

### Current Section 7.1.3.6

#### **7.1.3.6 Owner and Group Defaulting Rules**

The OWNER and GROUP fields are defaulted in the following scenarios:

- An add operation is performed and no SD value is provided.
- An add operation is performed and an SD value is provided, but the SD flags do not include the OWNER bit.
- An add or modify operation is performed and an SD value is provided, and the SD flags include the OWNER bit, but the OWNER field in the supplied value is NULL.

In the preceding cases, the OWNER field is defaulted as follows:

- If the user performing the operation is a member of the DAG for the object (when it is defined), the SID of this group is written into the OWNER field of the SD.
- Otherwise, if the requester's security context contains the TokenOwner field, then the SID contained in this field is written into the OWNER field of the SD.
- Otherwise, the requester's user SID is written into the OWNER field of the SD.

The GROUP field is defaulted as follows:

- If the DAG was used as the default OWNER field value, then the same SID is written into the GROUP field.
- Otherwise, the GROUP field is defaulted to NULL.

### Modified Section 7.1.3.6

#### **7.1.3.6 Owner and Group Defaulting Rules**

The OWNER and GROUP fields are defaulted in the following scenarios:

- The SD flags do not include the OWNER bit.
- The SD flags include the OWNER bit, but the OWNER field in the supplied value is NULL.

In the preceding cases, the OWNER field is defaulted as follows:

- If the user performing the operation is a member of the DAG for the object (when it is defined), the SID of this group is written into the OWNER field of the SD.
- Otherwise, if the requester's security context contains the TokenOwner field, then the SID contained in this field is written into the OWNER field of the SD.
- Otherwise, the requester's user SID is written into the OWNER field of the SD.

If the DC functional level is DS\_BEHAVIOR\_WIN2008 or higher, and the DAG was used as the default OWNER field value, then the same SID is written into the GROUP field. In all other cases, the GROUP field is not modified before the SD value is passed to the CreateSecurityDescriptor algorithm as specified in section [7.1.3](#).

Current Section 7.1.3 (changes are only in the description of CreatorDescriptor)

2. *CreatorDescriptor*: The current SD value stamped on the object.

Modified Section 7.1.3

2. *CreatorDescriptor*: The current SD value stamped on the object. When an LDAP add operation is performed and no SD value is supplied, the SD value is first defaulted according to the rules specified in sections [7.1.3.5](#) and [7.1.3.6](#).