integriti
INTEGRATED SOLUTIONS

User management using Active Directory

Document created with reference to

Integriti software V4.2.3.10022

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Certified System
Quality
ISO 9001

Introduction

Users in Integriti can be synchronised with Active Directory. When a user is created in Active Directory, the Active Directory Synchronisation communications handler will detect the change and add, update or remove the user within Integriti (depending on configuration settings). When a user that is synchronised with Active Directory is modified in Integriti, the Active Directory Synchronisation communications handler will detect the change and update the user in the Active Directory (depending on the configuration settings).

User synchronisation requires an 'Active Directory Users' license.

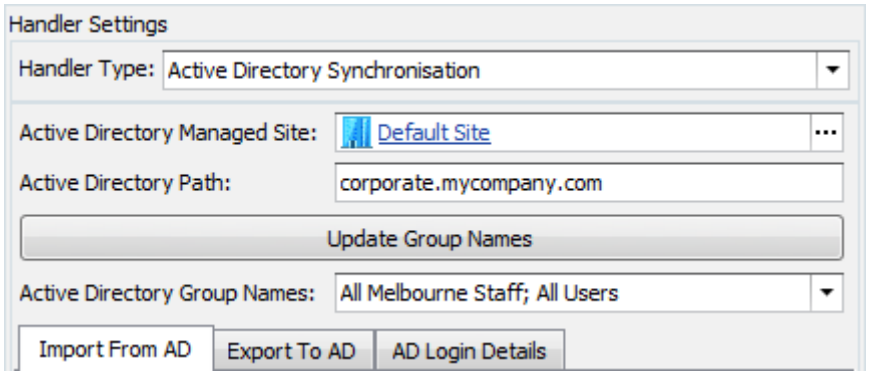
The Integriti Application Server is the service that requires AD read access to import changes from AD to Integriti and write access to export changes in Integriti to AD. The domain administrator will be required to make these changes. There are two methods to get this communications handler to work:

- Attach the PC that is running as the Integriti server to a Domain that belongs to a group with an AD security policy allowing read and/or write access.
- The user account that is used to launch the Integriti Application Server is part of the Domain and belongs to a group with an AD security policy allowing read and/or write access
  OR
  The Username and Password of a user account with the required access are entered in the AD Synchronisation setup.

User synchronisation uses a unique key for the purpose of looking up AD users against Integriti users. This unique key will automatically be stored in a Custom Field in each User called 'ActiveDirectoryGuid'. Modifying the contents of this field will result in a loss of synchronisation with Active Directory.

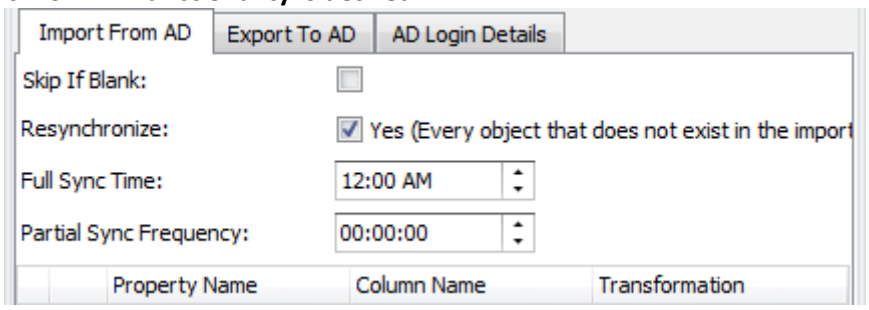
Configuring Integriti for Active Directory Synchronisation

1. Click on the Administration tab followed by Communication Handlers.
2. Click Add New. The Editor Window for a new Communications Handler should appear.
3. Give the Communications Handler a name.

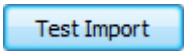


4. On the right-hand side under Handler Settings, change the Handler Type to 'Active Directory Synchronisation'.
5. Optionally change the Default Site from the Default top level site if you want to restrain AD users to a particular site within Integriti.
6. Enter the Active Directory Path. E.g. 'corporate.mycompany.com'.
7. Click on Update Group Names. This will update the list of available domain groups in the 'Active Directory Group Names' field.
8. Drop-down the 'Active Directory Group Names' list box and select the appropriate groups.

