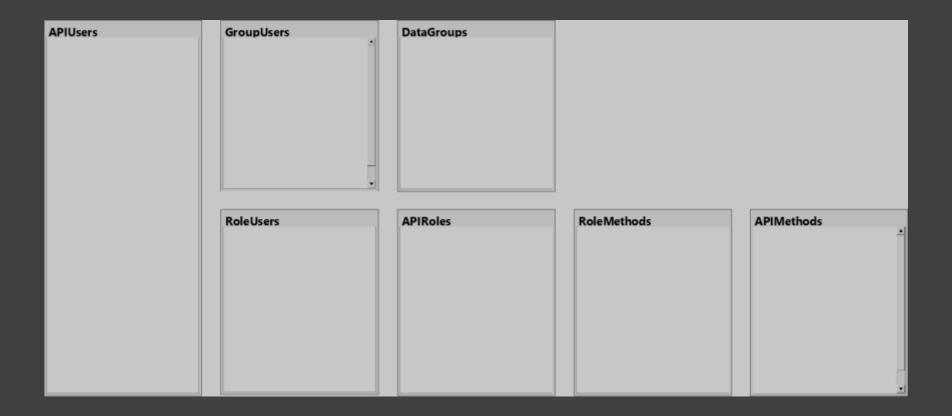
Security Forms Overview

One of the key parts of DGP Lattice security is the data-driven Role Based Access Control (RBAC) subsystem that controls not only user authentication (via HMAC hash) but also which accounts can call which API methods (APIMethod authorization) and which accounts can see which data in Lattice (DataGroup authorization). The heart of that subsystem is the SQL Server SysInfo database that stores all of the security tables and records. The security forms in the Lattice UI are used by system admins to manage and maintain all of the various security records.



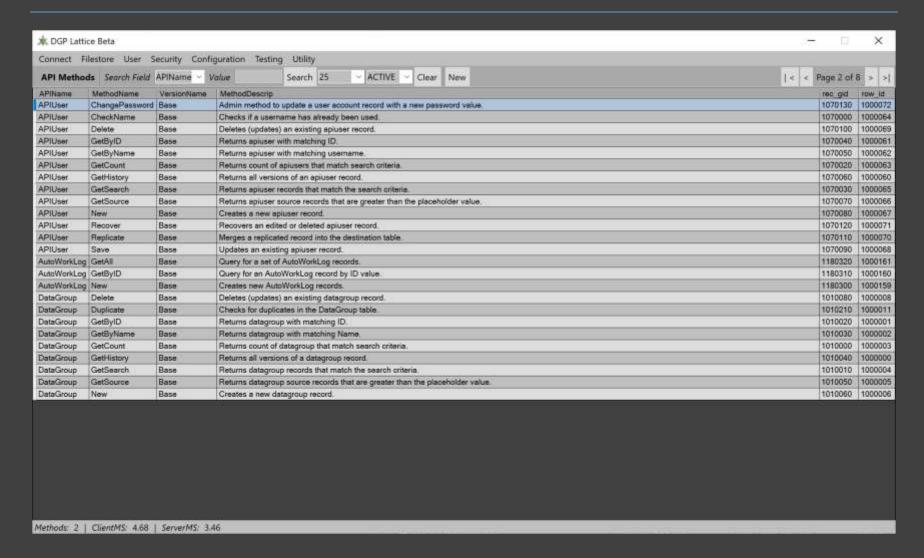
Each of the 4 forms that correspond to the 4 main entity tables in the SysInfo schema all have the same layout and functionality.

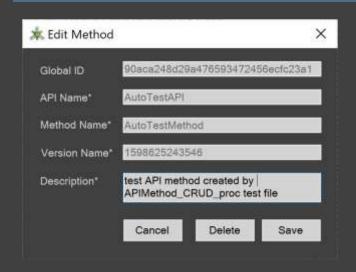
A toolstrip across the top of the form contains a dropdown to select a search field, a textbox for the search value, Search and Clear buttons, dropdowns for the number of page rows and the record state to search for, a button to add a new record, and the buttons to navigate pagination.

