

Organizational Structure Overview

To manage the organizational structure of your implementation, click the Administration menu and select System Management.

System Management

Structure

- Corporate
- Contacts
- Documents
- Events
- Forms
- Messages
- News
- Plans
- Reports
- Resources
- Roles
- 8.0 Edge Division
- 8.0 IE Department
- 8.0 IE Location
- 8.0 Location
- 8.0 Release Department
- 8.0 Release Location
- Backups
- Business Group
- DD
- Enterprise Data
- Enterprise DR Exercise
- KW
- NYDOH
- SMS Testing
- WF Sample
- Ztesters

Browse Filter - Results

[Filter](#) [Reset](#)

Organization Details

Title:

Type:

Parent:

Status Changes:

[Save](#) [Cancel](#)

Security Details

Permissions:	Name	Read	Write	Admin	Delete
	Admin Account (admin)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
		<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	Administrators	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Access Management	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

[Add New](#)

Ownership Details

Owner:

[Choose Owner](#)

The architecture of the site is easily customized to match that of your organization. Each organizational unit defined in the hierarchy is a dedicated work area within the Global AlertLink application. You may assign permissions to the organizational unit, store data, plans, and incidents within the dedicated work area.

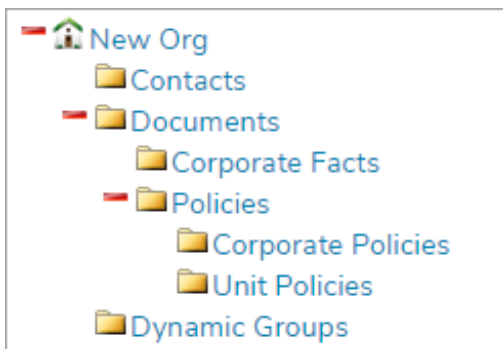
Tips

- Remember that when you create an organizational unit, you are creating a dedicated work area within Global AlertLink.
- You may assign permission to each organizational unit and functions and folders within each organizational unit.
- There are no limits on the number of organizational units or levels. We do recommend that you limit the number of levels for usability.
- Information may be shared, or cross linked, from one organizational unit to another.

In addition to the hierarchy of the organizational units, you may define a folder structure within each organizational unit and the respective data store component. The following items allow folders:

- Contacts
- Documents
- Dynamic Groups
- Events
- Forms
- Messages
- News
- Plans
- Reports
- Resources

The folder structure provides a framework for storing data or items within the application. There are no limits to the number of folders or levels of folders.



Tips

- You may define folder structures unique to each organizational unit.
- You may assign permission to folder structures.
- Each component within a work area allows for folders.
- There are no limits on the number of folders or levels.
- For contacts, folders may serve as groups for message distribution.
- A record may be shared in more than one folder.

You may create an unlimited number of security roles and use these roles to manage permissions within the application.

Tips

- Use security roles to define security for a specific role or use as a security group to define security for an entire set of users.
- Security may be inherited from parent organizations, so defining security at the parent can automatically flow down to all sub-units and folders.
- If you have multiple organizational units and users specific to those organizational units, you may consider creating security roles for each organization unit.

- Remember, any user assigned to the security role, automatically maintains that roles security permissions.

Note: The number of organizational units (hierarchy), the number of roles a user is assigned (permissions), how frequently this data changes, and how often a user accesses individual parts of the system can impact performance. GAL "calculates" a user's permissions to an object each time a user tries to access it, unless this permission has been previously calculated and is currently stored. Depending upon the variables mentioned above, the user's "security cache" is either current or needs to be rebuilt. Occasionally, if a user has not signed on for a while, and/or there has been a lot of changes to the hierarchy or their roles, the time to rebuild the cache may be excessive.

If you have any questions about this, contact us at support@resolver.com .