Framework Deployment Guide

Security Considerations

4/17/2025

Security Considerations

Contents

This section outlines some of the security capabilities provided in Configuration Layer for your data, both from access by unauthorized users and during its transfer between components. For more information about these and other security features, and for full implementation instructions, refer to the *Genesys Security Deployment Guide*.

Access to Hosts File at Start-up

By default, Genesys components try to read from the hosts file at startup to enable them to resolve host names. If an organization has a security policy against this, they can configure the environment variable **GCTI_DNS_USE_HOSTSFILE=**`0` to disable this access.

User Authentication

User authentication refers to ensuring that the user is actually who he or she claims to be. In Genesys software, this is implemented by the Configuration Server. The data that a Genesys solution requires for operating in a particular environment, as well as the applications and the solutions, is represented as Configuration Database objects. Any person who needs access to this data or these applications must have an account in this database.

Logging In

At startup, every Genesys GUI application opens a Login dialog box for users to supply a User Name and Password, which are used for authentication. The authentication procedure succeeds only if a User with the specified User Name and Password is registered in the Configuration Database. Otherwise, the working session is stopped.

Last Logged In

Starting in release 8.0, you can configure Configuration Server so that some Genesys GUI applications display the date and time of the previous login for the currently logged-in user. Each user can then detect if someone else had accessed the system using their credentials.

Forced Re-Login for Inactivity

You can configure some Genesys GUIs to automatically force a logged-in user to log in again if he or she has not interacted with any element of the interface for a set period of time. In some interfaces, open windows are also minimized, and are restored only when the user logs back in. This functionality is configured in each interface, and is therefore specific to that interface. By default, this functionality is not active, and must be activated on an instance-by-instance basis for those GUI applications that are to use the feature.

> **Important**

> This inactivity feature survives reconnection timeouts. In other words, if the interface application becomes disconnected from Configuration Server after the forced re-login timeout has expired but before the user has logged in again, the user must still log in before he or she can access the system.

User Authorization

User authorization refers to ensuring that an authenticated user is entitled to access the system, either all or parts thereof, and defines what the user can do to or with the data that they can access.

The security mechanism implemented in Configuration Server allows the system administrator to define, for each valid user account, a level of access to sets of objects. The access privileges of valid user accounts define what the user can and cannot do within the corresponding set of objects.

Starting in release 8.0, an additional layer of security is available through Genesys Administrator, called Role-Based Access Control. This enables the system administrator (or a designated individual) to define access to objects based on what is to be done (viewed, modified, deleted) to the objects.

This section provides an overview of the various mechanisms in place to ensure data is accessed by only authorized users. For detailed information about how Genesys software implements user authorization, refer to the *Genesys Security Deployment Guide*.

Access Permissions

The level of access to sets of objects granted by the system administrator is defined by a combination of elementary permissions. Each user must be assigned at least one permission; without it, the user has no access to any data.

Access control for daemon applications is different from that for GUI applications. Access permissions for GUI applications are determined by the profile of the person who is currently logged in.

Access Groups

Access Groups are groups of Users who need to have the same set of permissions for Configuration Database objects. By adding individuals to Access Groups-and then setting permissions for those groups-access control is greatly simplified.

Genesys provides preconfigured default Access Groups. You can also create your own Access Groups to customize your own security environment.

Master Account and Super Administrators

The Configuration Database contains a predefined User object, otherwise known as the *Master Account* or *Default User*. The Default User, named `default` and with a password of `password`, is not associated with any Access Group. The Master Account always exists in the system and has a full set of permissions with respect to all objects in the Configuration Database. You must use this account when you log in to the Configuration Layer for the first time since the Configuration Database

initialization. Genesys recommends changing the default name and password of the Master Account, storing them securely, and using this account only for emergency purposes or whenever it is specifically required.

Changing Default Permissions

The default permissions that the Configuration Layer sets provide users with a broad range of access privileges. You can always change those default settings to match the access needs of a particular contact center environment.

> **Important**
>
> Genesys does not recommend changing the default access control setting unless absolutely necessary. Remember, the more complex the security system is, the more difficult it becomes to manage the data and the more it affects the performance of the Configuration Layer software.

Genesys provides two mechanisms to help you manage changes to your permissions-propagation and recursion. Refer to the *Genesys Security Deployment Guide* for details about these mechanisms and how to use them.

New Users

Configuration Server does not assign a new user to an Access Group when the user is created. In effect, the new user has no privileges, and cannot log in to any interface or use a daemon application. The new user must be explicitly added to appropriate Access Groups by an Administrator or by existing users with access rights to modify the user's account. Refer to *Genesys Administrator 8.1 Help* for more information about adding a user to an Access Group.

