F.01 Security & User Access

200612 First Gas GTAC Transaction Management System

Version 2.0A

Table of Contents

1. F.01.01.01 System Configuration, Security & User Access

The initial configuration of roles and object partitioning will be developed by Tieto during the PCI phase and tested with First Gas prior to initial deployment. First Gas is responsible for providing a list of users for each role that is configured to Tieto. Note that First Gas may assign multiple roles to any user. For example, a given member of First Gas Commercial team, might be assigned the roles of Commercial Operator and System Operator in order to have all privileges of both roles.

It is worth noting that First Gas will be able to maintain this user / role configuration post Go-Live. The project will setup roles and assign them to users prior to SAT. During SAT, First Gas will be able to request changes to role access as part of their testing.

The initial list of roles identified during the PFA workshops are as follows:

Role	Commercial Operator	System Operator	Billing (Commercial)	Billing (Finance)	Allocation Agent
Description	First Gas internal role - Commercial	First Gas internal role - Operations	First Gas internal role – Commercial	First Gas internal role – Finance	First Gas or External Party
Object Partitioning / Access Restrictions	N/A	N/A	N/A	N/A	Location
Access by Process Area					
Users, Parties & Contracts	Full access	Read only	Read only	Read only	-
Interconnection Points, Pipelines & Zones	Read only (Zones are full access)	Full access	Read only	Read only	-
Forecasting					-
Nominations & Scheduling	Read only	Full access	Read only	Read only	Read only (for their locations)
Trades & Auctions	Full access (no access to daily trades from ems)	Read only	Read only	Read only	-
Metering, Gas Quality & Linepack	Read only	Full access	Read only	Read only	Read only (for their locations)
Operating Imbalances & Mismatches	Read only: (Aggregate pipeline position only for estimated Running Mismatch within day)	Full access	Read only	Read only	-
Capacity, Allocation & Curtailment	Read only	Full access	Read only	Read only	Can edit Allocated Quantities per location per shipper per day (for their locations)
Invoices & Fees	Read Only	-	Full access for billing process	Full access to revenue configuration	-

(continued)

Role	Metering Agent	Shipper	Interconnect Party	Critical Contingency Operator	emsTradepoint
Description	First Gas or External Party	External	External	External	External
Object Partitioning / Access Restrictions	Location	Contract Area	Location	N/A	N/A
Access by Process Area					
Users, Parties & Contracts	-	-	-	-	-
Interconnection Points, Pipelines & Zones	-	-	-	-	-
Forecasting	-	-	-	-	-
Nominations & Scheduling	See schedule for their locations only.	Submit nominations and see schedule for their contracts only	Confirm shipper nominations and see schedule for their locations only.	Read only	
Trades & Auctions	-	Bid in Auctions Trade gas Trade PR	See auctions at their locations only	Read only	Manage records for trades of gas (in EMS)
Metering, Gas Quality & Linepack	Read Only (meter data)	Read only Gas Type	Read only Gas Type	Read only Can issue notices	-
Operating Imbalances & Mismatches	-	Read only (own mismatch during the day, all mismatches after the day)	Read only (own mismatch during the day, all mismatches after the day)	Read only	-
Capacity, Allocation & Curtailment	-	-	-	Read only	-
Invoices & Fees	-	Read only (own invoices)	Read only (own invoices)	-	-

In addition to these roles, the System Admin role will have full access to the system. This role should only be granted to First Gas users with the highest degree of experience with the system.

EC comes with a complete administration functionality where access control profiles, emails, default values, etc., can be handled.

Likewise, all system attributes and settings can also be managed through dedicated screens in EC.

It is possible to set up access control profiles such that administrators can only access administration screens and not see actual data

EC supports several user authentication methods:

- EC internal, meaning users are authenticated through the EC internal user/password directory
- LDAP-based, meaning users are authenticated through a centralised LDAP-based repository, typically MS Active Directory

- Web Access Manager (WAM) based, meaning dedicated access management software (e.g. SiteMinder) is handling the user authentication.

Regardless of authentication method, when a user is authenticated to access EC, the access control will be based on the EC role concept. In EC access privileges are assigned to a user profile ("user role" in EC). Individual users can be member of one or more roles (it will always be the highest assigned privilege that will be applied when roles are overlapping).

When a user is authenticated to access EC, the access control will be based on the EC role concept. This means that the users get access to roles and not direct access to EC functions or data.

This greatly enhances system administration capabilities.

Energy Components provides complete auditing capabilities where any changes to such data are captured along with user credentials, time of change, etc. Moreover, EC will also keep copy of previous values so that it is also possible to see the exact nature of any such changes.

EC can also be configured to require the user to supply an explanatory text when making such changes. This is standard functionality in EC and applies for any part of the system. EC is fully SOX404 compliant and fulfils all necessary security policies when it comes to data integrity and audit ability.

The EC security model also allows access control to be employed in order to protect data from unauthorised changes.

All access control in EC is role-based. This facilitates greatly the system administration. The user interface will adapt according to the access privileges granted to a role, and the user will only see those selections accessible to him/her.

EC applies multiple access levels (e.g. read-only, read-modify, read-modify-insert, read-modify-insert-delete), etc. Depending on access, privileges and status data can be locked for editing by unauthorized staff. EC further implements a powerful "group-model" that allows customers to set up their own ownership hierarchy for data. EC will then provide access to data according to each user privileges according to such hierarchy.

Further, access control in EC is depending on the data status, i.e. it is therefore possible to assign different access privileges to e.g. raw, validated and published data.

In addition, EC has flexible and fully configurable verification/approval features, allowing customers to assign ownership and responsibility for data validation and approval according to own organizational hierarchy.

In addition to limit data access based on record status, EC supports full row level security, also mentioned as "ring-fencing". The row level security is configured at class level, including the option of inheriting security settings through a class hierarchy, reflecting settings from the "top level class" on all underlying classes. This concept is typically used if data from multiple legal entities are stored in the same EC database, where it is critical that users only can see own data. This is also referred to as "Object Partitioning", and is for instance applied on Royalty calculations for two different operations.

Further, EC includes the concept of "4-eyes approval", meaning it is possible to force data to be approved by two separate users before promoting to next approval level. This option is typically used for financial data, where segregation of duties is mandated.