



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Framework External Authentication Reference Manual

Security Considerations

12/22/2025

Security Considerations

Contents

- **1 Security Considerations**
 - **1.1 Configuring Server Authentication**
 - **1.2 Enable FIPS 140-2 compliance**
 - **1.3 Security Certificates**

This section contains recommendations and information about setting up secure connections to the LDAP server.

Warning

When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Genesys does not support specifying different client certificates (and/or certificate authority certificates) for different connections.

In addition, Genesys strongly recommends that you do the following:

- Set the Genesys URL used to access LDAP to use LDAPS (secure LDAP) protocol.
- Configure your LDAP server to prevent anonymous or unauthenticated access. For example, do not configure LDAP users with blank or empty passwords. This is in addition to not configuring users with empty passwords in the Configuration Database (see the Warning note in [Configuration Options](#)).
- Configure your LDAP server to prevent the directory base being set to null.
- Restrict knowledge of the structure of your LDAP data. For example, some of this information is contained in the External ID field of User objects in the Configuration Database. Therefore, a user who has access to these objects could figure out the LDAP structure.

For more information and recommendations for securing your LDAP environment, refer to the LDAP benchmarks published by the Center for Internet Security and available on the Center's web site.

Configuring Server Authentication

To set up LDAP server authentication, make the following changes to your LDAP configuration:

1. In Configuration Server, set the following options in the **gauth_ldap** section:

- **cacert-path**
- **cert-path**
- **key-path**

For example:

```
[gauth_ldap]
cacert-path=c:\server.cer
cert-path=c:\client.cer
key-path=c:\private.pem
```

2. If you have to adjust the default behavior of Configuration Server to verify the remote LDAP server certificate, set up the **LDAPCONF** environment variable in such a way that it is applicable for Configuration Server processes (for example, in a startup **.bat** file used to launch Configuration Server). For example:

```
LDAPCONF=c:\openldap\ldap.conf
```

3. If you have set up **LDAPCONF** as discussed in the previous step, make sure to specify the following in **ldap.conf**::

- Set **TLS_CACERT** to point to the location of the CA root certificate.
- Set the certificate-handling option (**TLS_REQCERT**) to demand.

For example:

```
TLS_CACERT c:\OpenLDAP\CARootCert.cer  
TLS_REQCERT demand
```

The valid values of the certificate-handling option are:

- **never**—The client never asks the server for a security certificate.
- **allow**—The client asks for a server certificate. If a certificate is not provided, the session proceeds normally. If a certificate is provided but the client is unable to verify it, the certificate is ignored and the session proceeds as if no certificate has been provided.
- **try**—The client asks for a server certificate. If a certificate is not provided, the session proceeds normally. If a certificate is provided but the client is unable to verify it, the session is terminated immediately.
- **demand**—The client asks for for a server certificate, and a valid certificate must be provided. Otherwise, the session is terminated immediately.

For client applications, the default value is demand.

Enable FIPS 140-2 compliance

Configuration Server 8.5.101.28 and later supports FIPS 140-2 compliance for authentication using LDAP.

With this version of Configuration Server, the **gauth_ldap_fips** folder contains the FIPS-consistent files. To enforce FIPS 140-2 compliance, replace the following files from the **gauth_ldap_fips** folder to the base folder, which contains the non-FIPS files:

- In Windows: **gauth_ldap.dll** and **gauth_ldap.pdb**
- In UNIX/Linux: **libgauth_ldap_64.so**

Important

- FIPS 140-2 is supported on Windows and Linux 64-bit only.
- Ensure to take a backup of the existing non-FIPS files in the base folder for future use.

Security Certificates

OpenSSL supports Privacy Enhanced Mail (PEM). PEM encodes the binary DER in base-64 (according to RFC 3548), creating a certificate file in text format.

Genesys Security Pack 8.5.000.15 and later supports a server certificate with an empty subject name and provides an Alternative Subject Name field when configuring a server certificate.

For more information about using TLS and security certificates, refer to the *Genesys Security Deployment Guide*.

Warning

Host names specified in the **Insurer**, **Subject**, and **Subject Alternative Name** fields are case-sensitive and must match the corresponding entries in the DNS. And if used in a Windows domain, they must also match Active Directory records.