If Import From AD functionality is desired:

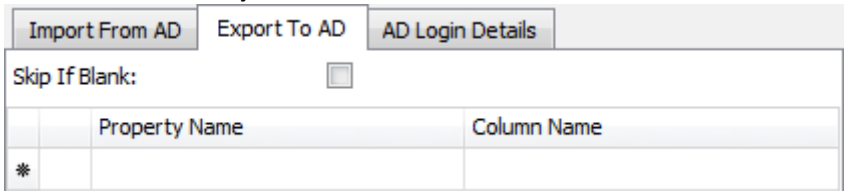


9. Select the 'Import From AD' tab.
10. Ticking the Skip If Blank option will stop Integriti user fields from getting blanked when the corresponding AD user has no data in matching fields.
11. The resynchronize option allows deletion of users from the specified site in Integriti that don't (or no longer) exist in the Domain controller. When a resynchronisation occurs, all of the AD users will be updated, added and/or removed from Integriti.
    If this option is not ticked, users are only added and updated.

12. Full Sync Time refers to the time that the Resynchronization will occur each day.
13. A partial sync is carried out at the interval specified in the 'Partial Sync Frequency' field. This time specified in this field is a frequency in hours, minutes and seconds. Partial syncs only update user changes
14. The import configuration table at the bottom of the Editor Window is used to map AD user attributes to Integriti users.
15. Use 

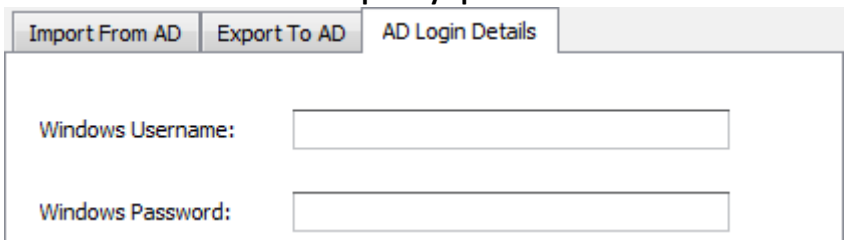
to open a window showing the AD user records and how they would be parsed in to Integriti according to the configuration of the import configuration table.

If Export To Ad functionality is desired:



16. Select the 'Export To AD' tab.
17. Ticking the Skip If Blank option will stop Active Directory user fields from getting blanked when the corresponding Integriti user has no data in matching fields.
18. The export configuration table at the bottom of the Editor Window is used to map AD user attributes to Integriti users.

If a Windows user account is to be explicitly specified:



19. Select the 'AD Login Details' tab.
20. Enter the Windows Username and Windows Password of the Windows user with the required read/write access permissions on the AD domain.

21. Save and close the editor window for the Communications Handler. When the Communications Handler is saved, the communications handler will carry out an initial full synchronisation of the AD users.