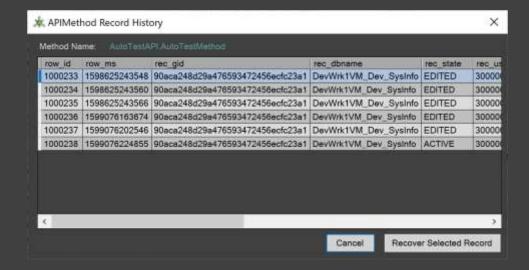
API Methods Form

Each APIMethod in the system must be documented in the APIMethods table or it cannot be linked to a role, in which case it cannot be authorized for any user to call it. User authentication and API method authorization functionality is built into each DGP web service, and there are no ways to bypass that logic, even for admin users.

APIMethods Context Menu	Description
Edit	Only allows the description field of the APIMethod record to be edited. This restriction is due to the
	"immutable, append-only" convention that strictly enforces backward compatibility. Editing any
	other APIMethod values would cause breaking changes to applications and systems that depend on
	the existing state to function correctly.
Method Roles	This is a simple list of the roles that the selected APIMethod has been assigned to.
View History	This form shows a grid of all versions of the selected record. If the record state is set to ACTIVE, the
	Recover Selected Record button is enabled to recover an edited version of the record as the current
	ACTIVE version. The process to recover a deleted record is different, so the Recover Selected Record
	button is disabled when the record state is set to DELETED.
Recover Deleted	This option is disabled unless the record state has been set to DELETED. Doing so allows the form to
	be used to search for deleted records. Selecting this option for a deleted record will recover the
	deleted record as the new current ACTIVE record.





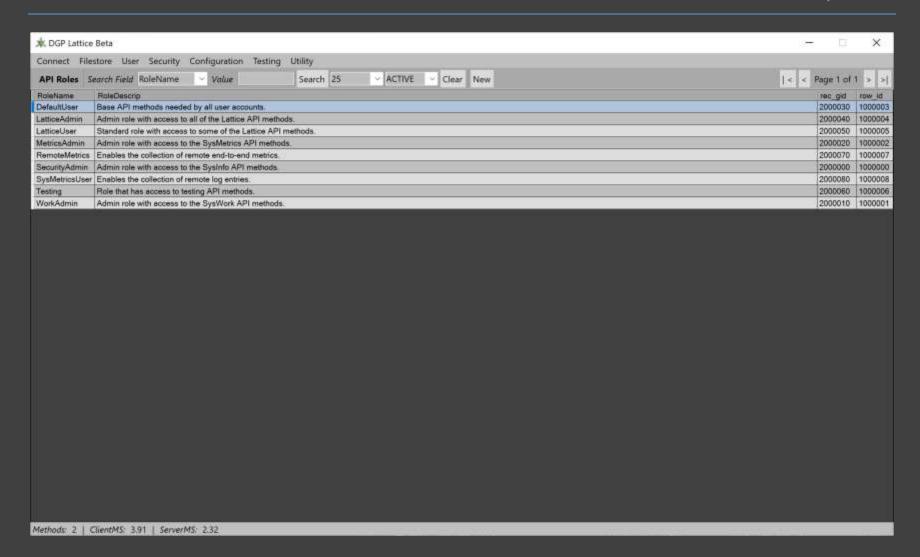


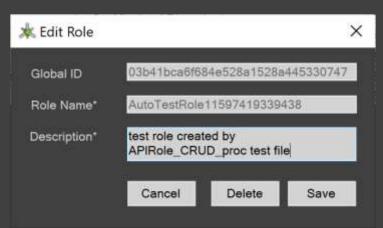
API Roles Form

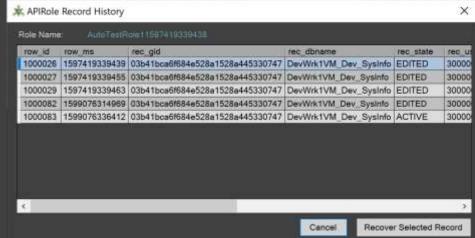
APIRoles are used to create collections of APIMethods that are easier to assign to users than would be the case if each method had to be assigned to each user individually. That is the main point of "Role Based Access Control" (RBAC). There is no limit to the number of roles in a system, and no limit to the number of roles that can be assigned to a user. The user account will end up with a superset of all the methods authorized by each role, without any duplicates.

