

7.1.3.2 SD Flags Control

When performing an LDAP operation (add, modify or search), the client may supply an SD flags control [LDAP_SERVER_SD_FLAGS_OID \(section 3.1.1.3.4.1.11\)](#) with the operation. The value of the control is an integer, which is used to identify which security descriptor (SD) parts the client intends to read or modify. When the control is not specified, then the default value of 15 (0x0000000F) is used.

The SD parts are identified using the following bit values: OWNER_SECURITY_INFORMATION, GROUP_SECURITY_INFORMATION, DACL_SECURITY_INFORMATION, SACL_SECURITY_INFORMATION, which correspond to OWNER, GROUP, DACL and SACL SD fields, respectively.

If the LDAP_SERVER_SD_FLAGS_OID control is present in an LDAP search request, the server returns an SD with the parts specified in the control when the SD attribute name is explicitly mentioned in the requested attribute list, or the requested attribute list is empty, or the requested attribute list contains an asterisk(*). Without the presence of this control, the server returns an SD only when the SD attribute name is explicitly mentioned in the requested attribute list.

For update operations, the bits identify which SD parts are affected by the operation. Note that the client may supply values for other (or all) SD fields. However, the server only updates the fields that are identified by the SD control. The remaining fields are ignored.