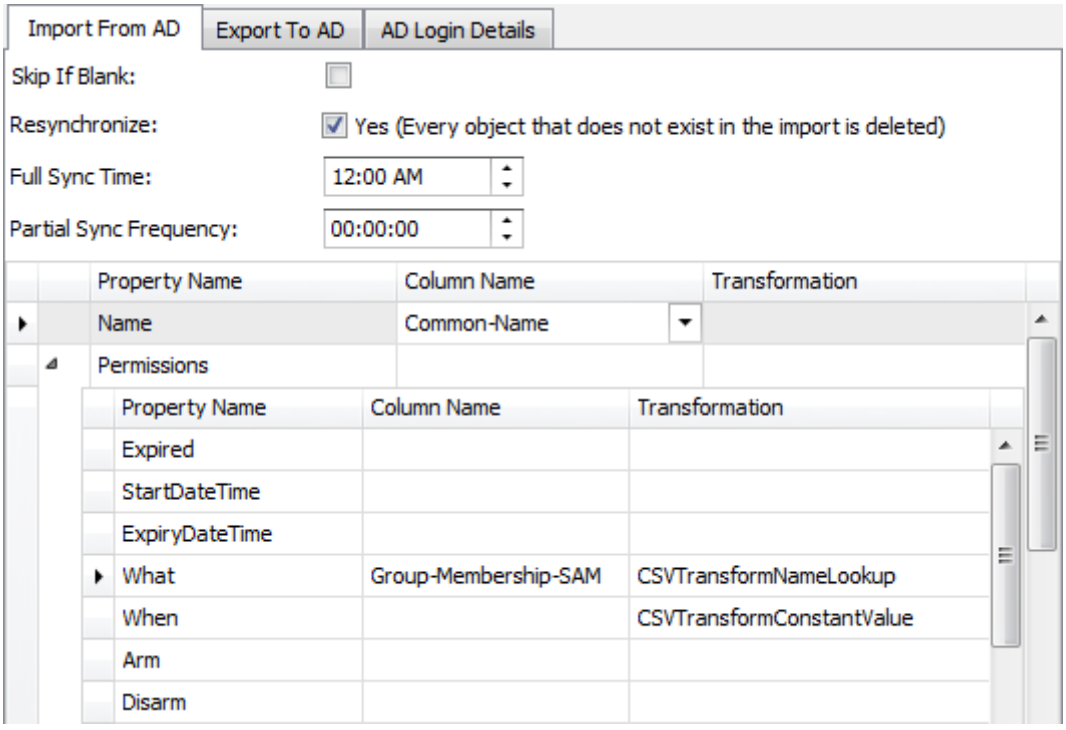
Importing From Active Directory to Integriti

To import changes made to users in Active directory the following steps must be taken:

1. Follow the above instructions to configure the Active Directory Synchronisation.
2. In the 'Import From AD' tab fill out the Import Configuration Table with mappings for each property to be synchronised. See below for instructions on configuring mappings for specific use cases.
3. Save the Communications Handler. When the Communications Handler is saved an initial import of users and settings from Active Directory will be carried out based on the settings and mappings provided.
4. After the initial import, a full synchronisation will occur once a day at the time selected in the 'Full Sync Time' property in the 'Import From AD' tab. A partial synchronisation, which will only pick up changes made in Active Directory to properties of users already synchronised to Integriti, will occur at the rate selected in the 'Partial Sync Frequency' property in the 'Import From AD' tab.

Assigning Multiple Active Directory Groups to Permission Groups

1. In the edit dialog for the Active Directory Communication Handler in Integriti add a new property mapping to the Import Configuration Table.
2. Under 'Property Name' select 'Permissions'.
3. In the list of property mappings that appears under the 'Permissions' mapping, set the 'Column Name' next to the 'What' property mapping to 'Group-Membership-SAM' to map it to the list of Active Directory groups that the user is a member of.

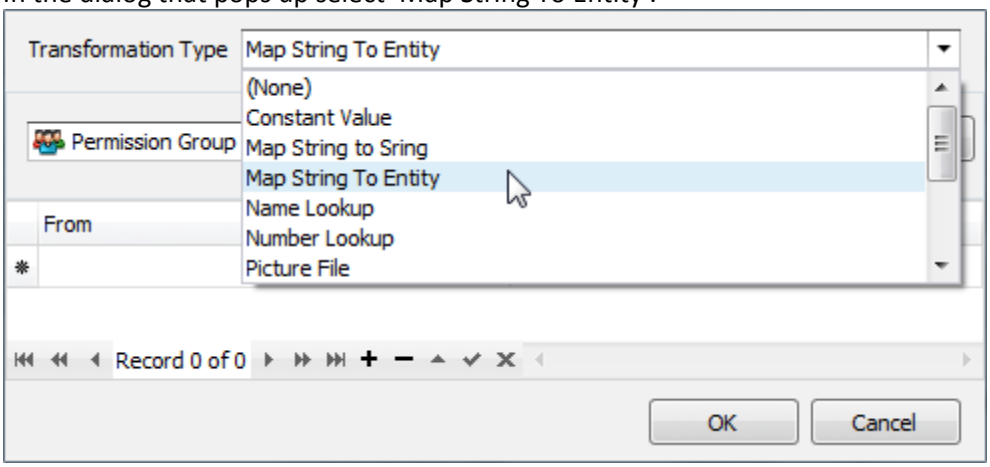


4. Click on the 'Transformation' property of the 'What' property mapping and select '…'.

EITHER:

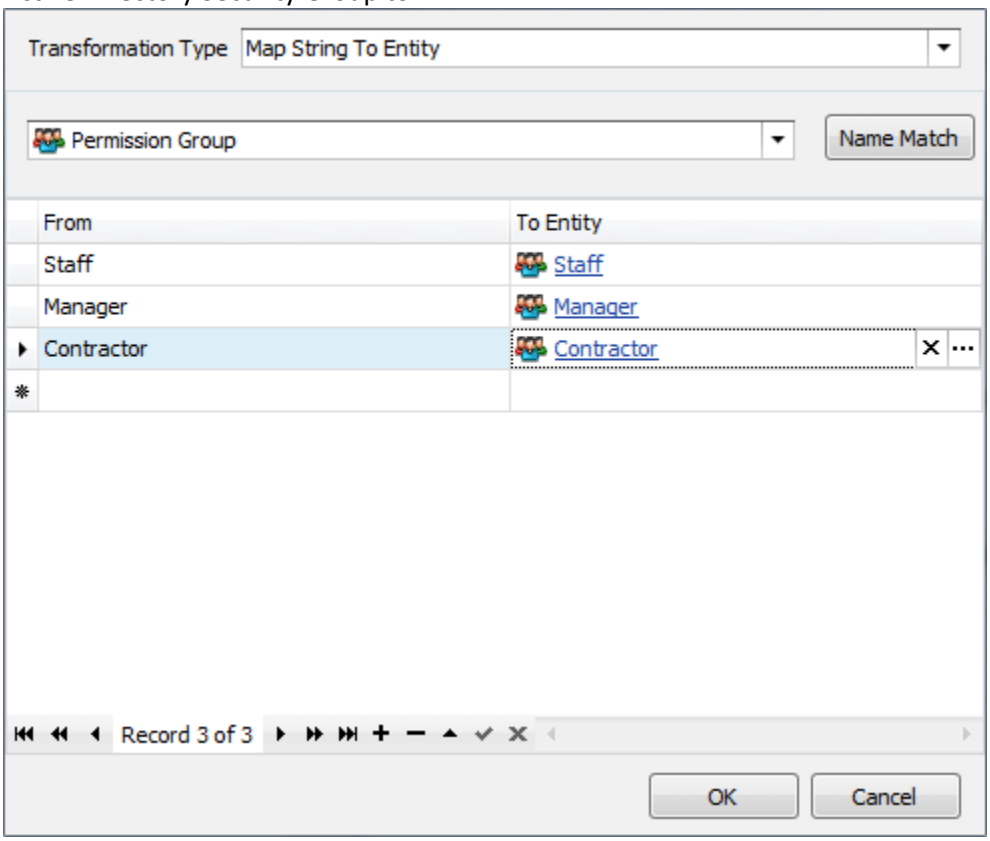
5.

a. In the dialog that pops up select ‘Map String To Entity’.



b. In the ‘From’ column type the name of each Security Group found in Active Directory.

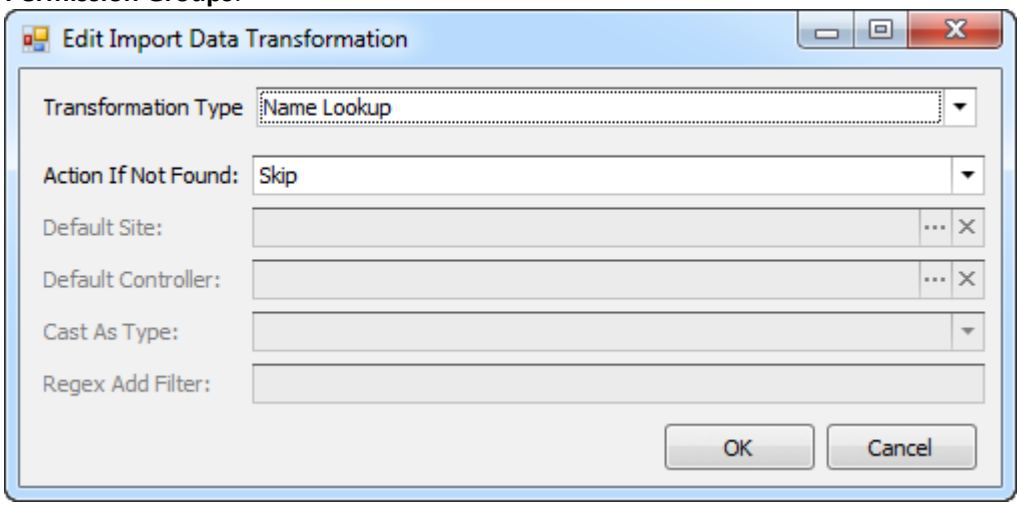
c. In the ‘To Entity’ column select the Integriti Permission Group to match each Active Directory Security Group to.



