

# Active Directory- GCS AD Change Monitor (NEW)

How to import Active Directory Users into the System Galaxy database and synchronize cardholder data.

- Configuring Prerequisites in SG
- Sign-in & Connect to the AD Controller
- Configure the Field Mapping
- Configure Data Synchronization Settings
- Manage Change Cookies
- Configuring Cardholder/Card Options
- Configure AD Service Settings
- Fetching AD User Groups / User Filtering
- Performing an import or synchronization

SG 11.8.6 | 2024

---

Contents

OVERVIEW .....3

    HOW IS AD USER DATA IMPORTED/PUSHED .....3

    HOW ARE CARD DATA, ACCESS PRIVILEGES, AND BADGE TEMPLATES IMPORTED/PUSHED .....3

    HOW IS AD USER DATA SYNCED/UPDATED.....3

    HOW ARE CARDHOLDERS HANDLED WHEN USERS ARE DELETED FROM ACTIVE DIRECTORY .....3

    HOW DATA IS IMPORTED & UPDATED .....3

REQUIREMENTS.....4

    TERMS IN THIS GUIDE .....5

INTEGRATION REQUIREMENTS FOR AD-SYNCHING: .....6

SYSTEM GALAXY PREREQUISITE PROGRAMMING.....9

    ABOUT INSTALLING SYSTEM GALAXY & INTEGRATED SOLUTIONS.....9

    ABOUT REGISTERING SYSTEM GALAXY .....9

    ABOUT PROGRAMMING SYSTEM GALAXY PREREQUISITES .....10

    CREATING A CUSTOMER .....10

    CREATING AN SG OPERATOR .....11

    CREATING AN ACCESS PROFILE.....13

    CREATING AN BADGE TEMPLATE.....14

CONFIGURING THE GCS AD CHANGE MONITOR APP.....15

    SIGNING-IN TO THE GCS AD CHANGE MONITOR APP .....15

    CONNECTING TO AD DOMAIN CONTROLLER .....16

    CONFIGURE FIELD MAPPING .....17

    CONFIGURE CARDHOLDER SYNCRONIZATION SETTINGS .....18

    CONFIGURE COOKIE RETENTION SETTING .....19

    CONFIGURE DEFAULT CARD OPTIONS .....19

    CONFIGURE GCS ACTIVE DIRECTORY SERVICE .....21

    SAVING CUSTOMER SETTINGS.....22

    MANAGING CHECKPOINTS .....22

Manually Importing AD Users into System Galaxy Database .....23

    FETCHING USERS .....23

## OVERVIEW

The **GCS Active Directory Change Monitor App** (i.e. AD App; APP) supports importing individual **Active Directory Users** into the System Galaxy database as corresponding cardholder records. Likewise, the **GCS Active Directory Change Monitor** supports updating and disabling cardholder records in the System Galaxy database whenever the corresponding AD Users are modified or deleted from the AD Domain. (AD Change Monitor App first released with SG 11.8.5 API.)

### HOW IS AD USER DATA IMPORTED/PUSHED

Importing new cardholders is accomplished by selecting the Org Unit and User Group(s) desired, then running the **Get Users** function to fetch the Users from chosen AD User Groups and then Push them into the SG Database. The initial import would be done manually, and the App would automatically continue syncing/updating the users through the GCS AD Service and saved customer settings.

### HOW ARE CARD DATA, ACCESS PRIVILEGES, AND BADGE TEMPLATES IMPORTED/PUSHED

The SG Operator can also choose to add a card record and include card data, access privileges and badge settings along with the AD User import (push), based on saved *Customer Settings* that are preconfigured in the **GCS AD Change Monitor App**. App and GCS AD Service refresh is required.

### HOW IS AD USER DATA SYNCED/UPDATED

AD User Data is synchronized based on the field that is selected *Synchronization Column* in the **GCS Active Directory Change Monitor App**. The Sync Column is a column from the SG Database. In the Field Mapping, an AD Property must be mapped to the selected SG Column and that column must be chosen as the Sync Column. The field used to sync by must have unique data for every single user record. This data is part of the saved Customer Settings in the **GCS Active Directory Change Monitor App**.

The synchronization will automatically occur when the Poll Interval elapses in the Customer Settings of the **GCS Active Directory Change Monitor App**, provided the GCS AD Service is running.

### HOW ARE CARDHOLDERS HANDLED WHEN USERS ARE DELETED FROM ACTIVE DIRECTORY

When an AD User is deleted from the domain then a delete cookie (checkpoint) will be created. When the **GCS Active Directory Change Monitor App** detects the checkpoint, it will deactivate the corresponding cardholder in System Galaxy.

System Galaxy does not delete cardholders or cards because it will delete the card and cardholder activity. Instead, the system deactivates the cardholder and keeps the activity history intact.

### HOW DATA IS IMPORTED & UPDATED

The SG Operator for a designated Customer will sign-in to the **GCS AD Change Monitor App** and configure the AD Field Mapping, Synchronization Settings, Default Card Settings, and GCS AD Service Settings as desired. The Operator will also designate which OU and User Groups to be fetched/synchronized.

Once the SG Operator is satisfied with the settings, the settings must be saved and then the AD App and GCS AD Service must be restarted to pick up the new settings.

After saving the Customer Settings, the Operator can fetch the desired User Group and run a manual push to import AD Users into the database for the specified customer. From there the App will periodically synch the AD Users. based the timing of the Poll Interval and the Synch Column and Customer designation.

The GCS Web API Service must be running for the Synchronization/updates to be done.

## REQUIREMENTS

1. **System Galaxy Registration:** System Registration must be completed and must include the Badging System if idProducer is being used to create badges. The idProducer software/web client must be installed before the System Registration is done.
2. **In System Galaxy, the relevant System Programming must be completed before you can import AD Users.** A *System Administrator (master operator)* must create the necessary system entities. The **Customer Name(s)**, **SG Operator(s)**, **Access Profile Name(s)**, and **Badge Template(s)** must be created in System Galaxy before they can be seen and used in the *GCS Active Directory Change Monitor App*.
3. (if used) **Customer Names:** The *Customer Name(s)* must be created in System Galaxy before they can be assigned to a System Operator if Customers are being used. The Customer Name must also be assigned to the Access Profile(s), and Badge Template(s) before you set up the *Active Directory Change Monitor App*.

A customer can be assigned to more than one SG operator – meaning you can have an SG operator for each customer. Also the *GCS Active Directory Change Monitor App* will filter access profile and badge templates based on the Customer Name that is assigned to the SG Operator who is actively logged in.