CA Certificates File

The following is an example of a sample Certificate Authority (CA) certificates file that can be used to validate the LDAP server authentication without mutual authentication, and is a concatenation of several CAs. The CA to validate the remote LDAP server certificate is selected automatically by Configuration Server. The first example is valid for the target host; the second is not.

```

-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIJA0GkFzNTb8K0MA0GCSqGSIb3DQEBBQUAMIGVMQswCQYD
VQQGEwJVSjTEVMBMGA1UECBMmU3Q0UgV0ZXJ1dXJnMRUwEwYDVQHQEwXjTdC5Q2XRl
cmJlcmcxEDA0BgNVBAsTB0bldmVzeXNkCzAJBgNVBAsTA1FBMRyYwFAYDQVQGEwQ0
OTIuMTUyMTJlZjg1ZjJyMSEwHwYJKoZIhvcNAQkBFhJyb290QDE5M14xNjguODUuMjIw
HhcNMTIwMTI3MTMyODM4W4hcNMTcwMTI1MTMyODM4WjCBTELMAKGA1UEBhMCUuX
FTATBgNVBAGTDFN0LLBldGvYyNvYzZEVMBMGA1UEBxMMMU3Q0UgV0ZXJ1dXJnMR
AwDgYDVQKKEwDHZW5lc3lzMQswCQYDVQKLEwJRQTEWMBQGA1UEAxMMNMTkyLjE2
0C44NS44MjEhBMB8CSqGSIb3DQEJARYScam9vdeAXOTIuMTUyMTJlZjg1ZjIyMiI
BhGgW0BhB8GCSqGSIb3DQEAQ8AMIIBCqGCSqGSIb3DQEAkKJTR7G4+XJOHvUwRb2
4az0tDIj/WN5uEuSQSotxzGLqCmQqW577xM1/Xyy5W5ik7tJnbToZyYjVVKamucmW
Mu9bQkr6726Q54ZHTLjFqAQ1L/E2vaHcTktxmdXEDXFH4uv9ghv7388/m5ptqorM0T
2uZwasjoliw9ehpt5UICirx0/LD8LvSP0Sc5odhdQCvF/VCA0ay8PY+0mT2eSPh/
tRly0DfVmpjN4X46w12qWwZoDzTk6g5WUXERPgkPyj6gKv0rUyKzMTIRITb+5Ky
82qoGRTL2aUC6n1VjYc1ZLCY9rU9d0LDf5mdX5P+Aqq+pOUARRDELtP/AMyo96q
SWIDAQABo4H9MIH6MB0GA1UdDgQWBBo7rdRmh9S/9AQKI+OHwVVCvbo/UjCBYgYD
VR0jBiHCMIG/gBTo7rdRmh9S/9AQKI+OHwVVCvbo/UqGBm6SBmDCB1TELM
AKGA1UEBhMCUuXFTATBgNVBAGTDFN0LLBldGvYyNvYzZEVMBMGA1UEBxMMMU3
Q0UgV0ZXJ1dXJnMRAwDgYDVQKKEwDHZW5lc3lzMQswCQYDVQKLEwJRQTEW
MBQGA1UEAxMMNMTkyLjE20C44NS44MjEhBMB8GCSqGSIb3DQEJARYScam9vde
AXOTIuMTUyMTJlZjg1ZjIyYggkA4aQXMI1Nvwo4W DAYDVR0TBAlUwAwEB/zAN
BgkqhkiG9w0BAQUFAAOCAQEAGkdPXqZ9j13Ekz3G42vUCIvvEonhUSF0/nGV8pE
JivHZ00+oYXndRCEi0RKF/6nzab17b+w15fbU0uEjYr+DSTiKvKEukBxguLe9
3k5Ds4vuj0JqcvZ9aM1cVUWXDj0jH9tWK++l7QU0D8cJQ T+kBwqhYqYwZE7r
CkPaz2tKo0ZR6APgY4B8fUk0qHbrJGtLxLNsXBis9VCjYh+LN1ZqdRPic8qYU
bct+7y4e9YVBVseoiSnnICPmaTKA50obvJx6XhNBSNiU5PIRP93LstSqum+Vj
7nC8kAMPVje60MKNSNLC56mH4/TY47wMJ6JHh9q0jB4jbybDTu45A==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIErTCCA8GaAwIBAgIJAj59nclvL1raMA0GCSqGSIb3DQEBBQUAMIGjM0swCQYD