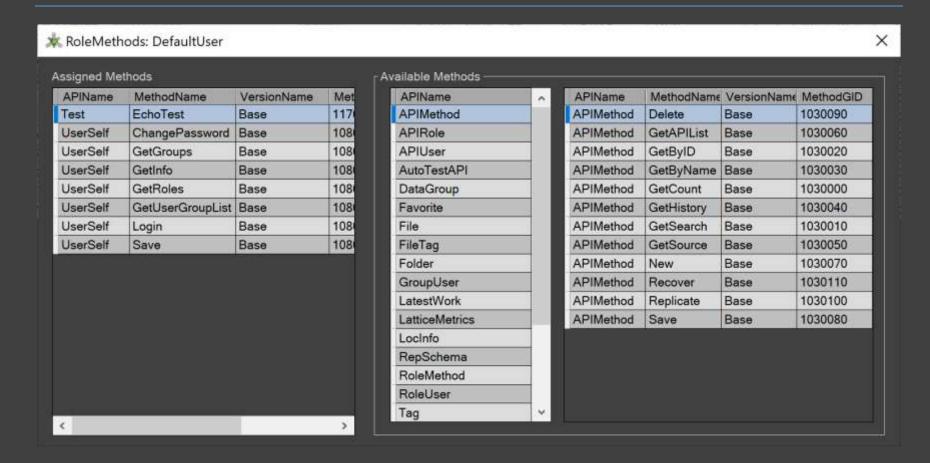
APIRoles Context Menu	Description
Edit	Only allows the description field of the APIRole record to be edited. This restriction is due to the
	"immutable, append-only" convention that strictly enforces backward compatibility. Editing any
	other APIRole values would cause breaking changes to applications and systems that depend on the
	existing state to function correctly.

Role Methods	This form creates "intersection" records assigning (linking) APIMethod records to one or more APIRoles.
	The form shows the methods currently assigned to the role in the left-hand grid. Double-clicking on an assigned method removes (soft deletes) the intersection record.
	Due to the large number of APIMethod records, the Available Methods section on the right shows a parent/child set of grids. Selecting one of the API's shows all of the API methods that have not yet been assigned to the role (in some cases the list of available methods will be empty if all methods have already been assigned). Double-clicking on an available method will assign it to the role.
View History	This form shows a grid of all versions of the selected record. If the record state is set to ACTIVE, the Recover Selected Record button is enabled to recover an edited version of the record as the current ACTIVE version. The process to recover a deleted record is different, so the Recover Selected Record button is disabled when the record state is set to DELETED
Recover Deleted	This option is disabled unless the record state has been set to DELETED. Doing so allows the form to be used to search for deleted records. Selecting this option for a deleted record will recover the deleted record as the new current ACTIVE record.









API Users Form

User account records are stored in the APIUsers table, and in addition to all the standard fields containing details of the user, it also contains cached authorization data for APIMethods and DataGroups, as well as an API method rate limit value per account.

APIUsers Context Menu	Description
Edit	The form allows most user values to be edited with the exception of the UserName and Password fields. The password value is not shown in the UI (and in any event is stored in encrypted form in the database record using zero-knowledge encryption).
User Methods	This form shows a simple grid of the superset of all methods that a user is authorized to call from the combined total of all their role memberships. A list of all the method names in this grid is cached in the APIUser record for API authorization, and updated every time the user calls the Login method.
User Roles	This form creates "intersection" records assigning (linking) APIUser records to one or more APIRoles. The form shows the roles currently assigned to the user in the left-hand grid. Double-clicking on an assigned role removes (via replica record update) the intersection record.
	The Available Roles section on the right shows all of the API roles that have not yet been assigned to the user. Double-clicking on an available role will assign it to the user.
Group Access	This form creates "intersection" records assigning (linking) APIUser records to one or more DataGroups.
	The form shows the groups currently assigned to the user in the left-hand grid. Double-clicking on an assigned group removes (soft deletes) the intersection record.
	The Available Groups section on the right shows all of the DataGroups that have not yet been assigned to the user. The appropriate access level (ReadOnly or ReadWrite) must be selected before Double-clicking on an available group to assign it to the user.