4. **System Operator's Privileges within SG:** When an SG AD Operator Login is created in System Galaxy to run the *GCS Active Directory Change Monitor App*, you must assign the appropriate Customer Name and configure the correct editing privileges for the operator profile. When that Operator is signed into the AD Change Monitor App, their same assigned *Customer Name* will also be assigned to each cardholder that is imported from AD.
  - Check 'No Filters' checkbox option will allow importing user data without restrictions.
  - Uncheck 'Prevent Card Data & Access Privilege Editing' checkbox to allow importing without restrictions.
  - Set Cardholders option to "Full Editing" to allow importing cardholders without restrictions.
  - Ensure Access Privilege & Department are set Ignore Filters or set in such a way that they cannot affect your imports.
  - Cardholder Options are not *hidden* or not *view only* and cardholder tabs are all available.
5. **Access Profiles:** If you are going to "always assign the default access profile from the System Galaxy, then the Access Profile Name(s) must be created in SG and assigned to the same customer name as the SG Operator before you configure Customer Settings in *GCS Active Directory Change Monitor App*. If you will be using the AD Primary Group as the Access Profile, then the spelling of the Access Profile name in System Galaxy must exactly match the spelling of the AD Primary Group.
6. **Windows User Login must be an admin account:** If the *Windows User Login* that signs-in on the PC where the *Active Directory Change Monitor* is running is not an admin account, then a separate *User Login* that does have admin rights will need to be must be specified on the Log On properties for the GCS Active Directory Service. See the related instructions in this guide for more information.
  - a. Replicating Directory Changes
  - b. Replicating Directory Changes All
  - c. Access to the Sync Container
  - d. Network Permissions

## TERMS IN THIS GUIDE

AD	(acronym) Active Directory
AD App	(or GCS AD App) is the <b>GCS Active Directory Change Monitor App</b>
AD Domain Controller	The AD Domain Controller you must connect to in order to fetch and sync AD Users
AD User	The <i>user</i> or <i>user record</i> listed in Active Directory. AD Users are imported into SG database.
AD User Group (UG)	a User Group (UG) in active directory is a division of users within an Organizational Unit (OU).
AD Org Unit (OU)	The Organizational Unit (OU) in active directory, which contains multiple UGs.
AD Property	a column or field in the <i>Data Mapping</i> grid of the GCS Active Directory Change Monitor (AD App); a data field in Active
Checkpoints (cookies)	Checkpoints are <i>change cookies</i> or <i>delete cookies</i> that are created by AD when any modifications or deletions to User records occur in the AD Domain. GCS Active Directory Monitor will update SG Cardholders based on the information in the checkpoints (changes or deletions/deactivations).
Customer Name [SG]	In System Galaxy, the <i>Customer Name</i> is used to segment the data, such as the population of cardholders, badges, operators, access profiles, etc. The <i>customer name</i> that is assigned to the SG Operator will also be assigned to the new and updated cardholder records when AD Users are imported into the SG database.
Data Field [disambig.]	A data field is any column in System Galaxy database.
Data Field Mapping	In the <i>GCS Active Directory Change Monitor</i> (AD App), the SG Operator can map AD Properties to existing SG Cardholder Columns (fields).
Data_# Field (1 thru 5)	System Galaxy contains specific <i>Cardholder "Data Fields"</i> that can be designated/reserved for a specific purpose – i.e. to hold specific data that is mapped to an AD Property (field). Data_1 thru Data_5 can be mapped with an AD Property (if they are not already in use for another purpose).
Synchronization Column	the <i>GCS Active Directory Change Monitor</i> (AD App) uses a chosen field/column to uniquely identify and synchronize each/every AD User & SG Cardholder record during the Import/Update procedure.
SG	(acronym) System Galaxy software or feature or component.
SG Operator	An authorized user profile (login credentials) of the SG software or GCS Active Directory App.

## INTEGRATION REQUIREMENTS FOR AD-SYNCHING:

All these requirements apply to both *manual AD Synching* (pushing) or *automated AD Synching* at poll intervals.

### INSTALLATION REQUIREMENTS OF GALAXY SOFTWARE AND SERVICES

This section covers the System Galaxy [SG] installation requirements (of software, database, services, and integrated solutions) as they relate to supporting the **AD Change Management App** (AD Tool herein). For full System Requirements you must see the [System Specifications Guide](#).

1. *System Galaxy* software (v11.8.5 or higher) must be completely installed (**all 3 parts**) on the Main SG Server.
2. The System Galaxy Database (Database SQL Server) must be online.
3. If customer badging is being used, then the **SG IIS** must be installed from the **Galaxy Install Media** (USB/ISO).
4. **The Core GCS Services** will install to run automatically during Step-3, including GCS Web API Service.
5. The **GCS Active Directory Service** must be started and running to perform auto-synchronization at poll intervals.
6. idProducer Badging must be installed **after the SG IIS Component is installed, but before the SG System Registration is performed** as a part of normal requirements for idProducer. idProducer badge templates must be created before you can configure for any AD import settings or perform the AD importing.

### PROGRAMMING REQUIREMENTS RELATED TO AD SYNCHING

This section covers the installation requirements of System Galaxy Software as they relate to supporting the AD Change Management App (AD Tool herein). For full System Programming you must see the [System Galaxy User Guide](#).

7. You should create a System Operator login to be used for the AD Tool configuration and cannot have a blank customer field ...
8. **Customer Name** programming must be configured as needed ...
  - On-Premises Systems: you do not need to create a Customer Name. System Galaxy has provided a preprogrammed "\*\*\*No Customer\*\*" option for your AD Operator Login.
  - If you are using **Customer Names** (for advanced idProducer must be created before you create System Operators, as well as Access Profiles, and Badges if used. (Program in the Customer programming screen.)
9. A Galaxy **System Operator Login account** must be created for use with the AD Tool and the following must be satisfied:
  - It is recommended to make an SG Operator login that is named "**AD Operator**" for use only with the AD Tool. This will create clear audit-tracking reports that will show whether a change was made by the *AD Change Management App* or by an *SG Operator* from the Cardholder screen.
  - The Operator "**No Filters**" checkbox should be enabled. The No-Filters option will override any *operator filters & limits*, which could prevent the AD Change Monitor App from updating data or cardholders.
  - The **Customer Name field** must be assigned:  
On-Premises systems that are not assigning customers will use the preprogrammed "No Customer" option. If any system is using Customers, they must create the Customer Names and assign them to each AD Operator login . SEE IMPORTANT REQUIREMENT FOR WINDOWS OS PRIVILIGES ON NEXT PAGE.

10. **Windows User Login must be an admin account:** If the *Windows User Login* that signs-in on the PC where the *Active Directory Change Monitor* is running is not an admin account, then a separate *User Login* that does have admin rights must be specified on the Log On properties for the GCS Active Directory Service. See the related instructions in this guide for more information.
- **Replicating Directory Changes:** The account needs the "Replicating Directory Changes" permission on the domain or container you want the AD App to synchronize. This permission allows the account to read objects and attributes in the directory for the purpose of synchronization.
  - **Replicating Directory Changes All:** For forest-wide synchronization, the account needs the "Replicating Directory Changes All" permission on the configuration container of the forest. This permission allows the account to read objects and attributes in any domain in the forest for synchronization.
  - **Access to the Sync Container:** If you are using a synchronization container, the account needs read access to the objects and attributes within that container.
  - **Network Permissions:** The account needs network permissions to communicate with the domain controllers for synchronization purposes.
11. If you will be using the **GCS AD Change Monitor App** to insert *Card Data* along with the User personal data, then the following things must be created in System Galaxy software before you perform any AD Syncs/Pushes.
- a) The appropriate **Badge Template(s)\*** must be created in *idProducer* and badges must be imported into System Galaxy and the appropriate Customer Name must be assigned to the Badge before you configure the AD Tool.
  - b) The **Access Profile Name(s)\*** must be created with the Customer Name assigned – depending on the behavior you want to use in the AD Tool. See chart below ...

