

**LDAP Cancel Operation**  
<[draft-zeilenga-ldap-cancel-11.txt](#)>

**1. Status of this Memo**

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as a Standard Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extensions mailing list <ldapext@ietf.org>. Please send editorial comments directly to the author <Kurt@OpenLDAP.org>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

The list of current Internet-Drafts can be accessed at <<http://www.ietf.org/ietf/1id-abstracts.txt>>. The list of Internet-Draft Shadow Directories can be accessed at <<http://www.ietf.org/shadow.html>>.

Copyright (C) The Internet Society (2004). All Rights Reserved.

Please see the Full Copyright section near the end of this document for more information.

**Abstract**

This specification describes a Lightweight Directory Access Protocol (LDAP) extended operation to cancel (or abandon) an outstanding operation. Unlike the LDAP Abandon operation but like the X.511 Directory Access Protocol (DAP) Abandon operation, this operation has a response which provides an indication of its outcome.

## Terminology

Protocol elements are described using ASN.1 [[X.680](#)] with implicit tags. The term "BER-encoded" means the element is to be encoded using the Basic Encoding Rules [[X.690](#)] under the restrictions detailed in [Section 5.1 of \[RFC2251\]](#).

DSA stands for Directory System Agent (or server).  
DSE stands for DSA-specific Entry.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14 \[RFC2119\]](#).

## [1. Background and Intent of Use](#)

The Lightweight Directory Access Protocol (LDAP) [[RFC3377](#)] provides an Abandon operation [[RFC2251](#)] which clients may use to cancel other operations. The Abandon operation does not have a response and calls for there to be no response of the abandoned operation. These semantics provide the client with no clear indication of the outcome of the Abandon operation.

X.511 Directory Access Protocol (DAP) [[X.511](#)] provides an Abandon operation which does have a response and also requires the abandoned operation to return a response indicating it was canceled. The LDAP Cancel operation is modeled after the DAP Abandon operation.

The LDAP Cancel operation SHOULD be used instead of the LDAP Abandon operation when the client needs an indication of the outcome. This operation may be used to cancel both interrogation and update operations.

## [2. Cancel Operation](#)

The Cancel operation is defined as a LDAP Extended Operation [[RFC2251](#), [Section 4.12](#)] identified by the IANA-ASSIGNED-OID. This section details the syntax of the Cancel request and response messages and defines additional LDAP resultCodes.

```
cancelRequestValue ::= SEQUENCE {  
    cancelID      MessageID  
}
```

### [2.1. Cancel Request](#)



The Cancel request is an ExtendedRequest with the requestName field containing the IANA-ASSIGNED-OID and a requestValue field which contains a BER-encoded cancelRequestValue value. The cancelID field contains the message id associated with the operation to be canceled.

## **2.2. Cancel Response**

A Cancel response is an ExtendedResponse where the responseName and response fields are absent.

## **2.3. Additional Result Codes**

Implementations of this specification SHALL recognize the following additional resultCode values:

canceled	(IANA-ASSIGNED-1)
noSuchOperation	(IANA-ASSIGNED-2)
tooLate	(IANA-ASSIGNED-3)
cannotCancel	(IANA-ASSIGNED-4)

## **3. Operational Semantics**

The function of the Cancel Operation is to request that the server cancel an outstanding operation issued within the same session.

The client requests the cancelation of an outstanding operation by issuing a Cancel Response with a cancelID set to the message id of the outstanding operation. The Cancel Request itself has a distinct message id. Clients SHOULD NOT request cancelation of an operation multiple times.

If the server is willing and able to cancel the outstanding operation identified by the cancelId, the server SHALL return a Cancel Response with a success resultCode and the canceled operation SHALL fail with canceled resultCode. Otherwise the Cancel Response SHALL have a non-success resultCode and SHALL NOT have impact upon the outstanding operation (if it exists).

The protocolError resultCode is returned if the server is unable to parse the requestValue or the requestValue is absent,

The noSuchOperation resultCode is returned if the server has no knowledge of the operation requested to be canceled.

