

Legacy Active Directory User Import

Legacy systems – Importing Users from Active Directory

Newer Systems use AD-Sync Tool

(OBSOLETE) System Galaxy v10.5.6 | JAN 2018



A How-To Guide
*For Importing users
from Active Directory*

Information in this document is subject to change without notice.
Therefore, no claims are made as to the accuracy or completeness of this document.

2nd edition JAN 2018

Copyright © 201 ♦ Galaxy Control Systems ♦ All rights reserved

No part of this document may be reproduced, copied, adapted, or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Galaxy Control Systems. Copyright protection claims include all forms and matters of copyrighted material and information, including but not limited to, material generated from the software programs, which are displayed on the screen such as icons, look and feel, etc.

Trademarks

Microsoft®, Windows®, Active Directory® and SQL Server® are registered trademarks of Microsoft Corporation in the U.S. and other countries.

Adobe®, Acrobat® are registered trademarks of Adobe Systems Inc.

This PDF is created with Adobe.

Graphics and illustrations by Candace Roberts, SQA & Technical Writer.

Galaxy Control Systems

3 North Main Street
Walkersville MD 21793
800.445.5560

www.galaxsys.com

TABLE OF CONTENTS

System Galaxy 10.x Active Directory Integration Notes.....	4
Requirements.....	4
Configuration	7
GCSActiveDirectoryChangeMonitor tool	7
GCSActiveDirectoryService	8
Encryption	9

Revision / Date	Changes
SG 10.3	AD Support introduced, using MS Server 2008 R2 operating system.
SG 10.5.1	2 ND Edition – changes include: <ol style="list-style-type: none"> 1. Update cover 10.5.1, 2. update OS support for 2008 R2 “(OR LATER)”. 3. Notice that changes in software provide greater scope of support for AD, transparent to user setup instruction document(this guide).

System Galaxy 10.x Active Directory Integration Notes

Summary: The integration allows user accounts in Active Directory to be pushed into the System Galaxy database manually or automatically. Along with textual data the user account can be assigned access profiles and badge templates. Any changes in Active Directory after that point can be pushed into the System Galaxy database automatically.

There are two new applications that provide the active directory integration capabilities:

GCSActiveDirectoryChangeMonitor

- Windows application for manually importing users as well as changes from active directory into the System Galaxy database. It also will set the parameters needed in the GCSActiveDirectoryService service.

GCSActiveDirectoryService

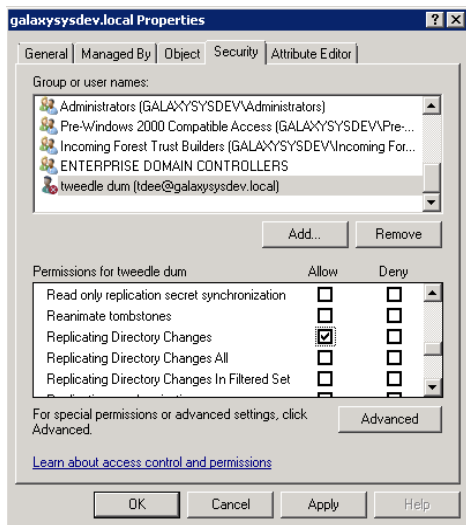
- Windows service that polls active directory for changes (new additions, updates and deleted users)