Card Behavior Setting	Purpose and Result
"Do not assign any access profile"	In this case, no <b>Access Profile Name</b> will be assigned to the imported Users by the AD Tool, even if other Card data is included in the AD User import/synchronization. Choose this behavior if you want to assign access privileges in SG <u>after</u> importing AD Users. (In this case, you can use Access Profiles, Access Groups, Personal Doors or any combination of access privileges, which can be created at any time independent of the AD Synchronization.)
"Always assign Default Access Profile"	In this case, the <b>Access Profile Name</b> must be already be created and assigned to the appropriate Customer Name in SG <u>before</u> the AD Tool Customer Settings are saved. If you do not see your Access Profile Name in the AD Tool, verify you have the correct Customer Name on your Operator Login, and that you have assigned the Customer to the Access Profile in SG. You can create one or more Access Profile Name for the same customer. The <b>Access Profile Name(s)</b> will be available in the <b>Default Access Profile droplist</b> whenever this behavior is chosen in the AD Tool. The term "default" here means that it will assign this Access Profile to all records being imported on the first import only. You can change the Access Profile later in System Galaxy and the AD Tool will not overwrite it because AD Tool Config Fields do not create change cookies.
"Use AD Primary Group as Access Profile"	In this case, the <b>Access Profile Name</b> will come from the AD Primary Group name. However, the Primary Group Name must already exist in SG as a real Access Profile Name with the exact same spelling – and with appropriate Customer assignment before the AD Tool performs the AD User import. This behavior will push the value that is stored in the AD Primary Group property for each imported user, and if it changes in the AD Domain, it will create a change cookie that the AD Tool will process to update the Cardholder – but the access card will not work until the Access Profile Name exists in SG with configured access rules.

\* If there is more than one *Badge Template* or *Access Profile* assigned to the same Customer as the SG Operator login, they will populate in their appropriate droplists in the Card Options group.

IMPORTANT: When you configure these Card Options you must [Save Customer Settings] in the **GCS AD Change Monitor App** **AND** restart **GCS AD Change Monitor Service** - **before** the AD Tool Pushes or Syncs data. Changes will not take effect until the settings are saved and the service is restarted. If you import users before saving and restarting service, then the imported cardholder records will not display the intended options you are trying to configure.

12. The **AD Domain Controller** connection parameters must be valid (IP Address, AD User Name and Password) to fetch users or perform any actions from the ACTIONS dropdown list in the **GCS AD Change Monitor App**.
13. The **AD Properties** (user data fields) must be populated appropriately with data that maps to SG Columns. SG Operator can map additional fields such a Cardholders.COMMON\_ID or DATA\_# (1 – 5).
14. The **AD Field Mapping** may need to be configured before you choose the Synch Column if nothing is mapped to the SG Column you want to Sync by – for example the DATA fields are unmapped by default.
15. Whenever you edit and **Save Customer Settings**, you must always restart the **GCS AD Service** to pick up the changes.
16. The **GCS AD Change Monitor App** can be launched from the System Galaxy Event Server.  
PATH: "C:\GCS\System Galaxy\OptionalServices\ActiveDirectory\GCSActiveDirectoryChangeMonitor.exe"



## SYSTEM GALAXY PREREQUISITE PROGRAMMING

Before you can use the GCS AD Change Monitor App, you must install and register System Galaxy and create the prerequisite system components that the *GCS AD Change Monitor* will need.

### ABOUT INSTALLING SYSTEM GALAXY & INTEGRATED SOLUTIONS

1. Install all 3 Steps of the System Galaxy software as per normal.
  - a. Install Step-1 Prerequisites on every Galaxy server and client,
  - b. Install Step-2 New SG Database & MSSQL Server on the computer where the database will reside.  
*Install Step-2 Native ODBC Client components on any client PCs (depending on your system needs).*
  - c. Install Step-3 System Galaxy Software and Services on the computer that is the *main event server*.  
*Install SG client software only on your client computers (depending on your system needs).*
2. IF YOU WILL BE DOING BADGING ...
  - a. Install IIS from the Galaxy Install Media before installing idProducer Web Badging Solution.
  - b. Install the idProducer Badging Solution if you will be creating ID Badges.

### ABOUT REGISTERING SYSTEM GALAXY

1. Launch System Galaxy Software from the desktop shortcut on the main Event server.
  - a. You will be prompted to create a master administrative operator name and password.
  - b. You will be prompted to sign-in to the software the master operator you just created.  
NOTE: you must be signed in as a master operator to create the programming needed.
2. Open the System Registration screen from SG Menu: **Configure > Options > Registration > System**.  
(Registration must be performed by the qualified Galaxy Dealer.)
  - a. Enter all the required Dealer information.
  - b. Set the product level and remaining system options according to the purchase agreement.
  - c. Be sure to choose the appropriate badging level and complete the registration code as required.  
NOTE: the idProducer Badging software must already be installed before you perform this registration so that the badging license is created correctly.
3. Close and restart your System Galaxy software.

## ABOUT PROGRAMMING SYSTEM GALAXY PREREQUISITES

This section covers how to program *prerequisite components* that you will need when configuring and operating the **GCS AD Change Monitor App**. Some of these components are mandatory and some are required depending on how you will configure customer settings in the AD Change Monitor app.

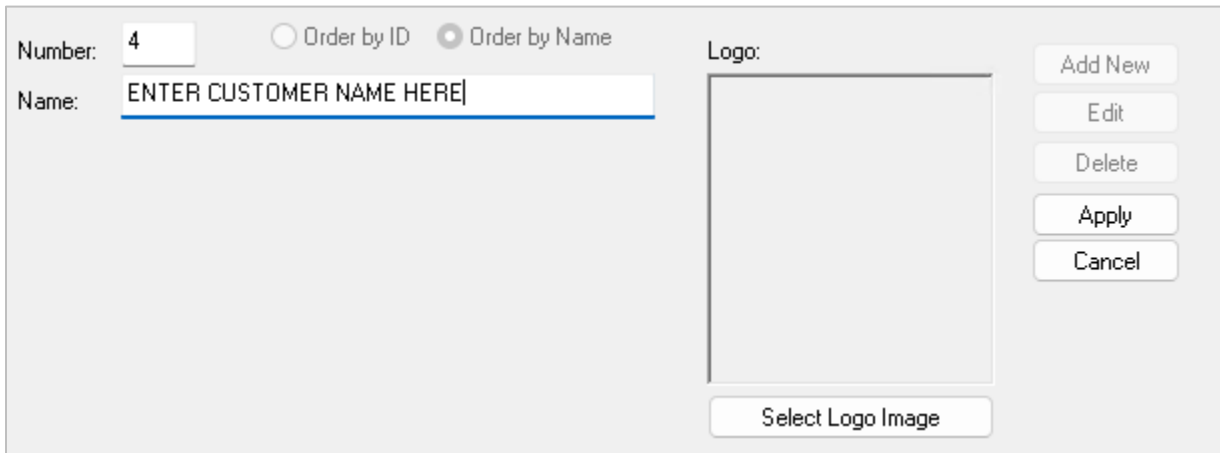
**IMPORTANT:** To create all the listed programming, you must be signed-in to System Galaxy using the master administrative credentials you created in the prior steps.

- Customer Names (mandatory)
- SG Operator Names (mandatory)
- Access Profile Names (mandatory if used)
- Badge Template Names (mandatory if used)

## CREATING A CUSTOMER

You must create the Customer Names first because you will need this for all the rest of the programming.

