Genesys Security Deployment Guide

Security Banner at Login

12/17/2025

Security Banner at Login

Contents

The security banner is a separate window that is displayed to a user when logging in to an application. The content of this window is defined by the system administrator, and can include such items as Terms of Use of the application or some kind of disclaimer. One security banner can be used by more than one application, and different applications can use different security banners.

The security banner can be enabled and configured in one of two ways:

- During application setup
- Before or after installation of the application, by creating specific registry entries in the application's host registry

The security banner can be configured differently for each application, to support a variety of corporate policies.

Security Benefits

The security banner does not actually provide true physical or virtual protection for your system. However, it can provide legal protection if an unauthorized user violates any access restrictions, such as Terms of Use, and accesses the system anyway.

Under the strictest configuration of the security banner, a user is not allowed to log in to an application without first accepting the contents of the banner. The various degrees of security depend on the options selected during installation.

Supporting Components

The following components support the implementation of the security banner as described in this chapter:

- Configuration Wizards
- Genesys Administrator
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager
- CCPulse+

Similar functionality can be achieved using customization features in the following components:

- Workspace Desktop Edition (formerly known as Interaction Workspace)
- Performance Management Advisors

For more information, refer to component-specific documentation.

Genesys Composer

Genesys Composer supports the basic concept of specifying and displaying a security banner. However, it implements a security banner differently than described in this document. Refer to Genesys Composer documentation for more information.

Genesys Desktop

Genesys Desktop supports the security banner in concept, but implements it differently from the way described in this document. In addition to a different installation procedure, all URLs related to the security banner must be in HTTP format (**http://**). Refer to the *Genesys Desktop 7.6 Deployment Guide* for more information.

Feature Description

The security banner is intended to display a user-defined security message prior to the login to a Genesys application, and provide the user with the means to confirm acceptance of the message. The message content is specified as an arbitrary URL, pointing to a document that can be displayed as an active document by Microsoft Internet Explorer 4.0 or later. Multiple URLs can be configured for redundancy.

The following characteristics of the security banner are configurable by the user, and can be configured differently for each application:

- Regularity with which the security banner is displayed. For example, it can be displayed only once for each user, only once for each user for each type of application, or for all logins.
- Whether the security banner is to be displayed, or if user acknowledgement is required.
- Behavior if the target URL of the security banner is not available.
- Title and dimensions of the security banner window.
- The timeout within which the security banner must be loaded and displayed on the screen. If this timeout expires, an intermediate message (**Downloading terms of use... Please wait...**) is displayed while the security banner loads.

By default, the security banner window contains user-defined text, two buttons (**Accept** and **Reject**) and a check box (**I Accept. Do not show this again**). The user logging in to the application must click **Accept** to proceed to the login dialog box. If the user clicks **Reject** or closes the security banner window without accepting the window contents, the application closes.

As previously described, an intermediate message (**Downloading terms of use... Please wait...**) is displayed whenever the security banner is not retrieved and displayed before the timeout expires. During this time, the user can close the window by clicking **Cancel**; the terms can only be accepted when the content is fully displayed.

You must also specify whether you allow a user to log in to the application if the security banner cannot be displayed; if you do not allow it, the application closes if the security banner cannot be displayed.

If the security banner cannot be retrieved at all, an error message is displayed. Error messages contain an **Exit** button instead of **Accept** and **Reject** buttons. The software includes a default error page, but you can also configure your own. The behavior of the error page depends on whether you have chosen to allow a user to log in to the application if the security banner is not displayed, as follows:

- If you have chosen to allow the user to log in, the error page closes automatically (if it is open) and the login dialog box appears. The user can then log in to the application.
- If you have chosen not to allow the user to log in, the error page included with the software is displayed, showing the error code. The login dialog box is not displayed, and the user cannot log in. For HTTP errors, refer to the HTTP specification. For system errors, refer to Microsoft technical documentation.

> Warning
>
> Genesys recommends that you use multiple redundant URLs, including a local file as appropriate, to minimize the risk that the security banner will not load.

Deploying the Security Banner for Multiple Applications on the Same Host

If, on a single host, you are installing two or more applications that support and will be using a security banner, you can choose to do one of the following:

- Provide individual settings for each type of application.
  In this case, if you choose to configure the security banner for just one (for this) application, all other applications will be deemed to have the security banner disabled. If you want any other applications to use a banner, you must enable and configure it for each of those other applications. In subsequent application installations, you can chose the for all option, but this will only set default values for subsequent installations; it will not impact the values for previous installations.
- Configure one security banner for all applications.
  In this case, the security banners for all applications on this host will have the same content and behavior. In effect, these settings become the default settings. You do not have to enable and configure the security banner for each application. Having done this, for each application with security banner that you subsequently install, you can choose to do one of the following:
  - Provide individual settings for this application only, while not impacting the default settings.
  -
  - Override the default settings by choosing to configure the security banner for all applications, and modifying the settings as required. The default values will appear in the installation interface, and can be overwritten or kept as is. If you change any of these values, all applications that use the default values, both those installed previously and subsequently, will be impacted.

In general, when setting up an application, the setup program looks first for a security banner configuration specific to this application. If one is not found, it then looks for a configuration common to all applications. In either case, it inherits the security banner attributes already defined. If it is unable to find any security banner configuration, it defaults to a disabled security banner, and you must then enable and configure the security banner from the beginning.

Feature Deployment

> **Important**
> To determine if this section applies to your component, see Supporting Components.

Deployment of the security banner consists of three steps:

1. Design and create the required security banners and optional customized error pages, using the editor of your choice.
2. Deploy security banner documents as files or as web content, and record the URLs. Each URL must be able to be resolved by the installed Microsoft Internet Explorer (IE) and displayed as an active page within the IE window.
3. Configure the URLs in one of the following ways:

As directed during installation of the GUI application **[+] Show steps**

The installation and configuration of the security banner is part of the application installation procedure for the following applications:

- Configuration Wizards
- Genesys Administrator
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

The security banner can also be installed after the application has been installed.

