Framework External Authentication Reference Manual

Kerberos External Authentication

4/3/2026

Kerberos External Authentication

Contents

This chapter describes how Configuration Server supports Kerberos external authentication for Genesys user interface applications.

Overview

Configuration Server and Configuration Server Proxy support the use of the Kerberos authentication protocol for user authentication in Genesys user interface applications. Kerberos enables secure communication between nodes over a non-secure network, using tickets to enable the nodes to prove their identity to each other in a secure manner.

Configuration Server uses Windows Active Directory and MIT key distribution centers to implement Kerberos authentication.

Kerberos vs RADIUS/LDAP

Kerberos, RADIUS, and LDAP are all types of external authentication. However, Kerberos differs from the existing external authentication protocols (RADIUS, LDAP, and others) by when the authentication is performed, as follows:

- Existing external authentication protocols operate in “in behind” mode. That is, the authentication is carried out when the interface application sends the request to Configuration Server, which then forwards it to the authentication system.
- Kerberos operates in “in front” mode. The authentication is activated on the client side before a connection to Configuration Server is made. When the actual connection to Configuration Server is made, the interface gets an authentication ticket (a Kerberos token) that is already authenticated. This ticket is sent to Configuration Server with the login request to assert that authentication is already done.

Kerberos runs independently of RADIUS and LDAP, and can run even when internal authentication is enforced (when `library=internal`).

Supported Environments

Configuration Server supports Kerberos authentication on the following operating systems:

- Red Hat Enterprise Linux (RHEL) version 5 and later
- Windows 2008 and later
- Solaris version 10 and later
- AIX version 5.3 and later

The following versions of MIT Kerberos are used:

- krb5-1.11 for supported UNIX platforms
- kfw-4.0.1 for Windows

Deploying Kerberos External Authentication

To deploy Kerberos, do the following:

1. Configure Kerberos on Configuration Server or Configuration Server Proxy. In the options of the Configuration Server or Configuration Server Proxy Application object, create the **gauth_kerberos** section, and set the following options:

- **SPN**
- **realm**
- **keytab**

2. Install Kerberos on the host on which that Configuration Server or Configuration Server Proxy is running. Follow the steps corresponding to the operating system of the host on which the Configuration Server or Configuration Server is running.

Prerequisite

- Kerberos must be configured on the Configuration Server or Configuration Server Proxy as described in Step 1.

[+] Show steps

Windows 32-bit

a. Install MIT kerberos for Windows 4.0.1 32 on the host on which Configuration Server or Configuration Server Proxy is running. The executable file is available here.

b. Make sure that the Kerberos Initialization File (**krb5.ini**) file contains correct information in the **libdefaults** and **realms** sections. This file is usually located in the Windows directory or in the Kerberos initialization directory (**C:\ProgramData\MIT\Kerberos5**), but may have been placed elsewhere. If you cannot find it, use a file-search utility, such as Windows Search, to locate it. See Kerberos Initialization File for more information about this file.

Windows 64-bit

a. Install MIT kerberos for Windows 4.0.1 64 on the host on which Configuration Server or Configuration Server Proxy is running. The executable file is available here.

b. Make sure that the Kerberos Initialization File (**krb5.ini**) file contains correct information in the **libdefaults** and **realms** sections. This file is usually located in the Windows directory or in the Kerberos initialization directory (**C:\ProgramData\MIT\Kerberos5**), but may have been placed elsewhere. If you cannot find it, use a file-search utility, such as Windows Search, to locate it. See Kerberos Initialization File for more information about this file.

RHEL

a. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available here.
The installation process is described http://web.mit.edu/Kerberos/krb5-latest/doc/build/doing_build.html here].

b. After executing **make install**, add the **/usr/local/lib** path to the **/etc/ld.so.conf** file.

c. Run **/sbin/ldconfig**.

d. Make sure that the Kerberos Initialization File (**/etc/krb5.conf**) file contains the correct information in the **libdefaults** and **realms** sections. This file is located in **/etc** by default, but its location can be overridden by setting the environment variable **KRB5_CONFIG**.
See Kerberos Initialization File for more information about this file.

