# Understanding end users

The **end users** of nGenue can be anyone who is involved in the natural gas industry, including:

* **Natural gas marketers** - Individuals or companies invloved in buy and sell natural gas.
* **Natural gas producers**: Companies that extract natural gas from the ground.
* **Natural gas distributors**: Companies that transport natural gas to customers.
* **Local distribution companies (LDCs)**: These are companies that distribute natural gas to end-use customers.
* **Utilities**: Companies that provide essential services to customers, such as electricity, gas, and water.
* **Pipelines**: Companies that transport natural gas over long distances.

Basically, anyone who is involved in the buying, selling, transporting, or distributing of natural gas could be an end user of nGenue application.

## Key tasks performed by end users

The key tasks that end users perform within the nGenue application depend on their specific role and the module they are using. However, some common tasks may include:

* **Data entry** - Entering data into the system, such as customer information, pricing data, or transaction details.
* **Data analysis** - Analyzing data to identify trends, patterns, and insights.
* **Reporting** - Generating reports to track performance, identify areas for improvement, and make informed decisions.
* **Transaction processing** - Processing transactions, such as sales, purchases, and payments.
* **Customer management** - Managing customer relationships, including handling inquiries and complaints.
* **Inventory management** - Managing inventory levels and tracking stock movements.
* **Regulatory compliance** - Ensuring compliance with relevant regulations and industry standards.

The specific tasks that end users perform will vary depending on their job function and the specific requirements of their organization.

## How are access levels and security settings managed for end users?

Each of nGenue’s software modules is designed for the enforcement of standard security protocols, adhering to several layers of security.

* nGenue recommends a windows-based authentication model for user access to all data. This places access to data directly under the authority of client network administrators. nGenue recommends a network role be set up for all nGenue application users. Within that role, access can be granted as needed at various levels (Read only, Admin, Reporting, etc.).
* Within nGenue, those with the administrator role can create any number of operational user groups that will be using nGenue. Every user interface screen within nGenue is then granted or denied access based on the role to which a user belongs.
* Within specific user interface screen layouts, certain actions are further restricted based on the permissions granted.
* At the most granular level, the nGenue database allows the use of row level security (RLS) whereby certain users are restricted at the row level based on whether they are part of a given group.

For example, if Jane Smith works in New Jersey and is not allowed to see information related to Pennsylvania, she can be restricted at the row level (as part of the database architecture) to see only information that is related to New Jersey. Though she has access to an *end user volume* screen, the database would only return data related to New Jersey.