1. Open the Customer programming screen from SG Menu: **Configure > System > Customer**.
2. In the Customer screen, click ADD NEW.
3. Enter a Customer Name (and select a logo and complete any other programming as appropriate).



System Galaxy > Customer Programming screen (cropped)

4. Click APPLY to save your programming.

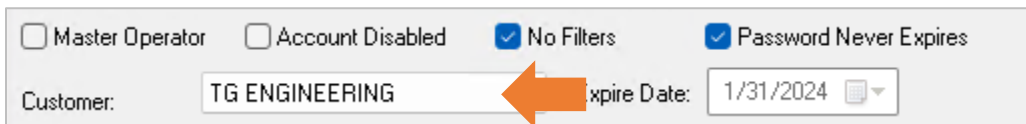
## CREATING AN SG OPERATOR

It is recommended you make a system operator that is dedicated to the purpose of AD synchronization.

- A. **No Customers or Basic Badging:** If you are not using Customer-subscriptions for basic badging, then you can make one AD Operator.
  - The AD Operator must be a No Filters operator in System Galaxy.
  - OS Login of the AD Operator must have the correct administrative rights within Active Directory
- B. **Customers or Advanced Badging:** If you are using Advanced idProducer Badging, you must make a separate AD Operator for each customer that will be importing/synching data from Active Directory.
  - Each AD Operator must be assigned to the appropriate Customer name it supports.
  - Each AD Operator must be a No Filters operator in System Galaxy.
  - OS Login of the AD Operator must have the correct administrative rights within Active Directory

**IMPORTANT:** Windows User Login that is used on the computer that the AD Tool will run on, must have Windows administrative rights and specific administrative rights within the AD Domain (i.e., ADUC or ADAC). See the prerequisites section of this chapter and the requirements section of the guide for login details.

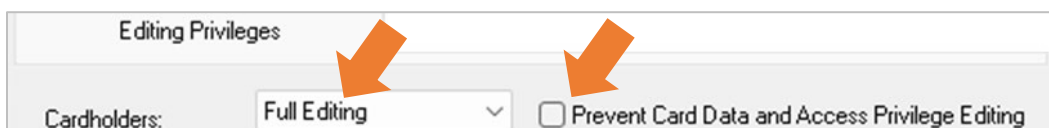
1. Open the Operator programming screen from SG Menu: **Configure > System > System Operator**.
2. In the Operator screen, click **Add New**.
3. Select the appropriate **Customer Name** for this Operator as appropriate or NO Customer if using basic badging.
4. Enter an **Operator Name** and enter the *password* and *confirmation password*.
5. By default, the **NO FILTERS** option is checked (which means SG will ignore any filtering or limited privileges you set for editing or viewing data. If you uncheck this, the system will use the privileges and filtering rules that are configured on the tabs below.



A screenshot of the 'SG Operator programming screen' showing configuration options. At the top, there are four checkboxes: 'Master Operator' (unchecked), 'Account Disabled' (unchecked), 'No Filters' (checked), and 'Password Never Expires' (checked). Below these, there is a 'Customer:' field with the text 'TG ENGINEERING' and an orange arrow pointing to it. To the right of the customer field is an 'expire Date:' field with the date '1/31/2024' and a calendar icon.

SG Operator programming screen (cropped)

6. Select the **Editing Privileges** tab ...
  - a. Set "Full Editing" for the Cardholders option in the.
  - b. Disable (uncheck) the "Prevent Card Data and Access Privileges Editing" option.



A screenshot of the 'SG Operator programming screen' showing the 'Editing Privileges' tab. The tab is titled 'Editing Privileges'. Below the title, there is a 'Cardholders:' field with a dropdown menu showing 'Full Editing' and an orange arrow pointing to it. To the right of the dropdown is an unchecked checkbox labeled 'Prevent Card Data and Access Privilege Editing' with an orange arrow pointing to it.

SG Operator programming screen (cropped)

7. Be sure you do not configure any limitations or filters that prevent data from being imported by the operator on the remaining tabs.
8. Click APPLY to save your programming.

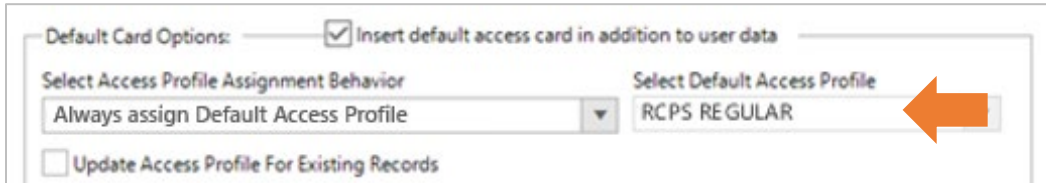
## CREATING AN ACCESS PROFILE

Skip this section only if you will not be using *GCS AD Change Monitor App* to set the Access Profile.

You need to create an Access Profile Name(s) for each *Customer* only if you are using the *GCS AD Change Monitor App* to insert the Access Profile Name (below).

### DEFAULT CARD OPTIONS ...

- "Do not assign Access Profile" ← Don't create Access Profile – skip to next section.
- "Always assign Default Access Profile" ← Must create Access Profile Name(s) for each Customer.
- "Use the Active Directory Primary Group ..." ← the Access Profile Name spelling must match AD exactly.

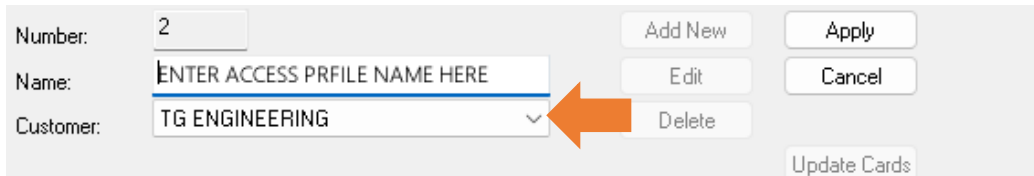


GCS AD Change Monitor App (cropped)

### REQUIREMENTS

- The Access Profile Name must have the Customer Name assigned.
- The *Galaxy Time Schedules* and *Access Groups/authorized doors* must also be created and assigned to the Access Profile before the cardholder will have working access privileges.
- A *Customer* can have more than one Access Profile. The Access Profiles will be listed in the droplist of the *GCS AD Change Monitor App*.

1. Open the Access Profile programming screen from SG Menu: **Configure > Cards > Access Profile**.
2. In the Customer screen, click **Add New**.
3. Enter an *Access Profile Name* and select the Customer Name.



SG Access Profile programming screen (cropped)

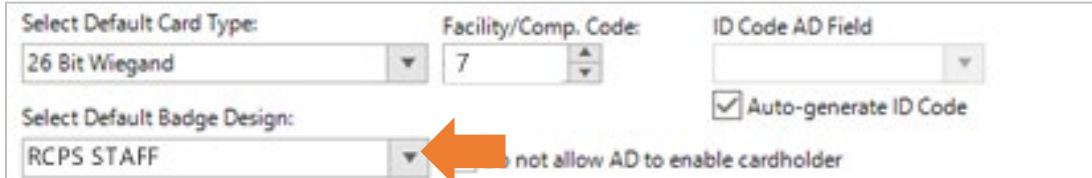
4. Complete the *Access Group* assignment in the programming screen as desired.  
(If you need instructions on creating *Schedule* and *Access Groups* see the [SG User Guide](#) for details.)
5. Click APPLY to save your programming.