Solaris 10 64-bit

a. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available http://web.mit.edu/Kerberos/dist/krb5/1.11/krb5-1.11-signed.tar here.]
The installation process is described here.

b. Extract the file as follows:

```
mkdir .krb5_install
cd .krb5_install
tar xvf ../krb5-1.11-signed.tar
tar xzvf krb5-1.11.tar.gz
```

c. During the installation, specify the following values for the following configuration options:

```
./configure CC='opt/SUNWspro/bin/cc' CXX='opt/SUNWspro/bin/cc'
CFLAGS='-g -v -xarch=v10' CXXFLAGS='-g -v -xarch=v10'
LDFLAGS='-xarch=v10' LIBS='-lsocket -lnsl -ldl -lresolv'
```

and

```
correspondent --prefix
```

d. After the **corresponding** stage, before the **make** stage, do the following:

i. Add a symbolic link, using the following command (on one line):

```
ln s <installation directory>/plugins/kdb/db2/libdb2/libdb.so
<installation directory>/lib/libdb.so
```

ii. Patch the code at line 358:

```
<source_dir>src.lib.krb5/os/expand_path.c
```

with:

```
-static const struct token {
+static const struct {
const char *tok;
PTYPE param;
const char *postfix;
```

e. Make sure that the Kerberos Initialization File (**/etc/krb5.conf**) file contains the correct information in the **libdefaults** and **realms** sections. This file is located in **/etc** by default, but its location can be overridden by setting the environment variable **KRB5_CONFIG**.
See Kerberos Initialization File for more information about this file.

AIX 64-bit

a. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available here.
The installation process is described here.

b. Extract the file as follows:

```
mkdir .krb5_install
cd .krb5_install
tar xvf ../krb5-1.11-signed.tar
tar xzvf krb5-1.11.tar.gz
```

c. During the installation, specify the following values for the following configuration options, as prompted:

```
./configure CC='/usr/vacapp/bin/xlc' CXX='/usr/vacapp/bin/xlc'
CFLAGS='-g -v -q64 -qlanglvl=newexcp' CXXFLAGS='-g -v -q64
qlanglvl=newexcp' LDFLAGS='-b64 -brtl' LIBS='-ldl' AR='ar -X 32_64'
```

and

```
correspondent --prefix
```

d. After the **corresponding** stage, before the **make** stage, do the following:

i. Add a symbolic link, using the following command (on one line):

```
ln s <installation directory>plugins/kdb/db2/libdb2/libdb.so
<installation directory>/lib/libdb.so
```

ii. Patch the code at line 358:

```
<source_dir>src.lib.krb5/os/expand_path.c
```

with:

```
-static const struct token {
+static const struct {
const char *tok;
PTYPE param;
const char *postfix;
```

e. Make sure that the Kerberos Initialization File (**/etc/krb5.conf**) file contains the correct information in the **libdefaults** and **realms** sections. This file is located in **/etc** by default, but its location can be overridden by setting the environment variable **KRB5_CONFIG**.

> See Kerberos Initialization File for more information about this file.

Kerberos Initialization File

When Kerberos is installed on the host of the Configuration Server or Configuration Server Proxy, it creates an initialization file that contains information about the realms used by Kerberos. This file has different names depending on the platform on which Kerberos is installed, but contains two or, optionally three, sections, as follows:

- **[libdefaults]**—This section is required by Kerberos, and must contain the name of the realm used for authentication. For Windows Active Directory, that default realm must match the name of the Windows domain. By default, this name is the same as the DNS zone where "A" records of all Windows computers in this domain reside. Alternatively, this is the actual name of the Windows Domain in Active Directory only if the domain and DNS namespaces are disjoined. The name of the realm must be in upper case (that is, UPPER_CASE) characters only.
- **[realms]**—This section must contain subsections keyed by Kerberos realm names. Each subsection describes realm-specific information, especially the kdc key with the key distribution center host.
- **[domain_realm]**—(Optional) You can specify mandatory conversion from DNS zone names to realm names, to ensure that only upper-case realm names are being handled by Configuration Server.

The following is a sample of a Kerberos initialization file:

```
[libdefaults]
default_realm = ROOTDOMAIN.CONTOSO.COM

[realms]
KRBTEST.GENESYSLAB.COM= {
   kdc = rh5qa64-1.genesyslab.com
   admin_server = rh5qa64-1.genesyslab.com
   }
ROOTDOMAIN.CONTOSO.COM = {
   kdc = 135.225.51.144
   admin_server = 135.225.51.144
   }

[domain_realm]
.rootdomain.contoso.com=ROOTDOMAIN.CONTOSO.COM
```

For more information, see http://web.mit.edu/Kerberos/krb5-1.5/krb5-1.5/doc/krb5-admin/krb5.conf.html.