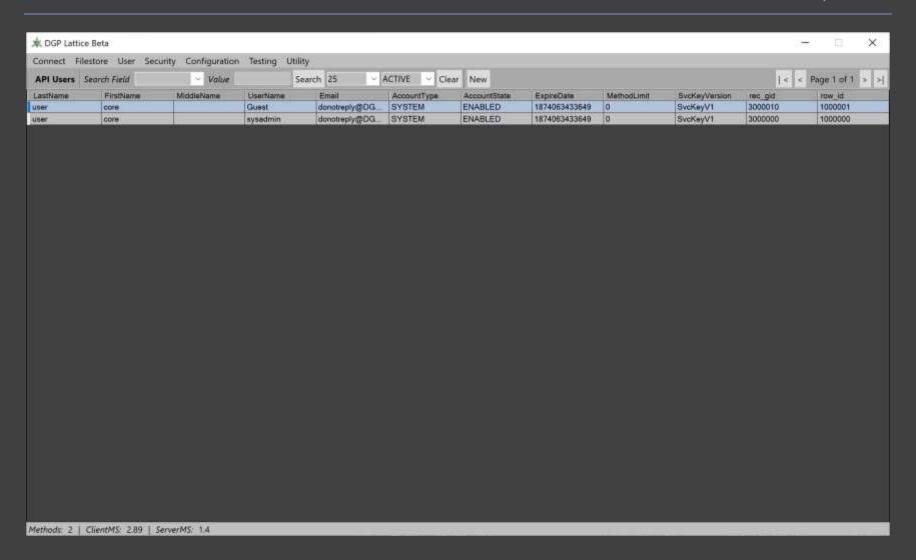
	The Country of the Co
Change Password	This form calls an API method that runs a process to change a user's password, store it in encrypted
	form in the database record, and set a new expiration date based on the configured expiration days.
View History	This form shows a grid of all versions of the selected record. If the record state is set to ACTIVE, the
	Recover Selected Record button is enabled to recover an edited version of the record as the current
	ACTIVE version. The process to recover a deleted record is different, so the Recover Selected Record
	button is disabled when the record state is set to DELETED.
Recover Deleted	This option is disabled unless the record state has been set to DELETED. Doing so allows the form to
	be used to search for deleted records. Selecting this option for a deleted record will recover the
	deleted record as the new current ACTIVE record.

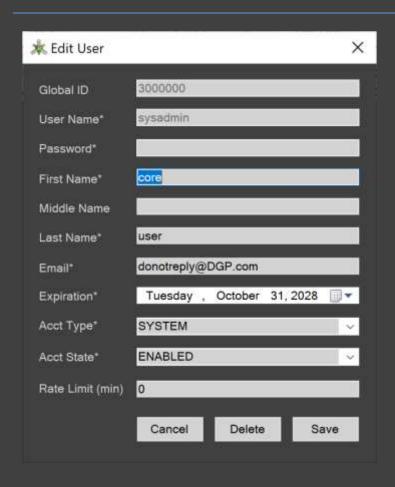
Note: SYSTEM accounts never expire and have no rate limit, since they bypass the expiration check and the rate limit check in the web service (which means any expiration or rate limit values set for system accounts have no effect). Expiration date and rate limit values only affect standard user accounts.

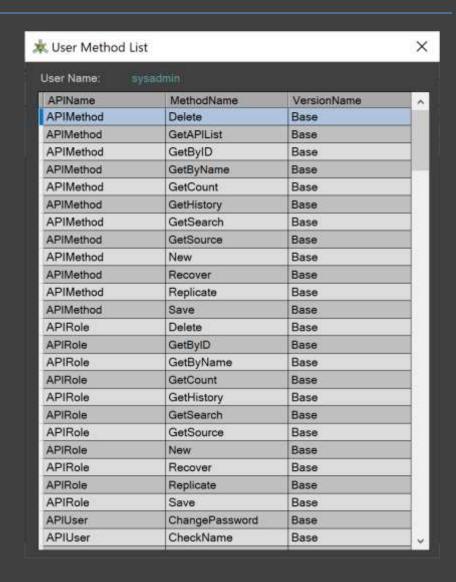
To improve the performance of account authentication and authorization used when processing each API request message, authorization data is cached in each user account record. This means that the authentication query only searches for and retrieves a single record from a single well-indexed table.

