers they will be prompted to do so the first time that they log into the IAD service post implementation of these changes. In instances where an individual needs to retrieve their password they will need to answer the three security questions. It is not proposed that xoserve validate these answers against the registered LSO details. Example screen prints have been published on the Joint Office website Industry information / user pays documentation / user group meetings 2008 / 14 July 2008.

In instances where an LSO/user needs to reset the password for their account, they will firstly need to answer the three security questions listed above. Once these have been answered successfully the user will be navigated to the modify password screen. In this screen the authorised user is able to modify the password for the IAD account.

Active Idle Time Functionality:

Implementation of the Active Idle Time functionality was discussed and proposed to be set at 30 minutes at the UPUC meeting on 14th July 2008. This means that any IAD account logged into the IAD Service and not active (i.e. does not perform a Transaction or a Hit to the IAD database) for a period greater than 30 minutes will result in the account automatically being logged out of the IAD Service. In instances where this occurs the user will then be navigated back to the IAD Service login screen automatically where they will then need to log back into the IAD Service.

It is proposed to implement these changes along with the batch job enhancements and the monitoring & reporting functionality to the IAD service on the weekend of the 11/12th October 2008. As the project moves closer to implementation and detailed planning has been completed, xoserve will communicate detailed outage timescales.

User comments are invited upon this implementation date by 1st August 2008. Should users have any questions regarding this matter, please do not hesitate to contact me or Neil Morgan (0121 623 2740 neil.a.morgan@xoserve.com).

In addition users are requested to indicate whether they intend to restrict password functionality to the LSO so that xoserve are able to schedule data fixes and if so prompt organisations for the answers to the above three questions nearer implementation.

David Addison
Project Manager
xoserve
david.addison@xoserve.com
0121 623 2741