Requirements

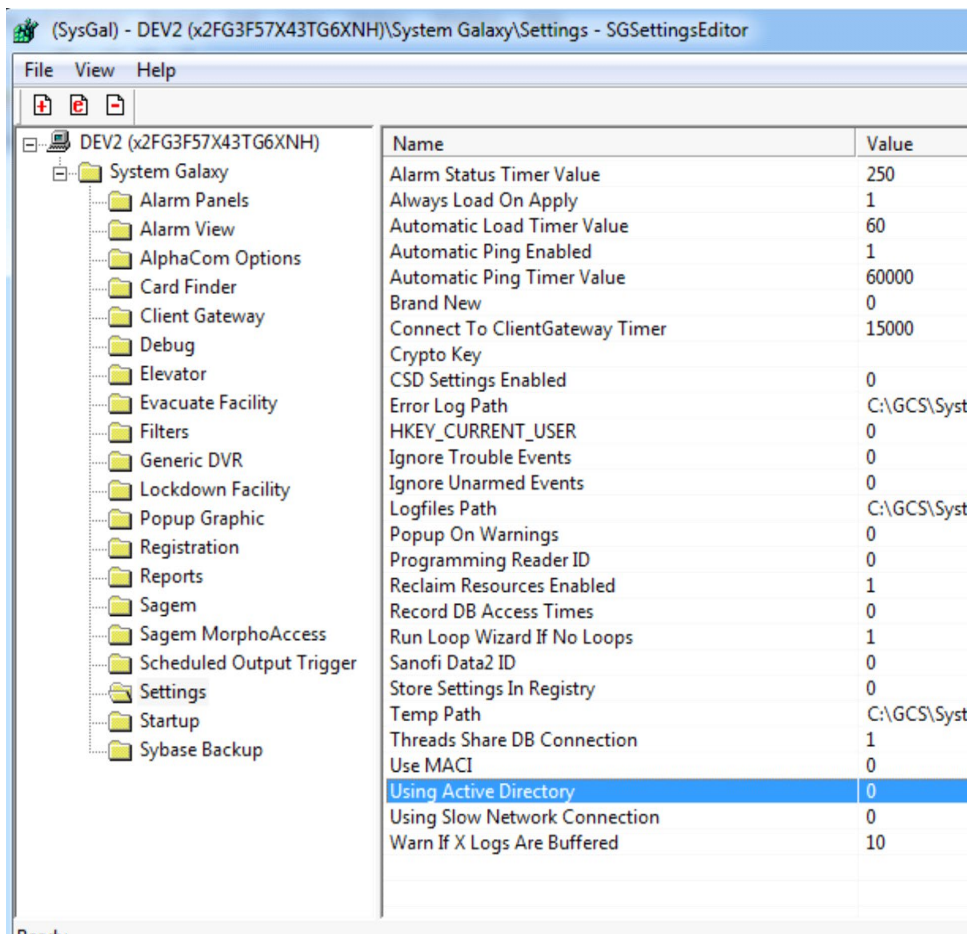
This integration is only supported using Active Directory provided with Windows Server 2008 R2 (or later) and System Galaxy 10.x. Any attempts to use this feature with other versions of SG and AD may work but will not be supported by Galaxy Control Systems.

Contact Galaxy Control Systems Certified Dealer for Questions.

- 1) PC needs to be already joined to the domain.
- 2) Users signed into Windows domain must have "replication directory changes" permissions in AD to use the GCSActiveDirectoryChangeMonitor program.
- 3) A domain user account must be assigned to the GCSActiveDirectoryService service to run and must have "replication directory changes" permissions in AD. Go to root of domain and assign user account REPLICATING DIRECTORY CHANGES



4) There is no registration feature for AD. It however needs to be enabled in SG Settings Editor. Set value to 1.

