Genesys Security Deployment Guide

Encrypted Configuration Database Password

4/14/2025

Encrypted Configuration Database Password

Contents

- 1 Encrypted Configuration Database Password
  - 1.1 Security Benefits
  - 1.2 Supporting Components
  - 1.3 Feature Description
  - 1.4 Feature Configuration

You can encrypt the password used to access the Configuration Database so that it appears in the Configuration Server logs as an encrypted string of characters.

> **Important**
>
> This encryption does not use the SALT used when encrypting user passwords. See Password Encryption.

Security Benefits

Once encrypted, the password to the Configuration Database is written as an encrypted string of characters into Configuration Server logs. This feature ensures that anyone reading the log cannot obtain the password and use it to access the Configuration Database directly through the DBMS.

Supporting Components

This feature is configured on the Configuration Server accessing the Configuration Database.

Feature Description

All entries in configuration files and logs are readable in plain text, unless explicitly configured to be hidden in some way. You can encrypt your password for accessing the Configuration Database. After password encryption, Configuration Server decrypts the value when reading its configuration file at subsequent startups. It accesses the Configuration Database using the decrypted value, and prints an encrypted string of characters as the password value into the log. In this way, the password does not explicitly appear in the Configuration Server logs.

Feature Configuration

To encrypt the Configuration Database password, do the following:

1. Force Configuration Server to encrypt the password. **[+] Show steps**

   > **Important**

Starting in release 8.5.1, the Configuration Server configuration file optionally supports an asymmetric encryption algorithm using separate encryption and decryption (private) keys that are not hardcoded. In this case, the keys are generated by Configuration Server and stored in separate files. The password is encoded using the key in the encryption file. Upon subsequent restarts of Configuration Server, it uses the key in the decryption file to decrypt and the password. See Encrypting the Configuration Database Password

Prerequisites

- Configuration Server is not running.
- Configuration DB Server is not running.

Start of Procedure

Force Configuration Server to encrypt the password, by starting Configuration Server with the following command line:

```
confserv -p <section name> <password value>
```

where:

-p	The command-line parameter that forces an instance of Configuration Server to start, encrypt the database password in the configuration file, and terminate.
<section name>	The section name in the Configuration Server configuration file that describes the Configuration Database whose access password is being encrypted.
<password value>	The password used for accessing the specified Configuration Database.

Important

- If the configuration file name differs from the default name (**confserv.conf** on UNIX or **confserv.cfg** on Windows), the command line should also contain the **-c** parameter followed by the file name. For a description of command-line parameters specific to Configuration Server, refer to the *Framework Deployment Guide*.
- If a password to be encrypted contains one or more UNIX shell special characters, the password must be enclosed in single quotes in the command line. For example, if the password is `$Montana`, enter the following at the command line:

```
confserv -p gauth_ldap '$Montana'
```

- When using Windows, if a password to be encrypted contains one or more special characters, the password must be enclosed in double quotes in the command line. For

example, if the password is `p&ssword`, enter the following at the command line:

```
confserv -p dbserver "p&ssword"
```

Repeat this step for each Configuration Database section listed in the configuration file of Configuration Server.

2. Configure the **encryption** option in the Configuration Server configuration file. **[+] Show steps**

Prerequisites

Any primary and backup Configuration Servers associated with this Configuration Server have encrypted the password.

Start of Procedure

1. In a text editor, open the Configuration Server's configuration file.
2. In the **[confserv]** section, set **encryption** to `true`. This value applies to all Configuration Database sections specified in the configuration file. Refer to the *Framework Configuration Options Reference Manual* for a full description of this option.
3. Save and close the file.

Now, Configuration Server is ready to operate with the encrypted password.

3. Restart Configuration Server as for a regular operation. Refer to the *Framework Deployment Guide* for detailed information about starting Configuration Server.