The cannotCancel resultCode is returned if the identified operation



does not support cancelation or the cancel operation could not be performed. The following classes of operations are not cancelable:

- operations which have no response,
- operations which create, alter, or destroy authentication and/or authorization associations,
- operations which establish, alter, or tear-down security services, and
- operations which abandon or cancel other operations.

Specifically, the Abandon, Bind, Start TLS [[RFC2830](#)], Unbind and Cancel operations are not cancelable.

The Cancel operation cannot be abandoned.

The `tooLate` resultCode is returned to indicate that it is too late to cancel the outstanding operation. For example, the server may return `tooLate` for a request to cancel an outstanding modify operation which as already committed updates to the underlying data store.

Servers SHOULD indicate their support for this extended operation by providing IANA-ASSIGNED-OID as a value of the 'supportedExtension' attribute type in their root DSE. A server MAY choose to advertise this extension only when the client is authorized to use it.

#### **[4. Security Considerations](#)**

This operation is intended to allow user to cancel operations they previously issued during the current LDAP association. In certain cases, such as when the Proxy Authorization Control is in use, different outstanding operations may be processed under different LDAP associations. Servers MUST NOT allow a user to cancel an operation belonging to another user.

Some operations should not be cancelable for security reasons. This specification disallows cancelation of Bind operation and Start TLS extended operation so as to avoid adding complexity to authentication, authorization, and security layer semantics. Designers of future extended operations and/or controls should disallow abandonment and cancelation when appropriate.

#### **[5. IANA Considerations](#)**



Registration of the following values [[RFC3383](#)] is requested.

### **[5.1.](#) Object Identifier**

It is requested that IANA register upon Standards Action an LDAP Object Identifier to identify the LDAP Cancel Operation as defined in this document.

Subject: Request for LDAP Object Identifier Registration  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Specification: RFC XXXX  
Author/Change Controller: IESG  
Comments:  
    Identifies the LDAP Cancel Operation

### **[5.2.](#) LDAP Protocol Mechanism**

It is requested that IANA register upon Standards Action the LDAP Protocol Mechanism described in this document.

Subject: Request for LDAP Protocol Mechanism Registration  
Object Identifier: IANA-ASSIGNED-OID  
Description: LDAP Cancel Operation  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@openldap.org>  
Usage: Extended Operation  
Specification: RFC XXXX  
Author/Change Controller: IESG  
Comments: none  
in 2

### **[5.3.](#) LDAP Result Codes**

It is requested that IANA register upon Standards Action the LDAP Result Codes described in this document.

Subject: LDAP Result Code Registration  
Person & email address to contact for further information:  
    Kurt Zeilenga <kurt@OpenLDAP.org>  
Result Code Name: canceled  
Result Code Name: noSuchOperation  
Result Code Name: tooLate  
Result Code Name: cannotCancel  
Specification: RFC XXXX





Author/Change Controller: IESG

Comments: request four consecutive result codes be assigned

## **6. Acknowledgment**

The LDAP Cancel operation is modeled after the X.511 DAP Abandon operation.

## **7. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#) (also [RFC 2119](#)), March 1997.
- [RFC2251] Wahl, M., T. Howes and S. Kille, "Lightweight Directory Access Protocol (v3)", [RFC 2251](#), December 1997.
- [RFC2830] Hodges, J., R. Morgan, and M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", [RFC 2830](#), May 2000.
- [RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", [RFC 3377](#), September 2002.
- [X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(1997) (also ISO/IEC 8824-1:1998).
- [X.690] International Telecommunication Union - Telecommunication Standardization Sector, "Specification of ASN.1 encoding rules: Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER)", X.690(1997) (also ISO/IEC 8825-1:1998).

## **8. Informative References**

- [RFC3383] Zeilenga, K., "IANA Considerations for LDAP", [BCP 64](#) (also [RFC 3383](#)), September 2002.
- [X.511] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory: Abstract Service Definition", X.511(1993).



## **9. Author's Address**

Kurt D. Zeilenga  
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

## Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

## Full Copyright

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed,



or as required to translate it into languages other than English.