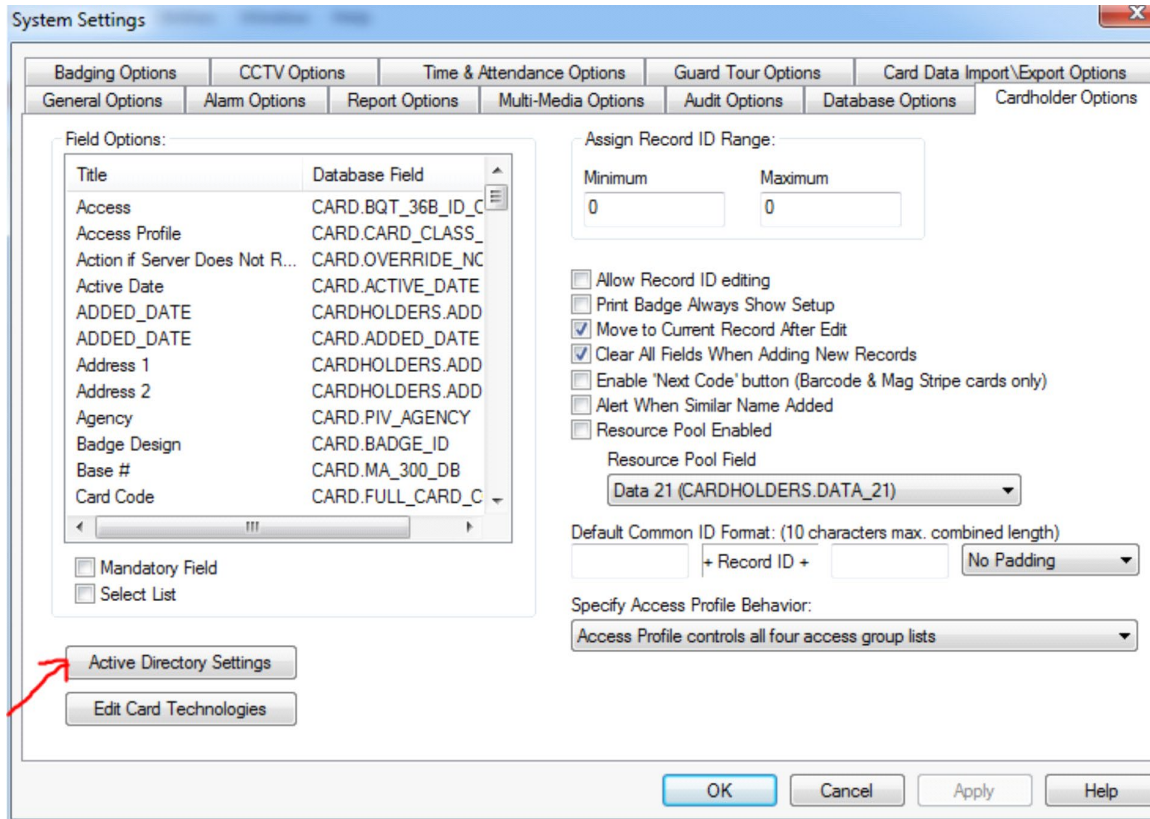


5) GCSDataloader service must be running for changes to take affect.

6) (Optional) Map fields between SG database and AD database. System Settings->cardholder options. The following fields are already mapped:

FirstName
LastName
HomePhone
Phone
State
Zip Code
Address 1
Address 2

Note - use the GCSActiveDirectoryChangeMonitor tool to see the AD column header names.

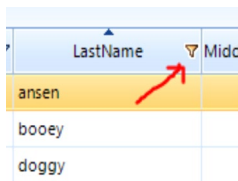


Configuration

GCSActiveDirectoryChangeMonitor tool

Summary: Use the tool to initially push desired cardholder accounts from AD into the System Galaxy database. Afterward, the GCSActiveDirectoryService service will add/modify/disable cardholder records automatically.

- 1) Launch the GCSActiveDirectoryChangeMonitor tool - %system drive%\GCS\System Galaxy\OptionalServices\ActiveDirectory\ and logon using SG credentials.
- 2) Click on [Read All AD Users] to list all AD user accounts. It is possible to filter by column so only selected records will be pushed to the System Galaxy database. Click on on the filter icon next to the column header name and select desired records.