## CREATING AN BADGE TEMPLATE

Skip this section only if you will not be using *GCS AD Change Monitor App* to set the Badge Template.

You need to create and import a Badge Template(s) for each *Customer* only if you are using the *GCS AD Change Monitor App* to insert the Badge Template Name (below).

### DEFAULT CARD OPTIONS ...

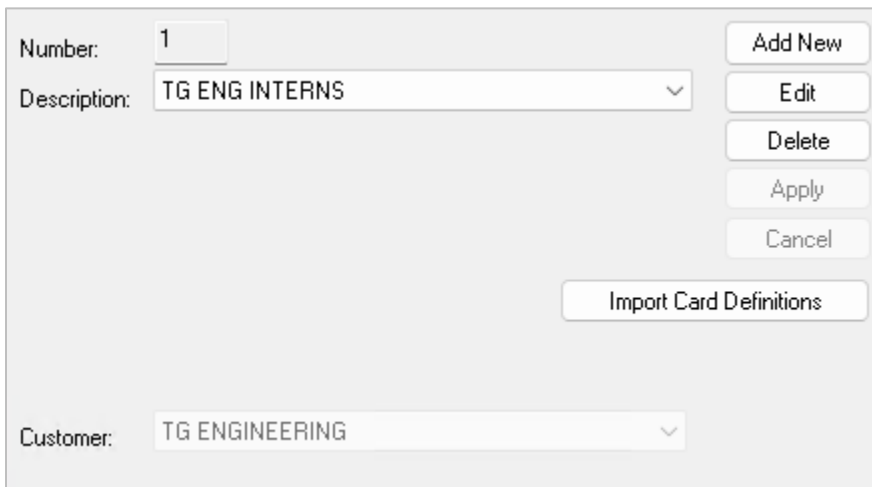


[GCS AD Change Monitor App \(cropped\)](#)

### REQUIREMENTS

- The Badge Template Name must have the Customer Name assigned.
- The Badge Template must have been created and imported into SG in order to appear in the Badge Layout screen. The badge import should happen automatically when the SG Operator signs-in to System Galaxy after saving the badge in the idProducer Client.
- A *Customer* can have more than one Badge Template.
- Badge Templates will be listed in the Default Badge Design droplist of the *GCS AD Change Monitor App*.

1. Open the Badging screen from SG Menu: **Configure > Cards > Badge Layouts/Designs**.
2. You should be able to see and select the Badge Name and see the the Customer Name is assigned to the Badge Template as desired.
3. If you do not see your Badge Template(s) here, then check the idProducer Client to ensure that the templates are created and saved for the appropriate Customer. Restart System Galaxy as needed to pick up the changes from the idProducer software. Refer to the [idProducer Guide](#) for more information.



[SG Badge Layout screen – already populated with Customer Badge Template](#)

4. Close the screen without making any changes.

## CONFIGURING THE GCS AD CHANGE MONITOR APP

The GCS AD Change Monitor App is installed during Part-3 of the System Galaxy Software installation.

### IMPORTANT

- The **GCS AD Change Monitor App** can be launched from the System Galaxy Event Server.  
PATH: "C:\GCS\System Galaxy\OptionalServices\ActiveDirectory\GCSActiveDirectoryChangeMonitor.exe"
- The AD Domain must be online, and the **GCS Active Directory service** must be running.
- The **AD Domain connection parameters** must be valid (IP Address, AD Username, and Password). And AD Domain credentials must have the appropriate permissions.
- All the Integration Requirements must be met (see Requirements section in this guide).
- The *Customer Settings* in the GCS AD App must be saved and the GCS AD Service refreshed before the AD Users can be properly imported.

### SIGNING-IN TO THE GCS AD CHANGE MONITOR APP

The SG Operator will sign into the **GCS AD Change Monitor App** using the appropriate SG Operator credentials. Then the operator must provide valid login credentials for the AD Domain Controller.

### IMPORTANT

- The **SG Operator** must be valid and active in System Galaxy and must have the correct editing privileges and Customer Assignment.
- The *Customer Name* that is assigned to the SG Operator will be assigned to all the imported AD Users (cardholders) when the Cardholder Synchronization (import/update) happens.

1. Ensure the **GCS Active Directory service** is running.
2. Navigate to the Galaxy **Active Directory** folder and launch the **GCS AD Change Monitor App**  
PATH: "C:\GCS\System Galaxy\OptionalServices\ActiveDirectory\GCSActiveDirectoryChangeMonitor.exe"
3. Enter valid **SG Operator credentials** in the Sign-in screen to log into the **AD Change Monitor App**.
4. The **Customer Name** should auto-fill (based on the assigned customer in System Galaxy Operator programming).

NOTE: Cardholder Synchronization (User import/update) will happen automatically at the designated Poll Interval after the customer settings are saved and the GCS AD Service is refreshed. Otherwise the App can manually push an import/update when the SG Operator clicks the [Push AD Users] button.

SG Operator/Customer Information:

SG Operator: Administrator

SG Customer: GCS Corporation

Active Directory Domain Credentials:

Domain/IP Address: 192.168.24.1

User Name: cs.county.k12.md.us\administrator

Password: .....

AD2016TEST

Test AD Connection

## CONNECTING TO AD DOMAIN CONTROLLER

You must provide valid AD credentials and click the *Test AD Connection* button to connect to Active Directory.

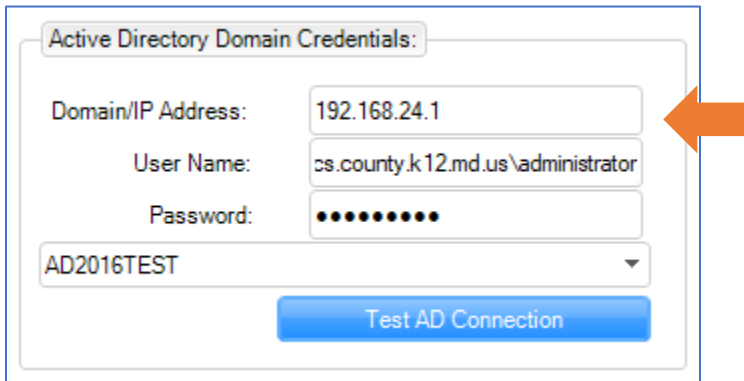
### IMPORTANT

- The AD Credentials must have the appropriate permissions on the domain to support fetching User Data in this tool.

### STEPS

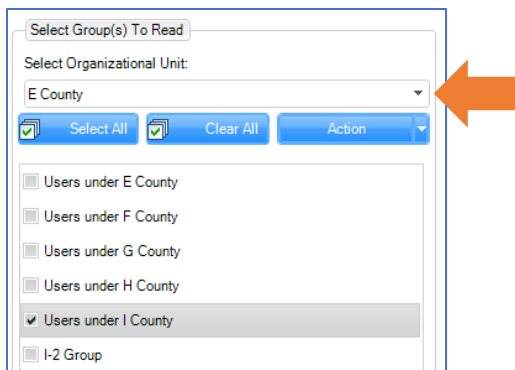
1. Enter the AD **Domain IP Address**.
2. Enter the AD **Username** with domain name ( i.e., domain-name\user-name ).
3. Enter the AD **Password**.
4. Click the [**Test AD Connection**] button: this makes a connection attempt to the AD Domain Controller using the credentials you provided.

