Company Hierarchy

A company hierarchy can be of 2 types:

Flat, i.e. one company in the hierarchy
Multi-level, i.e. Headquarter with have their own subsidiaries.

For multi-level hierarchy it is essential to understand Employee subsidiary companies that may
User Types

Employee User Types

User Type	Description	Available to
Company Administrator	Can see all activity they have the **rights** to view for any company within their hierarchy no matter where in the hierarchy they are placed.	Assureds, Licensees
Administrator* (Admin)	Can see/manage all activity they have **rights** to for their own company and any subsidiary of that company.	Assureds, Licensees
Power User	Can see/manage all activity they have the **rights** to within their own company and no other company in the hierarchy. *Partner company employees can only be Power Users.*	Any Company Type
Private User	Can see/manage only their own activity within the system.	Assureds Only

*An Admin set up at the Headquarter level has the same scope as a CA

Security Role Types

Created Security Roles are available to Employees or Companies based on the Security Role Type, which are explained below:

Roles	Description
Employee – Assured Role	Accessible to all Employees of an Assured Company
Employee – Partner Company	Accessible to all Employees of a Proprietary Company
Employee – Licensee Role	Accessible to all Employees of a Licensee Company
Employee – Licensee Policy Group Role	Accessible to all Employees of Licensee Companies associated to Policy Groups
Employee – Partner Company Policy Group	Accessible to all Employees of Proprietary Companies associated to Policy Groups
Company – Assured Company Role	Accessible to all Assured Companies and are assigned **when setting up a policy**
Company – Insurer/Broker Role	Accessible to all Proprietary Companies and are assigned **when setting up a policy**

insurity

Security Rights

A Security Role logic is governed by the Security Rights assigned to it. Security Role Types have a different sub-set of security rights:

Policy-centric – rights governing actions at a policy level or any other activities related to the policy (e.g. Confirm Policy, Edit Booked Shipment, Submit a Claim, etc.)
Admin rights – the ones governing actions to company reference data, e.g. managing company conveyances, managing employees, managing war scales, sanction scans configuration, etc.

It should be noted that certain policy configurations overturn users or companies' security rights, i.e. if a policy configuration does not allow shipment changes or cancellations, an Assured user/company with the security role rights to change or cancel shipments will not be able to use those rights.

Genoa Best Practices

1. All Security Roles should be created on a Headquarter level and shared down.
2. A Company Administrator managing Security Roles and Employees should have a Role, which will contain all available Security Rights.
3. Users cannot assign rights they do not have themselves.
4. When creating roles, it is recommended to have a series of roles (both Company and Employee) broken down into Security Rights Sections, e.g. Assured – Billing Rights, Assured – Shipment Rights with Premium, Assured – Shipment Rights No Premium, etc. This approach will make the Employee and Policy maintenance more efficient.
5. When assigning Roles to the company on a policy level, it should always be taken into consideration that a Company Role always supersedes an Employee Role, meaning that an employee role cannot use a right that their company role does not also have.

insurity