Framework External Authentication Reference Manual

Security Considerations

5/6/2025

Security Considerations

Contents

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** environement 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`.

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-----
MIIErTCCA5WgAwIBAgIJAOGkFzNTb8KOMA0GCSqGSIb3DQEBBQUAMIGVMQswCQYD
VQQGEwJSVTEVMBMGA1UECBMMU3QuUGV0ZXJidXJnMRUwEwYDVQQHEwxTdC5QZXRl
cmJ1cmcxEDAOBgNVBAoTB0dlbmVzeXMxCzAJBgNVBAsTAlFBMRYwFAYDVQQDEw0x
OTIuMTY4Ljg1LjgyMSEwHwYJKoZIhvcNAQkBFhJyb290QDE5Mi4xNjguODUuMjIw
HhcNMTIwMTI3MTMyODM4WhcNMTcwMTI1MTMyODM4WjCBlTELMAkGA1UEBhMCUlUx
FTATBgNVBAgTDFN0LlBldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJnMRAw
DgYDVQQKEwdHZW5lc3lzMQswCQYDVQQLEwJRQTEWMBQGA1UEAxMNMTkyLjE2OC44
NS44MjEhMB8GCSqGSIb3DQEJARYScm9vdEAxOTIuMTY4Ljg1LjIyMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAskkJTR7g4+XJOHVuwRbt4az0TdI/WN5u
EuSQSotxzGLqCmQQws77xM1/Xyy5W5ik7tJnbToZzYjVVkamucmWMu9bQkr6726Q
S4ZHTLjFqAQ1L/E2vaHcTktmdx0EDXfH4uv9ghv7J88/m5ptqorM0T2uZwasjolI
w9ehpt5UICirxO/lD8LvsP0Sc5odhDQCVf/VCaOaY8PY+0mT2eSPh/tRlyODfvMp
jN4Xa6wl2qWWZoDzTk6g5WUXERPgkPyj6gKv0rUyKzMTRITb+5Ky82qoGRTl2aUC
6nlVJYc1ZlCY9rU9d0LDft5mdX5P+Aqq+pOUARRDELtP/AMyo96qSwIDAQABo4H9
MIH6MB0GA1UdDgQWBBTo7rdRmh9S/9AQKI+OHWVCvbo/UjCBygYDVR0jBIHCMIG/
gBTo7rdRmh9S/9AQKI+OHWVCvbo/UqGBm6SBmDCBlTELMAkGA1UEBhMCUlUxFTAT
BgNVBAgTDFN0LlBldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJnMRAwDgYD
VQQKEwdHZW5lc3lzMQswCQYDVQQLEwJRQTEWMBQGA1UEAxMNMTkyLjE2OC44NS44
MjEhMB8GCSqGSIb3DQEJARYScm9vdEAxOTIuMTY4Ljg1LjIyggkA4aQXM1Nvwo4w
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAGKdPXqZ9j13Ekz3G42vU
CIvvEonhUSFO/nGV8pEJivHZ0O+oYXndRCeiORKF/6nzab17b+w15fbU0uEJyR+D
S3IkVkEukBxguleu93kQ5Ds4vuj0JqcvZ9aM1cVVWXDj0jH9tWK++l7QUOD8Cj0Q
T+kBWqhYgYwqZE7rcKapzQtKo0ZR6APgY4B8fUkb0qHbRJGEtLxlNsXBi9VGcYQh
+LN1ZqdRPic8qqYuBt+7y4e9VBVseoiSNnIcPmaTkASOobvJx6qQhBu8NSIU5pIR
RP93LtSqUm+Vj7nC8kAMpVje60MKNSNLC56mH4/TY47wMJ6JHh9q0jB4jbybDTu4
5A==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE2TCCA8GgAwIBAgIJAJ59nclvV1gRMA0GCSqGSIb3DQEBBQUAMIGjMQswCQYD
VQQGEwJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMQU2FpbnQtUGV0
ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAkGA1UECxMCUUExFjAUBgNV
BAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbWFuLnl1c2hpbkBn
ZW5lc3lzbGFiLmNvbTAeFw0wOTA0MDkwNjA1NDZaFw0xNDA0MDgwNjA1NDZaMIGj
MQswCQYDVQQGEwJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMQU2Fp
bnQtUGV0ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAkGA1UECxMCUUEx
FjAUBgNVBAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbWFuLnl1