RESULT: Immediately the App populates the *Select Groups List* with available Org Units & AD User Groups.



GCS AD Change Monitor App (cropped) > AD Domain Login

5. Click OK to close the **Connection Successful** message box to continue.
6. In the *Select Groups List* choose the desired Org Unit to filter the User Groups
7. Then place a *checkmark* in the checkbox of the User Group(s) you want to fetch records from.
  - Use the [Select All] and [Clear All] buttons to select/clear all the User Group checkboxes in the List.
  - Use the [Action] droplist to fetch User Groups



GCS AD Change Monitor App (cropped) > AD OU & User Group Selection



## CONFIGURE FIELD MAPPING

The AD Change Monitor App comes with the basic AD Field Mapping already configured. If you are satisfied with the default mapping, skip this section, and go to Setting Synch Settings (next section). Otherwise configure any additional AD Properties as appropriate.

### PREREQUISITES

- Before you configure the *Sync Column* and other settings, you might need to edit your field mapping to configure any remaining fields you will need to use – such as SG Cardholders.Data# fields.
- Make sure your Data fields are not already in use for another purpose or by another process that is integrated with System Galaxy before you map AD Properties to an SG Data field.

### IMPORTANT NOTICE

- Be sure the SG Column that you plan to use as your ‘Synch Column’, is mapped to the appropriate AD Property
- Ensure that the mapped AD Property will always have unique data for every individual cardholder. The accuracy of the import and update of AD Users depends on the integrity of the unique data in the Sync Column.

### STEPS

To change an existing mapped field or to add a newly mapped field, you must click on the field in the **AD Property** column.

1. In the *Field Mapping Table*, find the **SG Column** you wish to map – such as COMMON\_ID, DATA\_# (1 – 5), etc.
2. Click in the **AD Property** field that is adjacent to (same row) the SG Column you want to map.
3. Click a second time in the same **AD Property** field to display the list of available AD fields > then select the AD Property you want to map.

RESULT: The AD Property field will be chosen as the mapped field. Click away to exit the field as needed.

ABOUT MAPPING THE SYNCH COLUMN: It is possible to choose DATA\_1 as the synch column. However, in the case of the picture shown below, the postal code is already mapped, and it will not provide a unique value for every user. Therefore, you would either (a) choose a different field in the *Sync Column droplist*; or (b) you would change which AD Property that is mapped to the Data\_1 column ... an AD Property that will always have unique data.

S.G. Table	S.G. Column	A.D. Property
CARDHOLDERS	ADDRESS1	streetaddress
CARDHOLDERS	ADDRESS2	postofficebox
CARDHOLDERS	CITY	l
CARDHOLDERS	EmailAddress	mail
CARDHOLDERS	FIRST_NAME	givenname
CARDHOLDERS	HOME_PHONE	homephone
CARDHOLDERS	LAST_NAME	sn
CARDHOLDERS	MobileNumber	mobile
CARDHOLDERS	PHONE	telephonenumber
CARDHOLDERS	POSTAL_CODE	postalcode
CARDHOLDERS	STATE	st
CARDHOLDERS	COMMON_ID	
CARDHOLDERS	DATA_1	
CARDHOLDERS	DATA_2	
CARDHOLDERS	DATA_3	
CARDHOLDERS	DATA_4	
CARDHOLDERS	DATA_5	
CARDHOLDERS	DATA_6	

GCS AD Change Monitor App (cropped) > Field Mapping between SG Columns & AD Properties

4. Click the [ **Save Settings for Customer** ] button.
5. Restart the AD Synch App and the GCS AD Synch service to initialize changes.

CONFIGURE CARDHOLDER SYNCRONIZATION SETTINGS

The Sync Column sets which field is used to identify the correct corresponding Cardholder record when changes are detected in AD User Data. This field allows the records to stay synchronized when changes or deletions occur on the AD domain.

**IMPORTANT:** The chosen Cardholder field must be mapped to the appropriate corresponding AD Property. The AD Property must contain a unique and non-blank value in the mapped AD field for every AD User in the Active Directory User Group. Blank or duplicate data will prevent the AD User from being imported (pushed). *See previous instructions on mapping.*

STEPS

- 1. Choose the appropriate **SG Cardholder Column** in the 'Sync Column' droplist.

EXAMPLE: Image shows the Sync Column set to Email.Address – including the list of options in a callout.

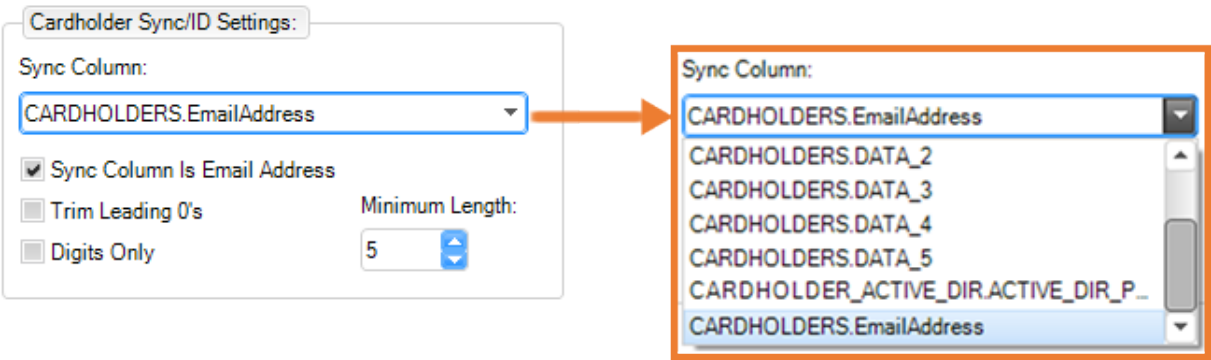


TABLE: Sync Column droplist – available columns with description of their behavior.

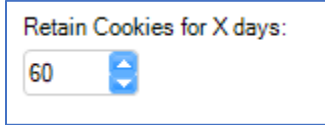
Available Columns	Behavior
CARDHOLDERS.COMMON_ID	This ID value must be unique for every individual cardholder/user
CARDHOLDERS.DATA_# (Data_1 thru 5)	The data field value must be unique for every individual cardholder
CARDHOLDERS ACTIVE_DIR.ACTIVE_DIR_PATH	Uses the active directory record for comparison in the sync.
CARDHOLDERS.EmailAddress	Email Address must be present in the AD User data. The Email Address from the AD User will be pushed to the Galaxy Cardholders.EmailAddress field for each user record and become the unique sync value.

- 2. Set the [Sync Column is Email Address] checkbox as appropriate ...
  - UNCHECKED: AD mail property will not be verified for valid email formatting. Uncheck this option if you are not choosing Email as the sync column.
  - CHECKED: the App will check the formatting of the AD mail address-- such as verifying the email does not contain spaces or invalid characters, and contains an @ symbol and .com or similar valid suffix. This option does not verify if the email address is active. It only checks for formatting mistakes.
- 3. Set the remainder of the checkbox options as appropriate ...
  - a) Set "Trim Leading Zeros" checkbox: Set to *checked* only when synchroning on a numeric value that contains leading zeros. The App will trim leading zeros from the incoming AD Data before pushing it into the SG field.
  - b) Set "Digits Only" checkbox: Set to *checked*, only when synchroning on a numeric value that is a numeric or integer value. The App will verify the data is not alpha-numeric or other non-numeric characters. Uncheck this option if you are syncing to email or other non-numeric data.
- 4. Enter the Min Length: (0 means it can be an empty field) – This sets the minimum character length required for the data in the synch column. The character length of data in the AD Property must meet or exceed the minimum character length to be valid for synchronization and import (push).