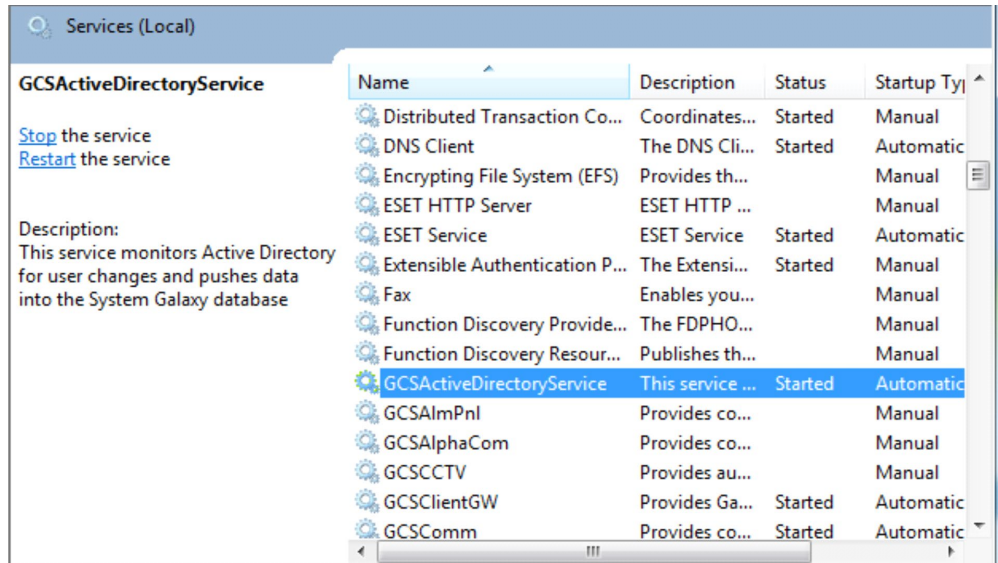
LastName	Midc
ansen	
boeey	
doggy	

- 3) Verify settings for [Default Card Options:] section. There are three important settings to choose from in this section pertaining to access assignment.
 - a) [Use person's active directory primary group as their access profile]. This option will automatically create an access profile within System Galaxy with the same name as the primary group for the user account in Active Directory. The default primary group for all user accounts in AD is domain users.
 - b) [Always assign default access profile]. This option will assign all selected user accounts a default access profile that is created in System Galaxy. You must choose a default profile to assign from the [Select Default Access Profile] dropdown list. This list will only populate if access profiles were created in SG beforehand.
 - c) [Do not assign any access profile]. No profiles will be assigned to selected user accounts.
- 4) Click on [Edit Settings] for the GCSActiveDirectoryService service. Additional settings need to be configured before they can be saved the service itself.
 - a) The default location for the log and cookie will work in most cases. Change to desired path if necessary.
 - b) Fill in the username and password field and click [ok] to save settings.
- 5) Determine how frequently the GCSActiveDirectoryService service will look for changes and click on [Save Settings For Service] button to save all the configuration parameters for the service.
- 6) Verify the correct user accounts are shown in the list and click on [Push AD Users to System Galaxy DB] button. Check within the System Galaxy to verify user account have come across with the proper information.
- 7)(Optional) Edit an Active Directory user account to make sure the changes are updating within the specified time set for the GCSActiveDirectoryService service.

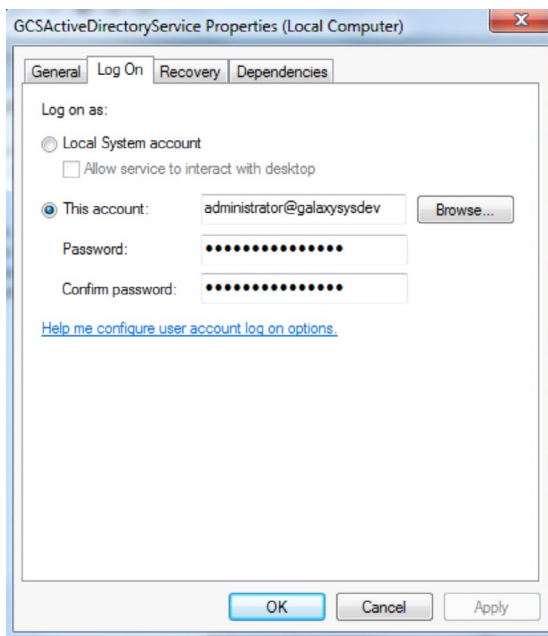
GCSActiveDirectoryService

Summary: Service will automatically add/modify/disable user accounts from Active Directory to the System Galaxy database.

- 1) The GCS Active Directory Service will install automatically with Part 3 of the Galaxy Software install and will be set to startup **MANUALLY**.
- 2) Verify service has installed properly, in the Windows service manager screen. You must edit the service properties and configure it to run **AUTOMATICALLY**.



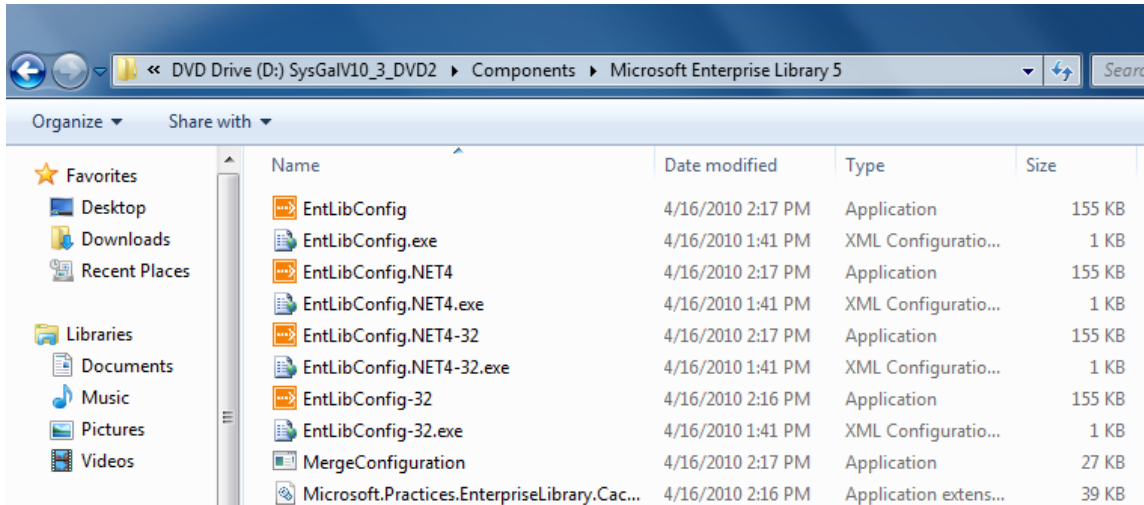
- a) Assign a domain user to the service.