For an initialization file on Windows, consult release notes about Windows distribution of Kerberos, at http://web.mit.edu/kerberos/kfw-4.0/kfw-4.0.html to determine the content and location of it.

> ### Important
>
> krb5.11 on Linux and Active Directory as KDC hasn't been tested. If any issue is reported and found to be platform specific, then Genesys support expects the customer to revert to one of the tested Kerberos architectures:

- CSProxy on Linux + krb5.11 compiled on the same host + MIT KDC on Linux.
- CSProxy on Windows + kfw-4.0.1 installed on the same host + Active Directory on Windows.

Service Principal Name

You must define the Service Principal Name (SPN) according to the rules set out by your key distribution center, and provision it in Configuration Server using the **SPN** option. You must use the same SPN as used during keytab file creation by the key distribution center.

When you are using a Windows-based key distribution center and you want to enable Windows-based Genesys client applications, such as Agent Workspace Desktop Edition, or your custom applications written using Genesys PSDK, to use Kerberos with Configuration Server, make sure that you register this SPN in Windows Active Directory, as described in Genesys PSDK documentation and/or documentation for the particular Genesys product that supports Kerberos.

Keytab File

A keytab file is a part of the Kerberos infrastructure. It contains information that is required by Configuration Server to validate user passwords indirectly using Kerberos. When you deploy Configuration Server with Kerberos enabled, you must obtain this file from your key distribution center (as discussed in the following paragraph) and put it in the path specified by the **keytab** configuration option of Configuration Server.

Obtaining the Keytab File

When Kerberos starts, the local host on which Kerberos is installed sends a request to the Key Distribution Center to generate the keytab file with the name that you specify. The KDC generates the keytab file, and stores it in the same folder as the Kerberos initialization file. It must be created before you start to use Kerberos. To configure keytab file creation, use the procedure relevant to the type of Kerberos you are using.

MIT Key Distribution Center

Important

You must have the Inquire administrator privilege to create the keytab file using MIT Key Distribution Center.

To generate the keytab file:

1. Change to the kadmin folder. For example, on UNIX enter:

   ```
   cd /usr/local/bin/krb5-testinst/bin/kadmin
   ```

2. Use the ktadd command to create the keytab file call inside the kadmin folder:

   ```
   ktadd -k <path to resulting keytab> <SPN name>
   ```

   For more details about the syntax of the ktadd comment, see http://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/Adding-Principals-to-Keytabs.html.

Example:

Path to resulting keytab file: /home/user/genesys_sample_keytab
SPN name: confserver/somehost

```
ktadd -k /home/user/genesys_sample_keytab confserver/somehost
```

Windows Active Directory

> **Important**
> You must have domain administrator rights to create the keytab file using Windows Active Directory.

Use the setspn command to map the SPN to a user:

```
setspn -A <SPN> <username>
```

Use the `ktpass` command to create the keytab file, specifying the realms in upper-case:

```
ktpass /princ <SPN>@<REALM> /mapuser <User name>@<REALM /pass <password> /out <Keytab file name> /crypto all /ptype KRB5_NT_PRINCIPAL
/mapop set
```

For more details about the `ktpass` command, refer to https://technet.microsoft.com/en-us/library/cc776746(v=ws.10).aspx.

Example:

User name (known by Key Distribution Center): `rootUser2` with password `genesys`
SPN: `confserver/somehost`
Keytab file name: `c:\genesys-rootdomain.keytab`
Realm: `ROOTDOMAIN.CONTOSO.COM`

Mapping of SPN "confserver/somehost" to rootUser2:

```
setspn -A confserver/somehost rootUser2
```

To create the Keytab file:

```
ktpass /princ confserver/somehost@ROOTDOMAIN.CONTOSO.COM /mapuser rootUser2@ROOTDOMAIN.CONTOSO.COM /pass genesys /out c:\genesys-
rootdomain.keytab /crypto all /ptype KRB5_NT_PRINCIPAL /mapop set
```

Sample Kerberos Configurations

This section contains examples of how to configure Kerberos for integration with an MIT Key Distribution Center implementation, and for a Microsoft Active Directory implementation.

[+] Show examples

MIT Key Distribution Center

This is an example of a Kerberos configuration to integrate with an MIT Key Distribution Center (KDC) implementation.