OR (if the security group names are the same in both Integriti and Active Directory):

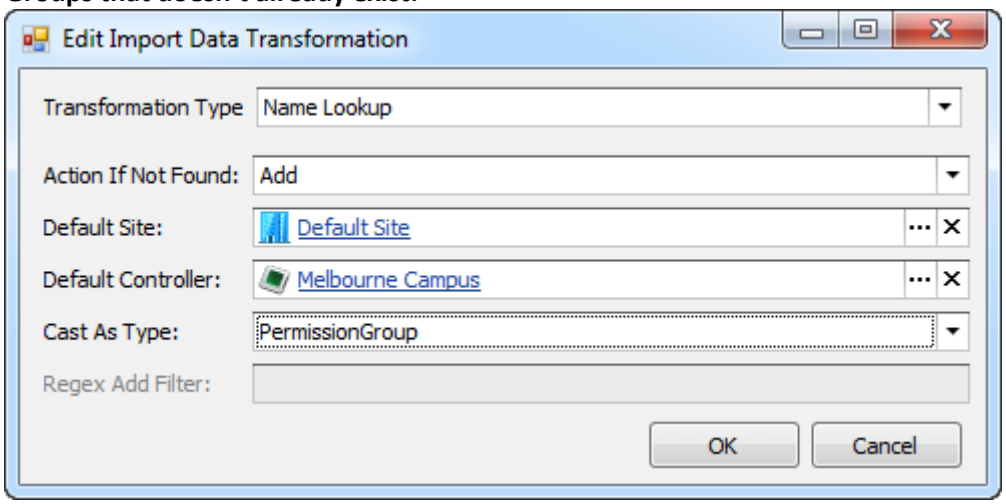
a. In the dialog that pops up select 'Name Lookup'. This will automatically find the corresponding Integriti Permission Group from the name of the Active Directory Security Group.

To only add permissions for Active Directory Security Groups that map to Integriti Permission Groups:



Leave the 'Action If Not Found' property as 'Skip'.

To automatically add a new Integriti Permission Group for any Active Directory Security Groups that doesn't already exist:

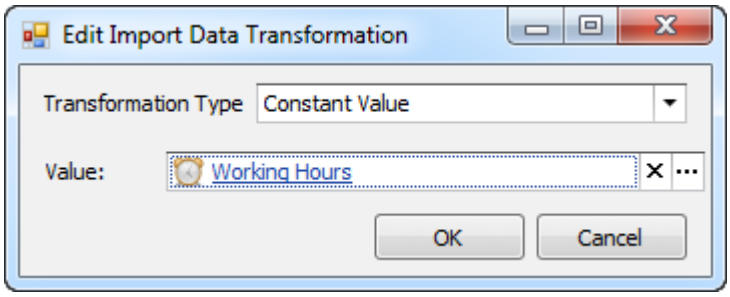


i. From the 'Action If Not Found' dropdown select either 'Add' or 'Add If Match Regex'
ii. Select the Default Site to add newly created Permission Groups to.
iii. Select the Default Controller to add newly created objects to.
iv. In the 'Cast As Type' dropdown select 'PermissionGroup' to create new Integriti Permission Groups.
v. Optionally (if 'Action Not Found' is set to 'Add If Match Regex') to only add Permission Groups with names that match the given Regular Expression.

1. Select ‘Ok’ in the Transformations dialog box to save the transformation settings.
2. In the list of property mappings under the ‘Permissions’ mapping, set up mappings for any other properties of the Permission to be set by the synchronisation. This can be done by:
    a. Selecting an Active Directory column in the Column Name (with or without a transformation, depending on the property) to map the property to.

