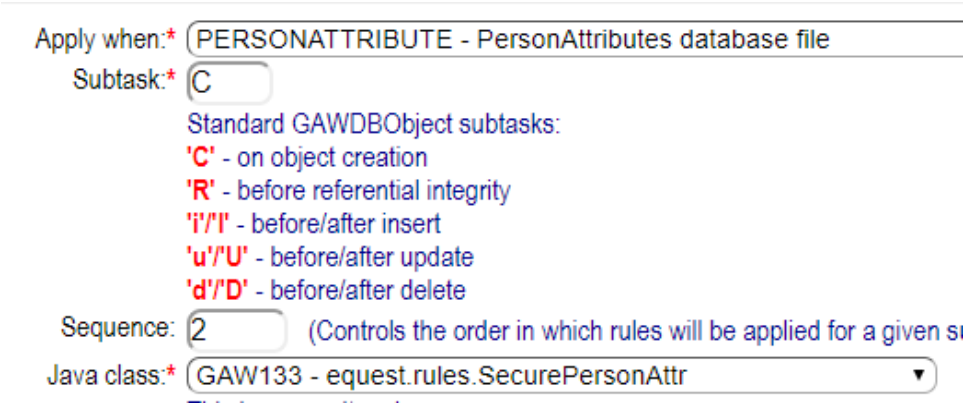
Rule GAW133 – SecurePersonAttr



This is a security rule.
This rule is designed to limit access to regular, special, and/or at risk person attributes.
By default, everyone authorized to view person attributes can view these.
With this rule, you can define which group(s) should NOT be authorized.
A NotAuthorizedException is thrown if an attempt is made to view one.
It is intended to be used On Creation of the PersonAttributes database file.

It uses the 'RULEPARMS' entry of the 'DEFAULTS'.
Valid properties are:

SecurePersonAttr.<groupid>.regular=n
SecurePersonAttr.<groupid>.special=n
SecurePersonAttr.<groupid>.atRisk=n

where <groupid> is the lowercase security group to be limited from seeing regular, special, and/or at Risk attributes.

Rule Setup:

Apply when	Sub-task	Seq	JAVA class
PersonAttribute	C	2	equest.rules.SecurePersonAttr

Rule Parms:

SecurePersonAttr.law.regular=n

Example:

This means that the security group “law” is not able to see regular person attributes.

See Table: Person Attribute Type (ATTRIBUTETYPE) for the meaning of regular, special or at risk person attributes.