Encryption

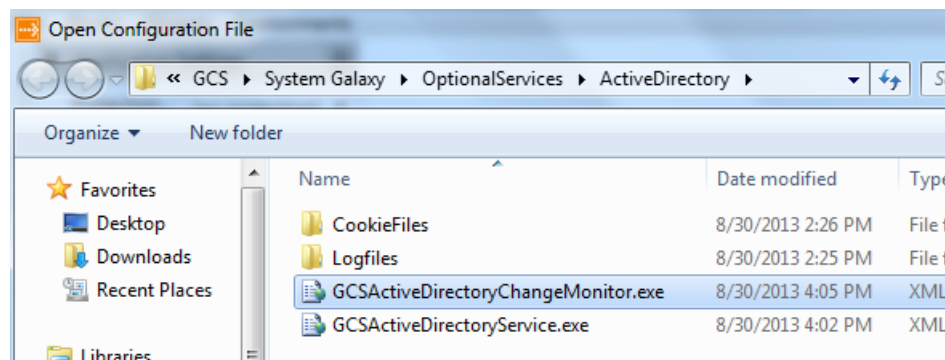
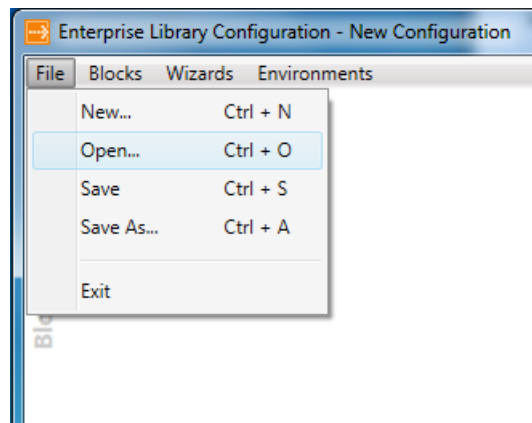
Summary: You can encrypt and decrypt the data in a configuration file's configuration sections. A configuration section contains the configuration information for an application block.

The Microsoft Enterprise Library Configuration Tool, located on disk2, must be used to edit and encrypt the database connection string. The file location is %optical drive%:\Components\Microsoft Enterprise Library 5:

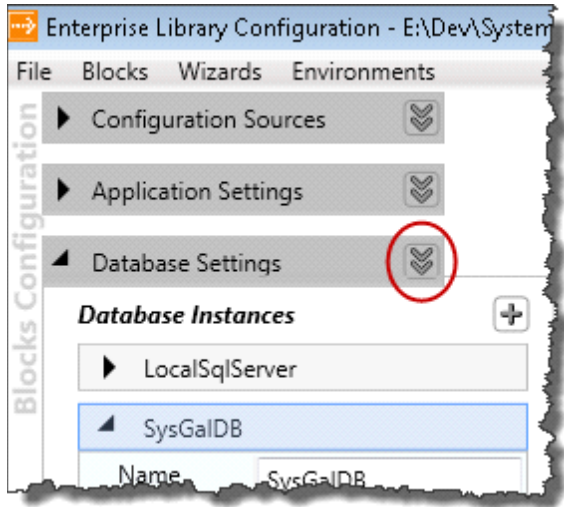


1) Execute the Enterprise Library configuration utility (EntLibConfig.NET4.exe or EntLibConfig.NET4-32.exe)

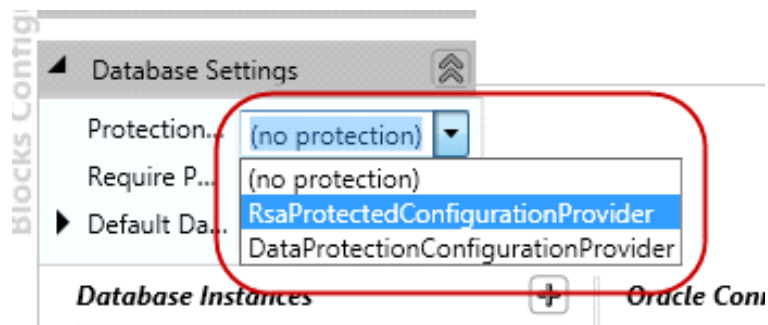
Open the application configuration file and select the desired AD configuration files:



2) Expand the desired section to be encrypted; in the example DATABASE SETTINGS is selected. Click on the double arrow icon highlighted below.



3) Choose the desired encryption method (refer to *Encrypting Configuration Data*)



4) Save the configuration file.

5) Open the configuration file with notepad and verify the appropriate sections are encrypted.