Document number	Revision
DOCU12197	1

Ldap replication

Background

Highstage does not manage or maintain user repository by default. In order to keep track of its users, it makes use of the LDAP interface provided by an Active Directory already present in the organization's infrastructure.

UserID definition

Users are imported with UserID set to Ldap user pre-windows 2000.

Even though user may logon using user@company the pre-win2000 user name will be used as userid and shown at top of web pages. Below is a sample of a user created with different User logon name and pre-win2000 User logon name. It will be the pre-win2000 user logon name testuser (without dot) that will be used. Observe that normally the two will be identical unless actively made different like in the sample below. Observe that maximum length of pre-win2000 user name is 20 characters, while the other may be much longer:

Observe that user may choose to logon as test.user@tsd.turbostage.com or tsd.turbostage.com\testuser, but in both cases testuser will be the userid used and displayed on top of web pages.

Important replication columns

Name	Description	Constraints
ObjectGUID	Global unique ID associated with Ldap object. Deleting the user account and re-creating the user account will cause a new ObjectGUID to be generated for the user account.	Replication assumes that this column is unique.
LogonName	Pre-win2000 logon name uniquely identifying user in organization IT infrastructure.	-
UserID	System unique UserID. Used by users to assign resources and to identify themselves and each other	Checked for uniqueness both by replication and Sql unique constraint.

Replication logic

#	GUID	Pre-win2000 LogonName	UserID	Description
1	guid1	company1\user1	user1	Imported
2	guid2	company2\user1	user1	Not imported due to UserID collision. This user will be denied access due to GUID mismatch.
3	guid3	company\user1	user1	Previous user was deleted in Ldap and new user with same logonname and userid was created. User will be denied access. Case1, same employee: Case2, new employee:

How to manage deviations

Mapping difficult user logon names to simple UserID's

This is for example required if LogonName is an employee number that makes no sense to other users or if UserID is too long to be used easily or if security requires that logon name is difficult to guess to hackers.

Alternative-1: Use pre-win2000 logon name as UserID.

Alternative-2: UserID may be changed locally in TurboStage if required,. When user logs on UserID will be looked up based on LogonName.

Deletion of existing user account and re-creation for same user

This will cause a new GUID to be generated for the Ldap user account object and a mismatch will occur between Ldap and replicated copy. User will be denied access until GUID's match. Clear the GUID in TurboStage and at next replication the GUID will be updated from Ldap, the GUID's will then match and the user will be allowed access.

Reuse of former user LogonName and UserID for new user

In some situations a user may quit the company and later a new user will be employed and given the previous LogonName. In this case the new user will be denied access since GUID's do not match. In this case the old UserID must be renamed to allow the new user to be imported from Ldap.

> **IMPORTANT!**
> Rename must be done using the object rename tool to ensure that all referencing tables are updated as well, otherwise the new user will have full access to the old users information and appears as author, reviewer etc. on old information.

Change of user LogonName and UserID due to change of marriage status

Change users information in Ldap and use the object rename tool to rename UserID and all information that referencesthe UserID.