Basic Information

KDC installed at: **rh5qa64-1.genesyslab.com**
Realm: **KRBTEST.GENESYSLAB.COM**
Sample service name: **genesys_sample**
Username (known by KDC): **testclient** with password **123456**

On Configuration Server machine, MIT Client Configuration

File **C:\ProgramData\MIT\Kerberos5\krb5.ini**, section **[realms]**:

```
KRBTEST.GENESYSLAB.COM = {
   kdc = rh5qa64-1.genesyslab.com:88
   admin_server = rh5qa64-1.genesyslab.com:749
   }
```

On Configuration Server (Server Level):

```
...
[gauth_kerberos]
SPN=genesys_sample/rh5qa64-1
realm=KRBTEST.GENESYSLAB.COM
kdc_host=rh5qa64-1.genesyslab.com
keytab=genesys-krbtest.keytab
...
```

and Person object with username `testclient` under the Environment tenant.

Microsoft Active Directory

This is an example of a Kerberos configuration to integrate with a Microsoft Active Directory implementation.

Basic Information

Windows domain controller is being used as KDC:

- Domain **rootDomain.contoso.com**
- Controller machine: **W2k8r-ay-root.rootDomain.contoso.com(135.225.51.14)**

Realm: **ROOTDOMAIN.CONTOSO.COM**
Sample Service name: **confserver/somehost**; there is a mapping made from this service name to the windows domain account **rootUser2** with password **genesys** to produce a keytab file with a secret password that can be used on the Configuration Server side.
User name (known by KDC): **rootUser1** with password **genesys**

On Configuration Server machine, MIT Client Configuration:

File **C:\ProgramData\MIT\Kerberos5\krb5.ini, section**, **[realms]**:

```
ROOTDOMAIN.CONTOSO.COM = {
   kdc = 135.225.51.144
   admin_server = 135.225.51.144
   }
```

On Configuration Server (Server Level):

```
...
[gauth_kerberos]
SPN=confserver/somehost
realm=ROOTDOMAIN.CONTOSO.COM
keytab=genesys-rootdomain.keytab
...
```

and Person object with username `rootUser1` under Environment tenant.

Character Case Considerations

When an instance of Configuration Server or Configuration Server Proxy is configured for Kerberos authentication, user objects are located by comparing the Windows login name provided by the Kerberos ticket with the user names of Person objects defined in Configuration Server. These searches are done on a case-sensitive basis. You can override this and make the search case-insensitive. This is especially useful if your system is using Microsoft Windows Active Directory as the Key Distribution Center, in which case, the Windows login names are case-insensitive.

To override the default behavior of the comparison, and make it a case-insensitive search, set the **ignore-case-username** option to `true`. If the search results in more than one user object with the same username regardless of case, Configuration Server will not authenticate the user. Instead, it will generate the CFGAccessDenied error.

This functionality does not apply if the username and password are provided directly in the registration request.

Redundant Configuration Servers

When primary and backup Configuration Servers are running on separate hosts, they can both use the same principal name (the **SPN** option). Each Configuration Server must be configured to use Kerberos, as described in this section; otherwise, no special configuration is required.

If the two servers are running on the same host and using the same **SPN**, the server applications must run under different system user accounts. That is, they must use a different user name in the Windows Services property—the **Log in as** field on the **Log on** tab.

Using Kerberos with Multiple Windows Active Directory Domains

You must specify Configuration Server SPN in Active Directory so that Kerberos-enabled Windows applications can get the proper ticket in a realm that matches the Configuration Server keytab. You can do this in one of two ways:

- Have the Configuration Server SPN (and keytab) defined in the same Windows domain (Active Directory service) as any client accounts that will be used to obtain tickets.
- In a forest of Windows Active Directory domains, you must set up a two-way transitive trust between domains if you want to use an account in one domain to access a Configuration Server for which its SPN (and keytab) are defined in another domain. **Example:**
  - Agents are in Active Directory Domain A.
  - Servers are in Active Directory Domain B. This includes Configuration Server Proxy, so Configuration Server Proxy SPN (SPN1) is also in AD Domain B.
  - Workspace Desktop Edition (WDE) is deployed with SPN1 in its settings.
  - Agents log in to WDE using accounts in Active Directory Domain A.

  As a result of the trust relationship, tickets that are obtained by agents in Active Directory Domain A to access the service defined by SPN1 are accepted by Configuration Server with the keytab generated for SPN1 in Active Directory Domain B.

  Refer to https://technet.microsoft.com/en-us/library/cc731335.aspx for detailed information about trusts in Microsoft Windows Active Directory.