OR (to have a constant value across all Permissions created)

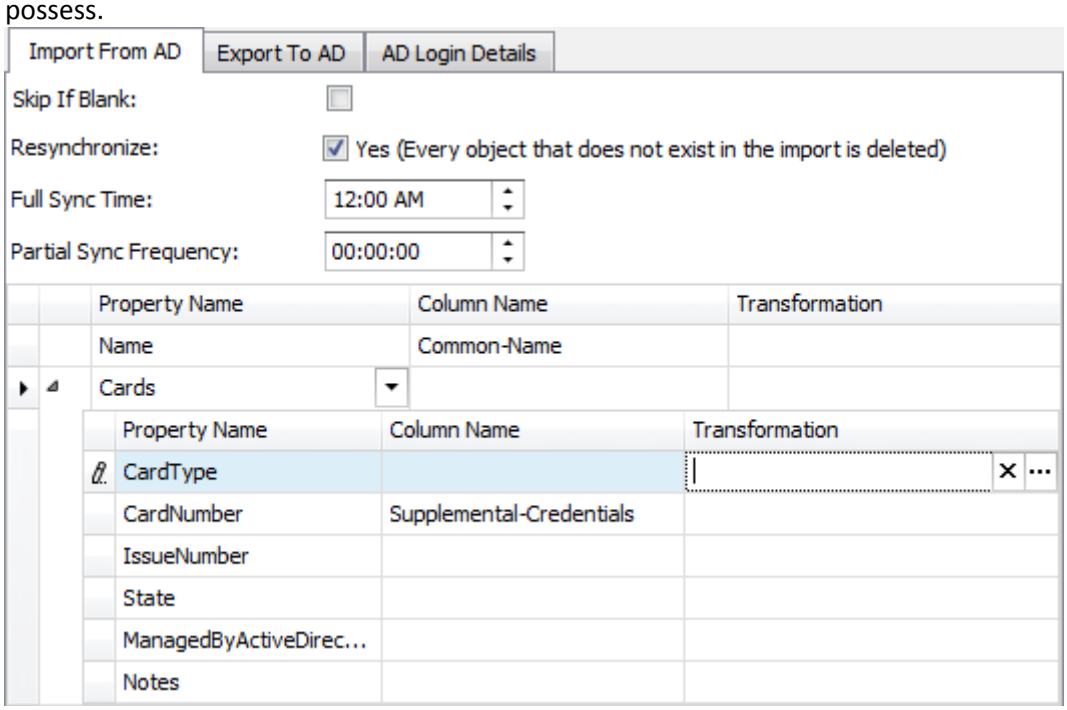
    b.



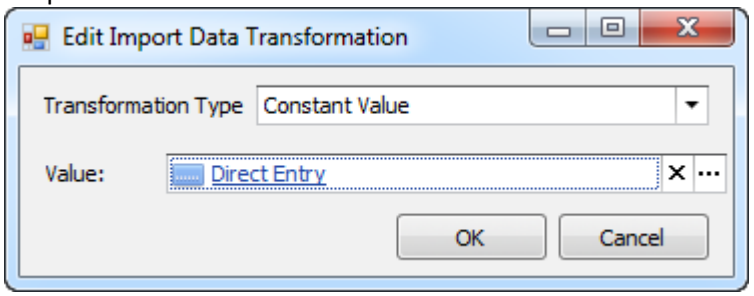
        i. In the ‘Transformation’ column of the property to be mapped select ‘…’.
        ii. In the dialog that pops up select ‘Constant Value’.
        iii. In the ‘Value’ field either:
            1. Select ‘…’ and select the Integriti entity to use as the mapping for that property for all Permissions created by the synchronisation
            OR
            2. Enter a string representation of the value to use for all Permissions created by the synchronisation.
3. Select ‘Ok’ in the Transformations dialog to save the transformation settings.
4. Save the Communications Handler. When the Communications handler is saved, the initial full synchronisation of the AD users.

Assigning multiple Active Directory Credentials to Integriti User Credentials

1. In Active Directory add an extra field to store the User's credential (if there isn't already one set up). This must be populated with the Card numbers that the User's possess.