```

VQQGEwJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMQU2FpbnQtUGV0ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAkGA1UECzM CUUEXfjAUBgNVBAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbW FuLn1lc2hpbkBnZW5lc3lzbGFiLmNvbTAeFw0wOTA0MDkwNjA1NDZaFw0xNDA0MDgwNjA1NDZaMIGjMQswCQYDVQQGEwJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMQU2FpbnQtUGV0ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAkGA1UECzM CUUEXfjAUBgNVBAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbW FuLn1lc2hpbkBnZW5lc3lzbGFiLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA0ZGBia4Dw878dtri7CuV0+r3hYD/voMB0brsPAhHMA64P0FTtVPexT8E7p55ysd0VLjf7593wHzcAYSfD5j3NTr07Nui80toB77U/urTxMu1jq9o3LfRqN6rgg0p0fbkuvIS7vmCiidS1G00bIob6GAav3swC38t8Rzv50NCmpiITxKS3GwwledVfijdlfG7ookxe2wJALGp8HYYgoQKqN2h5C+QUhvg4T/NNv3up+LI/1T4U269EK3NaElChf26q380H0BG/rYcX1iZJdPxiz1L4BsspMfhgK3Zff3WJVWjEoN5xG/Igbl82voNk73WCotSWIa22cqxsPK/BvP7jUCAwEAAa0CAQwwggEIMB0GA1UdDgQWBBRLdA7o98BjAragLk0L5rj89HsveDCB2AYDVR0jBIHQMIHNgBRldA7o98BjAragLk0L5rj89HsveKGBqaSBpjCBozELMAkGA1UEBhMCnUxEzARBgNVBAgTCnNvbWUtc3RhdGUxGTAXBgNVBAcTEFNhaW50LVBlldGVyc2JlcmcxZzARBgNVBAoTCmdlbmVzeXNsYWIXCzAJBgNVBAsTAlFBMRYwFAYDVQQDEw0xOTIuMTY4LjczLjIyMSowKAYJKoZIhvcNAQkBFhtyb21hbi55dXNoaW5AZ2VuZXN5c2xhYi5jb22CCQCefZ3Jb1dYETAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBZLUuooFJB4UFxlmrnVvyw0atrSN7dCiEr418uK4VgCNDrw+lgalPcmGe0IVRI0/uJuAKC+GJXPL5wheTT+NIhGW5BNpLam4PPikb3mo8GwdDldqXbbsVUmpI/9hL9eGNAh/IJ1CJD6Jkp7IKmiU6yTzv5qqw84EkXDDfvmhFvnYU6SG1zouxg2W8H20bWuFGIX9W4wNMmpdH+SaLWRnrVGX7ABv+AGNkhqCe8qmgw5Pkio/HbPd77jqgrSUMYtnWB6cEXhzqkV3T0kb9sFKN9APYx/L7AesD0+LdciI13yBjsy9KUIcroeBF7J1HGqLfnw0v+SY40I+7m6QXiMMk

Output Using OpenSSL Utility

openssl.exe is the main utility in the OpenSSL toolkit. When it is run against the CA certificates file in the previous section, the following output is produced:

```
depth=1 /C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
verify return:1
depth=0 /C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
verify return:1
---
Certificate chain
0 s:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
i:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
1 s:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
i:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDKTCCAHECCQChnoaG7KJ6jANBgkqhkiG9w0BAQUFADCBTELMAKGA1UEBhMC
ULUxFTATBgNVBAGTDfN0LlBldGVyYnVyZzEVMBMGGA1UEBxMMU3QuUGV0ZXJidXJn
MRAwDgYDVQQKEwdHZW5lc3lzMQswCQYDVQQLLEwJRQTEWMBQGA1UEAxMNMTkyLjE2
OC44NS44MjEhMB8GCSqGSIb3DQEJARYScm9vdEAXOTIuMTY4Ljg1LjIyMB4XDTEy
MDEzMDEwNDExNVoXDTE1MDEyOTEwNDExNVowZoxCzAJBgNVBAYTALJVMRUwEwYD
VQIEWwTdc5QZXRLcmJlcmcxFTATBgNVBACTDfN0LlBldGVyYnVyZzEQMA4GA1UE
ChMHR2VuZXN5czELMAKGA1UECXMUUEXfjAUBGNVBAMTDTE5Mi4xNjguODUuODIx
JjAkBgkqhkiG9w0BCQEWf3Z2b2xvZGluQWdlbmVzeXNsYWYyY29tMIGfMA0GCSqG
SIb3DQEBBQUAA4GNADCBiQKBgQCrlZ+/59mVFg3sTGZrnQf0Ln5VdypLz55HoHlq
FfxOnax70BLgGzqhvioUL7vwmwmhzUXqcpeJxBLAGKGYzHh6SPkBHInAqLfdKG5o
9108Iu+S9RtdTBMGc8hQH1zuQQlaraSLvKS5TPTvkyd+mHMLKvDCGAg0cl/q585V
+ir3pwIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQBmR82yIr/j0iYu9I1+sprv+gMV
9XTHSpqBKG7XuwI+X4G3tGI+uS05gdHHZGz5or76nMIUUSYCsDC86aAapXDyGfxf
lLbY/NoQdn1FPrJQpeRFK1o4i7zFR2+lyYZfNr3JDbhLGspe6N0HkzNBFghxWpG
ysJIXXLTBvdKcM5Tj/PGSMQTsCFWai0brm9P5L6yxx+uFdF+oLYa/hE0V99d0fYI
sYYocjKrYmNNgpKK2kPWuu8F1uG01MhLAskihjYD2LT3MkPoSowphtMkDw6Gnxz5
Z4YB2JJW2r//IEIhNvt/qhV+A0Tv0EYL6Lo4BAHleTMwvhrWltDAK73LooDB
-----END CERTIFICATE-----
subject=/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
issuer=/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
---
No client certificate CA names sent
```

Security Considerations

```
---
SSL handshake has read 2179 bytes and written 340 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher : AES256-SHA
  Session-ID: 7D705B895D61F2A200108095528864BB8C74EDE80168B69FA96AF3AD5FE0F4F8
  Session-ID-ctx:
  Master-Key: F1446F0B8F8B6E605AD923B0B24A08BADD91B82ABA24C13FCEB59D3B939822779A331F583C66EC91187740F49F2F572C
  Key-Arg : None
  Krb5 Principal: None
  Start Time: 1351273962
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
---
```