Framework External Authentication Reference Manual

Error Handling

12/21/2025

Error Handling

Contents

When there is an error, the LDAP AM delivers two error-related properties to Configuration Server: `error code` and `error description string`. The property `Error code` is reported in the log files, but only the property `error description string` is shown on the client's GUI.

The LDAP AM uses one of three methods to extract this property (listed from highest priority to lowest):

1. Explicit error description returned by the LDAP server.

2. Error description produced from an error code based on the mapping table inside the Authentication Module. This table is populated from a supplied and configured LDAP error description file (`ldaperrors.txt`). See Error Codes.

3. Error description produced from a standard LDAP error code. See Error Codes.

Management Layer Configuration

You can configure the Management Layer to generate various alarms in response to error codes sent from the LDAP AM. See the Framework Management Layer User's Guide.

Special Treatment

If the LDAP AM receives an error code that is marked for retry in the error description file (see Error Codes), it initiates retry attempts according to the policy described in the `retry-attempts` and `retry-interval` parameters specified for this connection. A negative response is returned back to the client only after all retry attempts on all available servers were completed without success.

Error Codes

The LDAP Directory Administrator (Novel E-Directory, IBM Tivoli Directory Server, or Microsoft Active Directory) defines the error codes. Please refer to their documentation.

The following is the content of the default error file (`ldaperrors.txt`) that corresponds to the error descriptions in the OpenLDAP client package:

; server codes

1 Operations error

2 Protocol error

3 Time limit exceeded

4 Size limit exceeded

5 Compare False

6 Compare True

7 Authentication method not supported

8 Strong(er) authentication required

9 Partial results and referral received

10 Referral

11 Administrative limit exceeded

12 Critical extension is unavailable

13 Confidentiality required

14 SASL bind in progress

16 No such attribute

17 Undefined attribute type

18 Inappropriate matching

19 Constraint violation

20 Type or value exists

21 Invalid syntax

32 No such object

33 Alias problem

34 Invalid DN syntax

35 Entry is a leaf

36 Alias dereferencing problem

47 Proxy Authorization Failure

48 Inappropriate authentication

49 Invalid credentials

50 Insufficient access

51 Server is busy

52 Server is unavailable

53 Server is unwilling to perform

54 Loop detected

64 Naming violation

65 Object class violation

66 Operation not allowed on non-leaf

67 Operation not allowed on RDN

68 Already exists

69 Cannot modify object class

70 Results too large

71 Operation affects multiple DSAs

80 Internal (implementation specific) error

 ; API codes

81 Can't contact LDAP server

82 Local error

83 Encoding error

84 Decoding error 85 Timed out

86 Unknown authentication method

87 Bad search filter

88 User cancelled operation

89 Bad parameter to an ldap routine

90 Out of memory

91 Connect error

92 Not Supported

93 Control not found

94 No results returned

95 More results to return

96 Client Loop

97 Referral Limit Exceeded

```
; Old API codes
```

-1 Can't contact LDAP server

-2 Local error

-3 Encoding error

-4 Decoding error

-5 Timed out

-6 Unknown authentication method

-7 Bad search filter

-8 User cancelled operation

-9 Bad parameter to an ldap routine

-10 Out of memory

-11 Connect error

-12 Not Supported

-13 Control not found

-14 No results returned

-15 More results to return

-16 Client Loop

-17 Referral Limit Exceeded

16640 Content Sync Refresh Required

16654 No Operation

16655 Assertion Failed

16656 Cancelled

16657 No Operation to Cancel

16658 Too Late to Cancel

16659 Cannot Cancel

retry-errors
```
    81 85 91 -1 -11
```

Error Messages

This section describes error messages returned by the LDAP server.

> **Important**
>
> The messages in this section correspond to standard LDAP messages. However, your particular LDAP server may be configured to produce different messages in the same situations.

Inappropriate Authentication

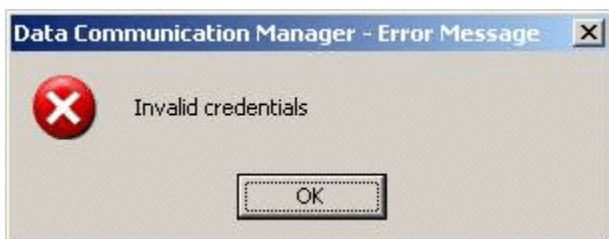A message similar to that shown in the following figure may appear when both of the following conditions are true:

- Option `allow-empty-password` is set to `true` (the default).
- A blank password has been passed to the LDAP AM.

To correct this error, log on to your GUI application with a valid non-empty password.

Invalid Credentials

A message similar to that shown in the following figure may appear when an incorrect password has been passed to the LDAP AM:

To correct this error, log on to your GUI application with a valid non-empty password.

Can't Contact LDAP Server

A message similar to that shown in the following figure may appear when the Configuration Server cannot contact any LDAP server for one or more of the following reasons:

- The LDAP server is down.

- The LDAP server cannot be accessed due to network problems.

- If you configured Genesys Security Using the TLS Protocol, one or more security parameters specified in the configuration file are not valid.

To correct this error, do the following:

- Check that at least one LDAP server is running.

- Check that at least one LDAP server is accessible over the network.

- If you configured Genesys Security Using the TLS Protocol, check that the security parameters specified in the configuration file are valid.