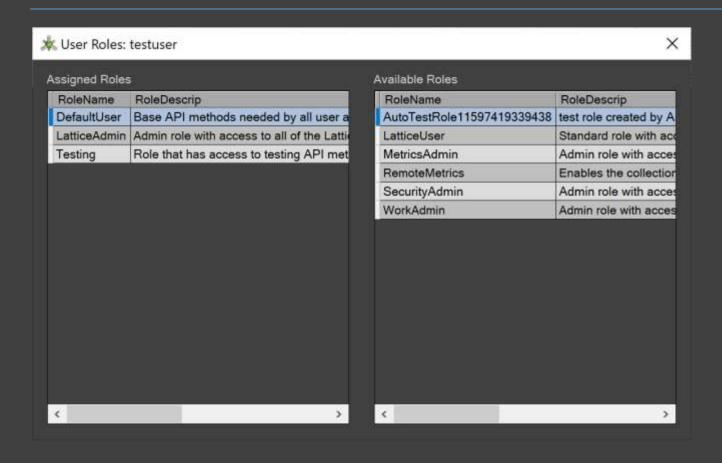
The cached data is updated via a lazy just-in-time process that runs as part of the Login API method for standard accounts. This is to help spread out the workload when very large numbers of user accounts are affected by a change to the data, such as adding a new method linked to a role that already has many users.

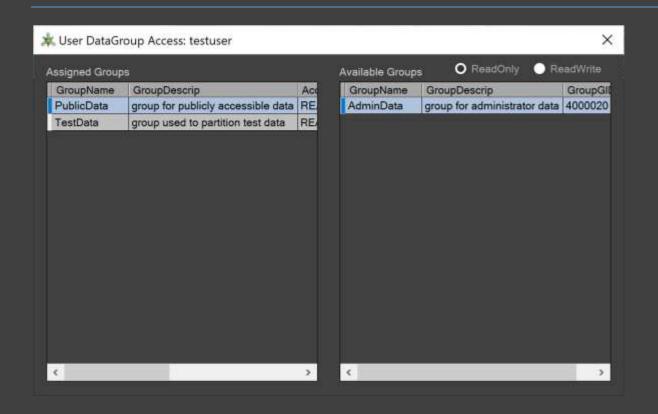
The authorization data cached in system accounts is updated whenever the parent tables such as APIRoles, DataGroups, etc. are changed, under the assumption that there will only be a small number of system accounts, and the workload of updating all of them at once will not bog down the system.











DataGroups Form

DataGroups are used as a value embedded in the records of shared tables to horizontally partition the data by the DataGroup global ID value. The SQL syntax of the data access methods automatically include DataGroup membership and access levels of the user account when running all queries on those shared tables. Currently, only the Lattice Folders and Files tables use DataGroups for this type of data partitioning.

The net result is of those queries is that users are only able to see the folders that they are authorized to see, and the same is true for all of the files stored in the system as well. Users are not be able to tell that all other folders and files that they have not been authorized to access even exist.

APIMethods Context Menu	Description
Edit	Only allows the description field of the DataGroup record to be edited. This restriction is due to the "immutable, append-only" convention that strictly enforces backward compatibility. Editing any
	other DataGroup values would cause breaking changes to applications and systems that depend on
	the existing state to function correctly.
View History	This form shows a grid of all versions of the selected record. If the record state is set to ACTIVE, the
	Recover Selected Record button is enabled to recover an edited version of the record as the current
	ACTIVE version. The process to recover a deleted record is different, so the Recover Selected Record
	button is disabled when the record state is set to DELETED.
Recover Deleted	This option is disabled unless the record state has been set to DELETED. Doing so allows the form to
	be used to search for deleted records. Selecting this option for a deleted record will recover the
	deleted record as the new current ACTIVE record.