## CONFIGURE COOKIE RETENTION SETTING

The fetches are dependent of the presence of AD Cookies (Delete cookies or Change cookies). Cookies will automatically be created every time a change is picked up from the Active Directory domain. When the **Poll Interval Value** elapses, the App will look for new cookies – see the GCS Service settings for more information.

1. Enter the **number of days** you want to retain cookies. (default value = 60 Days / 0 = 23hrs;)



## CONFIGURE DEFAULT CARD OPTIONS

The *Default Card Settings* control whether a new card record is added and card data is included when the Sync occurs. This data does not come from AD Domain Properties. This data must be preconfigured in SG as instructed in prior sections.

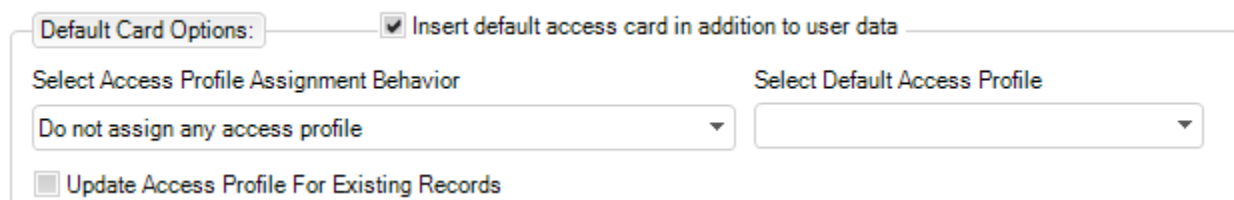
1. Set the checkbox **[Insert Default Access Card in addition to User Data]** as desired:
  - If *checked*, a new card record is inserted with these card access settings whenever AD User Data is synced.
  - If *unchecked* the App will not create a new card record and card data will not be pushed.
2. Select the **[Access Profile Assignment Behavior]**: this determines how the AD Sync will set the access profile.

	Behavior Setting	Result
1	Do not assign any access profile	No access profile will not be assigned during import process.
2	Always assign Default Access Profile	The <i>access profile</i> that is chosen in the <b>Default Access Profile droplist</b> will always be pushed with every AD User that is synced/imported.
3	Use AD Primary Group as Access Profile	This option will push the value that is in the AD Property for the primary group as the Access Profile for each user. You should preconfigure the matching Access Profile Name in SG. See earlier section in this guide for instructions.

3. Select **Default Access Profile**: this field is only available if you chose option-2 "Always assign Default Access Profile".

NOTE: the *Access Profile Name* must already exist in System Galaxy and must already be assigned to the same customer that the SG Operator is assigned to.

4. Set the checkbox **[Update Access Profile for Existing Records]** as needed:
  - When *checked* the App will also update the *Access Profile* for the preexisting cardholder records in System Galaxy. (This will overwrite the access profile field for existing cardholders if checked.).
  - When *uncheck* the App will not update the access profile for existing cardholder records.



GCS AD Change Monitor App > Default Card Options (cropped)

Continue programming the Default Card Options on the next page ...

5. Select the **Default Card Type** (card technology): this field identifies the *card type* or card technology to use for all new SG Cardholders.
6. Set the **Facility / Company Code**: (optional) as appropriate for the selected card type, which was set in the prior step. NOTICE: if you leave this blank or at zero, you will need to manually configure the FAC/CC in the System Galaxy Cardholder screen for each individual cardholder after the push/import is done. Remember that changes in Customer Settings will not create an update cookie. You can delete all cards and reimport after resaving your corrected settings and restarting the AD Change Directory Service.
7. Set the **AD Field** that will hold the ID Code (optional).
  - Leave this field unset/blank if you are going to auto-generate the card codes or manually enroll them later in System Galaxy.
  - If chosen, the AD Field must contain valid card numbers based on the selected card type. And card numbers in the AD Field must be unique for each individual AD User. Duplicate card codes are not allowed in System Galaxy.
8. Set the checkbox "**Auto-Generate ID Code**":
  - When *checked* the App will automatically generate the ID Code (card code).
  - When *unchecked*, the APP will not generate an ID Code and you can enroll/add the card code later in the System Galaxy Cardholder screen after the AD Sync/Import is performed.
9. Choose the **Default Badge Design**: (optional) The Badge Design must exist in System Galaxy and must be assigned to the same customer as the SG Operator who is running the APP. The badge name will auto-fill. If there is more than one badge for the same customer, the Operator should be able to select it from this droplist.
10. Set the checkbox "**Do not allow AD to re-enable a Cardholder**":
  - When *checked* the AD App will not re-enable the *Cardholder Active* checkbox in System Galaxy Cardholder screen. This applies to cases where the cardholder previously deactivated based on the prior AD change/deletion.
  - When *unchecked*, the AD App will re-enable the Cardholder via the Cardholder Activate checkbox in the SG Cardholder screen.

Default Card Options: ☒ Insert default access card in addition to user data

Select Access Profile Assignment Behavior: Do not assign any access profile Select Default Access Profile:

☐ Update Access Profile For Existing Records

Select Default Card Type: 26 Bit Wiegand Facility/Comp. Code: 0 ID Code AD Field:

Select Default Badge Design:  ☒ Auto-generate ID Code

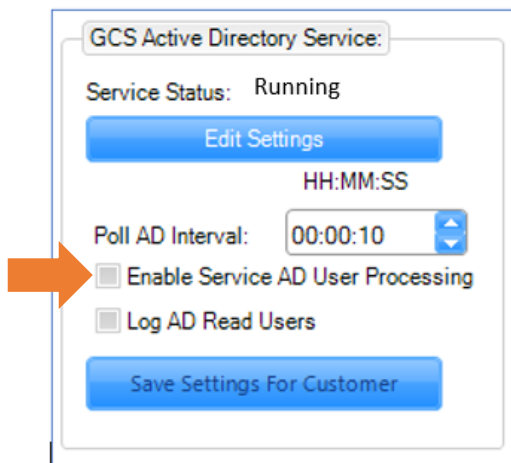
☒ Do not allow AD to re-enable cardholders

GCS AD Change Monitor App > Default Card Options (cropped)

## CONFIGURE GCS ACTIVE DIRECTORY SERVICE

These settings control the behavior of the GCS Active Directory Service. Active Directory creates the checkpoints (cookies) whenever a change or deletion is detected from the AD Domain. These checkpoints are transmitted to the GCS AD App.

