Combination of security groups - rules for data restrictions

Contents

Combination of security groups - rules for data restrictions

When you combine independent or non-independent security groups, you use restrictions to specify the records that are visible to members of a security group.

When you combine security groups and use restrictions, the following rules apply:

- If a user is a member of multiple groups that are not independent and one security group has a restricted level of access, the user is granted the highest privileges across the security groups. For example, take two security groups that are not independent: the Managers security group and the Maintenance security group. The user has access to pay rate information in the Managers security group, but does not have access to the information in the Maintenance security group. When the two security groups are combined, the user has access to pay rate information in the Maintenance group.
- Data restrictions always combine across security groups by using the OR operator regardless of whether the groups are marked as independent. For example, take two security groups: one security group contains a READONLY data restriction condition ":orgid [equals character] 'EAGLENA'". The second security group contains a READONLY data restriction condition ":orgid [equals character] 'EAGLEUK'". Regardless of whether one, both, or neither security group is marked as independent, the restrictions combine to make the object or attribute read only if the ORGID is EAGLENA _OR_ EAGLEUK.

Therefore, you must consider the conditions that you apply to data restrictions carefully.