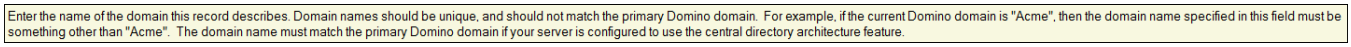
How panagenda SecurityInsider Works

SecurityInsider first scans the **primary addressbook** on the group scan server as specified on SecurityInsider configuration. If it **detects directory assistance** configured on that server, it will also scan all **trusted** secondary addressbooks configured therein.

Note that SecurityInsider does not support a Group scan server configured for a central directory architecture – in essence this means that the primary addressbook must NOT be specified in your directory assistance database – this is also documented in "da.nsf" itself, when hovering over the domain field label:



After scanning all applicable addressbooks on the group scan server and resolving groups and certifiers, it writes information about the groups into the SecurityInsider database (this is part one of why SecurityInsider needs "some" memory ;-))

It then scans all configured database servers, reusing the group information if possible. In general, if a server to be scanned for databases has the same replica id for its primary addressbook, it is assumed to be the same as on the group scan server, and all directory information is reused when resolving database ACLs. If the replica id of the primary addressbook of a database server does not match the group scan server's primary addressbook replica id, SecurityInsider will fully resolve that server's addressbook infrastructure (similar to the group scan server) and resolve ACLs accordingly.

A group entry is considered unknown, if:

- it does not have a corresponding group or person record according to the scanned server's addressbook infrastructure
- it does not match the parent's group group type - as a simple example, if a multipurpose GroupA has a subgroup GroupB of type mail only, then entries in GroupB are considered unknown for the purpose of security

Last but not least, if endpoint processing is enabled, SecurityInsider will ultimately compute a matrix of *who* has *which* access to *what*, AND through which group paths each endpoint is a member of a group – if multiple group paths lead to membership in a group, all paths are resolved and can be seen in the respective endpoint documents in the SecurityInsider database. In most cases, an endpoint is an individual user or server.