1. **Service Status:** this field is a courtesy status indicator that shows the current status of the GCS AD Service
  - **Running:** the service is actively running
  - **Unknown:** the service may not be running
  - **Stop:** the service is not running
2. Click the **Edit Settings** button to see or edit the log file path.
3. Set the **Poll AD Interval (HH:MM:SS)**: this value determines the time interval that the GCS AD Service will poll Active Directory Domain Server to create new checkpoints (i.e., change and delete cookies).
  - Default setting is 10 seconds ( 00:00:10). You can set this value to poll every few minutes or hours.
  - Checkpoints (cookies) will be retained for the number of days configured in the Sync settings.
4. Set the checkbox **“Enable Service AD User Processing”** as desired: When *checked*, the App will process the AD Changes provided the GCS AD Service is already running. When unchecked, the App will not process AD Changes even if the service is running.



**Notice: check the AD User Processing option to import users & changes.**

GCS AD Change Monitor App > GCS AD Service options  
(cropped)

5. Set the **Log AD Read Users**: when *checked* the App will create a log of the users read.

## SAVING CUSTOMER SETTINGS

The Customer Settings will take effect when the SG Operator saves the customer settings and refreshes the AD service.

**IMPORTANT:** If the SG Operator has made any changes to any of the configurable settings, they must Save Settings for Customer and restart/refresh the GCS AD Service for the recent changes to take effect in the AD Sync/import process.

1. Click the [Save Settings for Customer] button: this will save all the configuration in the shaded areas.

The screenshot shows the GCS Active Directory Change Monitor application. The 'SG Operator/Customer Information' section has 'SG Operator' set to 'ron Jones' and 'SG Customer' set to 'Roanoke CPS'. The 'Active Directory Domain Credentials' section has fields for 'Domain/IP Address', 'User Name', and 'Password'. The 'Cardholder Sync/ID Settings' section has 'Sync Column' set to 'CARDHOLDERS.EmailAddress' and 'Sync Column Is Email Address' checked. The 'Default Card Options' section has 'Insert default access card in addition to user data' checked. The 'GCS Active Directory Service' section has 'Service Status' set to 'Running' and 'Poll AD Interval' set to '06:00:00'. The 'Active Directory User Data' section shows a table of 12 records. A red box highlights the 'Save Settings for Customer' button in the 'GCS Active Directory Service' section. An orange arrow points from the 'Save Settings for Customer' button to the 'Push AD Users To System Galaxy DB' button.

S.G. Table	S.G. Column	A.D. Property
CARDHOLDERS	ADDRESS1	streetaddress
CARDHOLDERS	ADDRESS2	postofficebox
CARDHOLDERS	CITY	i
CARDHOLDERS	DATA_1	postalcode
CARDHOLDERS	EmailAddress	mail
CARDHOLDERS	FIRST_NAME	givenname
CARDHOLDERS	HOME_PHONE	homephone
CARDHOLDERS	LAST_NAME	sn
CARDHOLDERS	MobileNumber	mobile
CARDHOLDERS	PHONE	telephonenumber
CARDHOLDERS	STATE	st
CARDHOLDERS	COMMON_ID	
CARDHOLDERS	POSTAL_CODE	
CARDHOLDERS	DATA_2	

### GCS AD Change Monitor App > Saving Customer Settings

2. Close the GCS AD Change Monitor App.
3. Stop and restart the GCS AD Service from the Services window.
4. Then you can sign-into the GCS AD Change Monitor App again and fetch and push your AD Users as needed.

## MANAGING CHECKPOINTS

Contact your Technical Support to get assistance in managing checkpoints.

# Manually Importing AD Users into System Galaxy Database

## FETCHING USERS

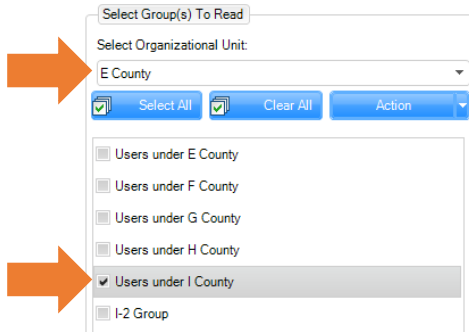
After the operator selects the desired Org Unit, the associated User Groups will populate the User Group list. The SG Operator can filter which User Groups to be fetched (retrieved).

### STEPS

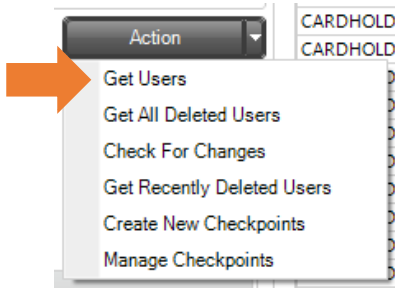
1. Choose the **Organizational Unit** (OU) from the [Select OU] droplist.

RESULT: The associated AD User Groups will populate/fill the list, based on the selected OU.

2. To choose a **User Group**, place a "checkmark" in the checkboxes beside the Group Name that you want. *You can choose multiple User groups as needed.*
  - When "checked", the AD App will perform the chosen Action for the selected User Groups.
  - The AD App will not fetch users from unchecked groups.
  - The **Select All** and **Clear All** buttons will add or remove checkmarks for all the User Groups in the list.



3. From the [Action] droplist, choose the action to run on the selected User Groups, (Get Users).



RESULT: The App will immediately fetch the qualifying users that match the chosen action.

Actions	Behavior
Get Users	Fetches users from the chosen User Group(s)
Get All Deleted Users	Fetches all the Delete Users from the entire domain (domain-wide fetch), based on the AD Domain Controller's record of deleted users.
Check for Changes	Uses the <i>Change Cookie</i> to determine which users to fetch from the chosen User Group(s).
Recently Deleted Users	Uses the <i>Delete Cookie</i> to fetch all deleted users domain-wide based on the last delete cookie.
Create New Checkpoints	Manually creates a <i>Change Checkpoint</i> to <i>Delete Checkpoint</i> irrespective of changes or deletions.
Manage Checkpoints	Contact Technical Support for assistance managing checkpoints.

4. The **User Data tab** shows the AD Users that were fetched and will be sent to System Galaxy database.

Active Directory User Data		Messages						
DisplayName	LastName	FirstName	EmailAddress	AccountDi...	GroupNames	Company	Departme...	
Ines A'llward	A'llward	Ines	Ines.A'llward@acme.com	No	Domain Users	ACME Corp.	IT	
Ira Dennett	Dennett	Ira	Ira.Dennett@acme.com	No	Domain Users	ACME Corp.	Engineering	
Isidor Gebuhr	Gebuhr	Isidor	Isidor.Gebuhr@acme.com	No	Domain Users	ACME Corp.	Engineering	
Iseabal McCaffery	McCaffery	Iseabal	Iseabal.McCaffery@acme...	No	Domain Users	ACME Corp.	Finance & Accou...	
Isidor Gainfort	Gainfort	Isidor	Isidor.Gainfort@acme.com	No	Domain Users	ACME Corp.	Purchasing	
Cody Mobley	Mobley	Cody		No	Domain Users			
▶ Ramon A. Mobley	Mobley	Ramon	rmobley@acme.com	No	Domain Users			
Kevin O'Shank	O'Shank	Kevin		No	Domain Users			

5. When you have retrieved your AD User Groups and are satisfied with the Customer settings, click the button to **[Push AD Users to System Galaxy DB]**.

RESULTS: A progress bar will appear. The fetched AD User data will be imported (inserted or updated) into the SG database, along with any applicable *Default Card Settings* that are saved at the time of the push.



6. NOTICE: The **Messages tab** shows any pertinent messages the operator may encounter with the Data or other functions including database messages when pushing user data to the SG database.