By default, this behavior applies to all new users added by Configuration Server release 7.6 or later. Users created before release 7.6 keep their existing set of permissions and Access Group assignments. If you want new users to be added automatically to pre-defined Access Groups, as was the behavior prior to release 7.6, you must manually disable this feature by using the Configuration Server configuration option **no-default-access**.

For more information about this feature, including how it works and how to modify it, refer to the *Genesys Security Deployment Guide*.

Login Security Banner

You can create your own security banner to be displayed to a user logging in to Genesys Administrator. You define the content of the banner, typically the terms of use of the application. Users must accept the terms to proceed, or they can reject the terms to close the application without access.

The user-defined security banner is specified during the installation of each instance of a GUI application, such as Genesys Administrator.

Refer to the *Genesys Security Deployment Guide* for more details about the security banner.

Genesys Security Using the TLS Protocol

Genesys supports the optional use of the Transport Layer Security (TLS) protocol to secure data transfer between its components. TLS is supported on Windows and UNIX platforms.

To enable secure data transfer between Genesys components that support this functionality, you must configure additional parameters in the Host objects and Application objects that represent these components. Certificates and corresponding private keys are generated using standard Public Key Infrastructure (PKI) tools, such as OpenSSL and Windows Certification services.

For detailed information about Genesys Security Using the TLS Protocol, refer to the *Genesys Security Deployment Guide*.

Multiple Ports

To provide flexibility in configuring a system with the Genesys Security using the TLS Protocol feature, you can configure multiple ports on a given server with either secure or unsecured connections. You specify the additional ports in the **Server Info** section on the **Configuration** tab of the server's Application object.

Each port can have one of the following listening modes:

- unsecured—The port is not secured by TLS. This is the default status of a port.
- secured—The port is secured by TLS.
- auto-detect—This status applies only to ports on the Configuration Server, and is used only when configuring secure connections to the Configuration Server. If an application that is trying to connect to an auto-detect port has security settings specified in its configuration, Configuration Server checks the validity of those settings. Depending on the results, the client will be connected in secure or unsecured mode.

Refer to the *Genesys Security Deployment Guide* for more information about multiple ports.

Multiple Ports on Configuration Server

When you install Configuration Server, the listening port that you specify during installation is stored in the configuration file as the **port** option. When Configuration Server first starts with an initialized database, it reads the **port** option in the configuration file. The value of the **port** option is also propagated to the Configuration Database, where it is stored as part of the Configuration Server Application object. As additional ports are configured, they are also stored in the Configuration Database as part of the Configuration Server Application object. On subsequent startups of Configuration Server—that is, on all startups after the first—Configuration Server reads the port information from the Configuration Server Application object, ignoring the **port** option in the configuration file.

If necessary, you can specify an additional unsecured listening port in the Configuration Server command line during subsequent startups. This additional port is not written to the Configuration Server Application object, and does not survive a restart of Configuration Server. Use this option only when regular ports cannot be opened. See **-cfglib_port** for more information about this option.

Dedicated Ports for Client Connections

Starting in release 8.5.1, you can configure separate ports on Configuration Server or Configuration Server Proxy that are restricted for use only by client User Interface type (UI) applications. All other applications would continue to use the assigned listening ports as usual. A firewall is used to direct these applications to the dedicated port, where they are authorized before being allowed access. For more information and instructions, see Configuring a Dedicated Port for Client UI Applications later in this Guide.

The same principle applies in an HA Configuration Server configuration. Configuration Server Proxy has a dedicated port to which the firewall directs the UI applications, while other applications connect through other ports on the proxy server. For instructions on configuring this dedicated port, see Configuring a Dedicated Port for Client UI Applications.

Secure Connections

In addition to configuring secure ports on your server applications, you must configure your client applications, both server and user interface types, to connect to these ports. Use Genesys Administrator to configure these connections.

There are only two exceptions to this standard procedure, as follows:

- Configuring secure connections to the Configuration Server—You must configure a Configuration Server port as an auto-detect port.
- Configuring a secure connection between DB Server and Configuration Server—You must configure the secure connection in the configuration files of the two components.

Refer to the *Genesys Security Deployment Guide* for detailed instructions for configuring secure connections.

European Data Protection Directive Disclaimer

The Genesys suite of products is designed to make up part of a fully functioning contact center solution, which may include certain non-Genesys components and customer systems. Genesys products are intended to provide customers with reasonable flexibility in designing their own contact center solutions. As such, it is possible for a customer to use the Genesys suite of products in a manner that complies with the European Data Protection Directive (EDPD). However, the Genesys products are merely tools to be used by the customer and cannot ensure or enforce compliance with the EDPD. It is solely the customer's responsibility to ensure that any use of the Genesys suite of products complies with the EDPD. Genesys recommends that the customer take steps to ensure compliance with the EDPD as well as any other applicable local security requirements.