c2hpbkBnZW5lc3lzbGFiLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAOZGBia4Dw878dtri7CuVO+r3hYD/voMBObrsPAhHMA64P0FTtVPexT8E7p5
5ysd0VLjf7593wHzcAYSfD5j3NTrO7Nui8OtoB77U/urTxMu1jq9o3LfRqN6rgg0
p0fbkuviS7vmCiidS1G0ObIob6GAAv3swC38t8Rzv50NCMpiITxKS3Gww1edVfij
dlfG7ookxe2wJALGp8HYYgoQKqN2h5C+QUhvg4T/NNv3up+LI/1T4U269EK3NaEl
Chf26q380H0BG/rYcX1iZJdPxiZ1L4BsspMfhgK3Zff3WJVWjEoN5xG/Igbl82vo
Nk73WCotSWIa22cqxsPK/BvP7jUCAwEAAaOCAQwwggEIMB0GA1UdDgQWBBRLdA7o
98BjAragLk0L5rj89HsveDCB2AYDVR0jBIHQMIHNgBRLdA7o98BjAragLk0L5rj8
9HsveKGBqaSBpjCBozELMAkGA1UEBhMCcnUxEzARBgNVBAgTCnNvbWUtc3RhdGUx
GTAXBgNVBAcTEFNhaW50LVBldGVyc2J1cmcxEzARBgNVBAoTCmdlbmVzeXNsYWIx
CzAJBgNVBAsTAlFBMRYwFAYDVQQDEw0xOTIuMTY4LjczLjIyMSowKAYJKoZIhvcN
AQkBFhtyb21hbi55dXNoaW5AZ2VuZXN5c2xhYi5jb22CCQCefZ3Jb1dYETAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBZlUuooFJB4UFxlmrnVvywOatr
sN7dCiEr418uK4VgCNdRw+lga1PcMGeOIVRI0/uJuAKC+GJXPL5wheTT+NIhGW5B
NpLam4PPikb3mo8GwdDldqXbbsVUmpI/9hL9eGNAh/IJ1CJD6Jkp7IKmiU6yTzv5
qqw84EkXDDfvmhFnvnYU6SG1zouxg2W8H20bWuFGIX9W4wNMmpdH+SaLWRnrVGX7
ABv+AGNkhqCe8qmgw5Pkio/HbPd77jqgrSUmYtnWB6cEXhzqkV3T0kb9sFKN9APY
x/L7AeSD0+LdciIl3yBjsy9KUicroeBF7J1HGqlFnw0v+SY4OI+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/email/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-----
MIIDKTCCAhECCQCHnhoaG7KJ6jANBgkqhkiG9w0BAQUFADCBlTELMAkGA1UEBhMC
UlUxFTATBgNVBAgTDFN0LlBldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJn
MRAwDgYDVQQKEwdHZW5lc3lzMQswCQYDVQQLEwJRQTEWMBQGA1UEAxMNMTkyLjE2
OC44NS44MjEhMB8GCSqGSIb3DQEJARYScm9vdEAxOTIuMTY4Ljg1LjIyMB4XDTEy
MDEzMDEwNDExNVoXDTE1MDEyOTEwNDExNVowgZoxCzAJBgNVBAYTAlJVMRUwEwYD
VQQIEwxTdC5QZXRlcmJ1cmcxFTATBgNVBAcTDFN0LlBldGVyYnVyZzEQMA4GA1UE
ChMHR2VuZXN5czELMAkGA1UECxMCUUExFjAUBgNVBAMTDTE5Mi4xNjguODUuODIx
JjAkBgkqhkiG9w0BCQEWF3Z2b2xvZGluQGdlbmVzeXNsYWIuY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCrlZ+/59mVFg3sTGZrnQf0Ln5VdypLz55HoHlq
FfxOnax70BLgGzqhvioUL7vwmwmhzUXqcpeJxBlAGKGYzHh6SPkBHinAqLfdKG5o
91O8Iu+S9RtdTBMGc8hQH1zuQQlaraSLvKS5TPTvkyd+mHMlKvDCGAg0cl/q585V
+ir3pwIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQBmR82yIr/j0iYu9I1+sprv+gMV
9XTHSpqBKG7Xuwi+X4G3tGI+uS05gdHHzGz5or76nMIUUSYCsDC86aAapXDyGfxf
lLbY/NoQdn1FPrJQpeRFrK1o4i7zFR2+lyYZfNr3JDbhLGspe6NOHkzNBFghxWpG
ysJIXXLTBvdKcM5Tj/PGSMQTsCFWai0brm9P5L6yxx+uFdF+olYa/hE0V99dOfYI
sYYocjKrYmNNgpKK2kPWuu8F1uGO1MhlAskihjYD2lT3MkPoSowphtMkDw6Gnxz5
Z4YB2JJW2r//IEIhNvT/qhV+AOTv0EYL6Lo4BAHleTMwvhRWltDAK73LooDB
-----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
```

```
---
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)
---
```