  When Configuration Server is used to authenticate users from multiple Active Directory domains, use the **enable-upn** option to utilize UPN-style usernames and to avoid issues with duplicate usernames across multiple domains.

Configuration Options

This section describes the configuration options used to configure Kerberos on Configuration Server and Configuration Server Proxy.

> ### Warning
> Configuration section names, configuration option names, and predefined option

> values are case-sensitive. Type them in Genesys Administrator exactly as they are documented here.

Setting Configuration Options

Unless otherwise specified, set Kerberos configuration options in the options of the Configuration Server or Configuration Server Proxy Application object. This will allow clients, such as Workspace Desktop Edition, to negotiate Kerberos authentication with Configuration Server or Configuration Server Proxy, when Kerberos is available on the client side.

Mandatory Options

The following options are mandatory, and must be set before using Kerberos.

- **SPN**
- **realm**
- **keytab**

authentication Section

This section is mandatory on the Server level to enable external authentication. It can, however, appear in other locations as mentioned in Setting Configuration Options.

This section must be called *authentication*.

enable-upn

Default Value: `0`
Valid Values: `0` to 2
Changes Take Effect: After next login

Specifies whether Configuration Server allows Kerberos users to be configured and authenticated using Windows-compatible User Principal Name (UPN) format of usernames.
Valid values are:

- `0` (zero, the default value)—Kerberos authentication for UPN usernames is not enabled. Users authenticated through Kerberos should not have the "`@domain`" suffix in their usernames on Configuration Server.
- 1—UPN-style usernames and plain usernames are allowed for the same user to log in. When Configuration Server login contains UPN credentials, the first user object with UPN is searched for. If the user object is not found, the domain name in the UPN credentials is removed and another search attempt is made. The user is authenticated successfully if either format of username is configured. You must configure this value when you migrate from using the plain username to UPN-style usernames across users authenticated through Kerberos.
- 2—UPN-style login is used strictly. When Configuration Server login contains UPN credentials, the user with UPN is searched for and if the user is not found, an error is returned.

gauth_kerberos Section

This section is mandatory, and contains information about the Kerberos installation on this Configuration Server or Configuration Server Proxy.

This section must be called *gauth_kerberos*.

SPN

Default Value: Empty string
Valid Value: Any valid name
Changes Take Effect: Immediately

The Service Principal Name, in the format `service/hostname`, the same as that used by a client in the service parameter. This name must be registered with the key distribution center to which this configuration is pointing (as defined by the platform-specific configuration).

realm

Default Value: Empty string
Valid Value: Any valid name
Changes Take Effect: Immediately

The name of the Kerberos infrastructure, as known by the MIT client library and/or the key distribution server being used. The value must be specified in all upper-case letters in the form of a domain address (`ENTITY.SUBDOMAIN.ROOTDOMAIN`).

keytab

Default Value: Empty string
Valid Value: Any valid name
Changes Take Effect: Immediately

The name of the keytab file that is generated by the key distribution center and propagated to the host on which this Configuration Server or Configuration Server Proxy is running. This file must exist in the installation directory of this Configuration Server (primary or backup) or Configuration Server Proxy.

krb-max-ticket-length

Default Value: `12000`
Valid Values: Integer between `12000` and `64000` inclusive
Changes Take Effect: Immediately

Specifies the maximum length (in bytes) of the Kerberos ticket or GSS token to be validated by the Kerberos/GSS authentication library. A ticket/token with a length greater than the value of this option is rejected. If this option is not specified, or the value is less than `12000` or greater than `64000`, the default value (`12000`) is used.

ignore-case-username

Default Value: `false`
Valid Value: `true`, `false`
Changes Take Effect: Immediately

When locating the authenticated user object based on its login name, this option specifies whether the comparison of the login name of the objects with the username specified in the Kerberos ticket is made on a case-insensitive (`true`) or case-sensitive (`false`) basis. If this option is set to `true`, and the search results in more than one user object with a username matching the provided login name, Configuration Server will not authenticate the user. Instead, it will generate the CFGAccessDenied error.

This option is useful if the environment is using Microsoft Windows Active Directory as the Key Distribution Center, in which case the usernames are case-insensitive. This option does not apply if the username and password are provided directly in the registration request.

Troubleshooting

If you have Kerberos authentication issues on the Configuration Server side, enable additional logging from the MIT Kerberos implementation by adding the environment variable KRB5_TRACE=<`log file name and path`> and make this environment variable available to the Configuration Server process. Be sure to restart Configuration Server.