2. In the edit dialog for the Active Directory Communication Handler in Integriti add a new property mapping to the Import Configuration Table.
3. Under 'Property Name' select 'Cards'.
4. In the list of property mappings that appears under the 'Cards' mapping, set the 'Column Name' next to the 'Card Number' property mapping to the name of the new field added in step 1.
5. In the list of property mappings under the 'Cards' mapping, click on the 'Transformation' property of the 'Card Type' mapping and select '…'.
6. In the dialog that appears select 'Constant Value' from the 'Transformation Type' dropdown.



7. Select '…' in the Value property and double click the Card Type to use for any synchronised cards from the list of possible Card Templates.
8. Select 'Ok' in the Transformations dialog box to save the transformation settings.
9. Save the Communications Handler. When the Communications handler is saved, the initial full synchronisation of the AD users.

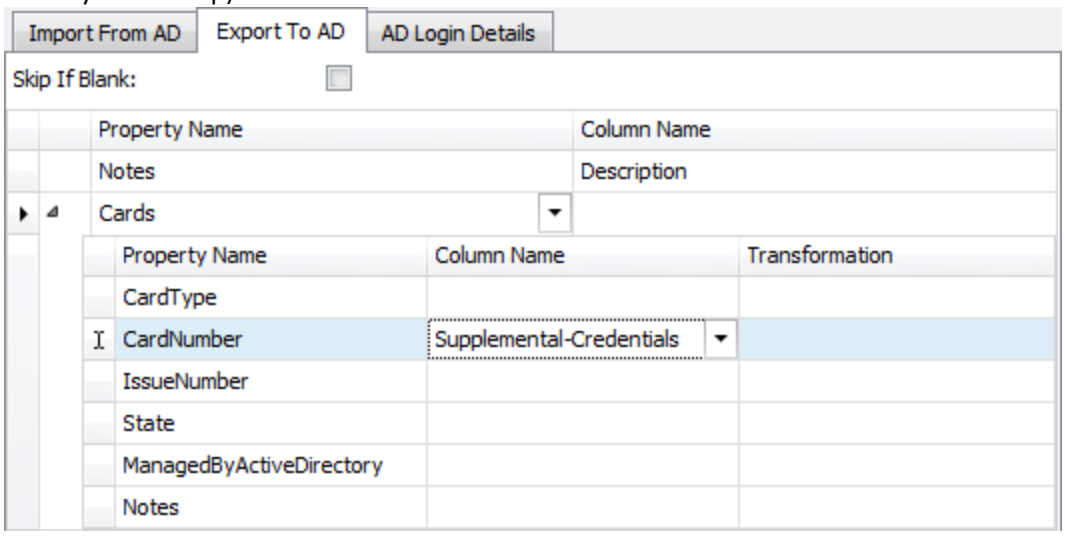
Exporting To Active Directory From Integriti

To export changes made to users in Integriti to the corresponding user in Active Directory the following steps must be taken:

1. Follow the above instructions to configure the Active Directory Synchronisation.
2. In the 'Import To AD' tab enter at least one mapping (of any property) into the Import Configuration Table. This allows an initial import to be performed that links the imported Integriti users to the Active Directory users.
3. In the 'Export To AD' tab fill out the Export Configuration Table with mappings for each property to be synchronised. See below for instructions on configuring mappings for specific use cases.
4. Save the Communications Handler. When the Communications Handler is saved an initial import of users and settings from Active Directory will be carried out based on the settings and import mappings provided.
5. After the initial import any future changes to a property of one of the imported users that has been mapped in the Export Configuration Table will be exported to the mapped property in the corresponding Active Directory user.

Exporting Integriti User Credentials to Active Directory User

1. In Active Directory add an extra field to store the User's credential (if there isn't already one set up).



2. In the edit dialog for the Active Directory Communication Handler in Integriti add a new property mapping to the Export Configuration Table.
3. Under 'Property Name' select 'Cards'.
4. In the list of property mappings that appears under the 'Cards' mapping, set the 'Column Name' next to the 'Card Number' property mapping to the name of the new field added in step 1.
5. Save the Communications Handler. When the Communications Handler is saved, any future changes to an Integriti User's cards will be exported to the Active Directory field added in step 1 for the selected user.