Refer to documentation for your application for detailed instructions about installing the application. Use the following procedure only if you select the **Enable Security Banner** option when installing the application.

Prerequisites

- You are installing one of the supporting components listed above, and have reached the **Security Banner Configuration** page of the installation wizard.
- You have created, and have the URLs of, the security banner and any custom error pages that will be used.

Start of procedure

1. On the **Security Banner Configuration** page of the installation wizard for the application that you are installing:
   a. In the **Select Security Banner behavior and configuration** section, select whether you want the security banner that you are about to define to be used by all applications that support the security banner feature, or just by applications of this type.
   b. Click **Next**.

2. On the **Security Banner Parameters** page, specify the parameters for the security banner as follows:

   a. Select how the security banner is displayed to the user the next time an application of this type is started:

      - **Until each user chooses to turn it off**—The security banner includes an **I Accept. Do not show this again.** check box that, by default, is not selected. If the user selects this option and clicks **Accept**, the security banner will not be displayed again to that user, regardless of the application that the user is starting. Each Windows user account must explicitly select this option and click **Accept** to disable the security banner for all applications.
      - **Until each user chooses to turn it off once for each application type**—The security banner includes an **I Accept. Do not show this again.** check box that, by default, is not selected. If the user selects this option and clicks **Accept**, the security banner will not be displayed again to that user when starting any application of this type. However, each time the user starts another type of application for which the security banner is active, the security banner will be displayed. Each Windows user account must explicitly select this option and click **Accept** to disable the security banner for this type of application.
      - **Every time the application starts**—The security banner does not include an **I Accept. Do not show this again.** check box. The security banner is displayed to every user every time any Genesys application is started.

      > Important
      >
      > If you select **Until each user chooses to turn it off** or **Until each user chooses to turn it off once for each application type**, and the user logging in selects **I Accept. Do not show this again.** in the security banner window, this setting will apply for all subsequent installations of the one or multiple applications. It (the **AckMandatory** registry variable) must manually be removed or reset to zero (**0**) in the registry by an authorized person.

   b. Select how to proceed if the security banner message at the specified URL cannot be displayed:

      - **Proceed to login without banner**—The user can log in to the application anyway.
      - **Exit, no login dialog box is displayed**—The user is not permitted to log in.

      > Warning
      >
      > Selecting the **Exit, no login dialog box is displayed** option effectively disables access to the application when the document specified by the URL cannot be retrieved or rendered for any reason.

   c. (Optional) Specify the title that appears in the title bar of the security banner window. If you do not specify a title, the window title is derived from the following:

      - If the security banner is an HTML file, the **<title>** element.
      - If the security banner is an HTML file but has no **<title>** element, the URL address.

- If the security banner is not an HTML file, the URL address.

In all cases, the application name follows the title in the title bar.

> **Important**
>
> If rebranding resources are present, the corresponding rebranding resource overrides this entry.

d. Specify the timeout, in milliseconds, within which the security banner must be displayed. The default is 3000. If the entire document is not available for display within this time, an intermediate message, **Downloading terms of use ... Please wait ...,** is displayed until the security banner itself can be displayed.

e. Specify the height and width, in pixels, of the security banner window, intermediate window, and any error window, if defined. The default values are 180 and 360 pixels, respectively. If neither of these values is specified (the default), the window is sized to fit the complete content of the document at the specified URL. At no time does the window exceed the work area of the screen. The document retains its size between logins, and once displayed, can be resized using standard IE tools.

> **Important**
>
> If the exact screen size for the security banner documents cannot be determined or estimated, Genesys recommends that the height and width parameters be specified.

f. Click **Next**.

3. On the **Security Banner Documents** page, for each document containing text that will be displayed in the security banner, specify the URL of the document and click **Add**. When you have added all the URLs, click **Next**.
   If this URL is not specified, all of the other options are ignored, and:
   - If an older security banner bitmap is configured, it is displayed.
   - Otherwise, no security banner is displayed.
4. On the **Security Banner Error Documents** page, do one of the following:
   - If you selected **Proceed to login without banner**, click **Next**. Do not enter any URLs on this page.
   - Otherwise, specify the URL of an error document—either the default error page or one that you specifically created—and click **Add**. When you have added all the URLs, click **Next**.

End of procedure

Next Steps

- Finish installing your application, as required. Refer to product-specific documentation for detailed instructions.

By modifying registry entries directly. **[+] Show steps**

Warning

Editing a registry incorrectly can cause serious, system-wide problems, and correcting them might require you to reinstall your operating system. Genesys cannot guarantee that any problems resulting from editing the registry can be solved. Edit your registry at your own risk. If you do decide to edit the registry, Genesys strongly recommends that you back up the registry file before editing it.

The Security Banner feature and URLs are defined in the registry of the application's host. Only someone with Write access (the Change permission) to the **HKEY_LOCAL_MACHINE** registry key—normally the system administrator—can set up and maintain the security banner.

This authorized person should:

- Specify the target URLs of the security banners and any customized error pages.
- Customize the windows as required.
- Subsequently modify the behavior as required, by changing the listed registry entries. This can be done either locally or remotely.

Configuring Security Banner Functionality

Configure the security banner functionality by using the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner

The values in this key specify the default behavior for all applications. Each entry can be redefined for specific applications in the subkeys, as follows:

HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\<CfgAppType>

where **<CfgAppType>** is the numeric value of the application type, as defined in the following table.

CfgAppType	Application
13	Outbound Contact Manager
19	Configuration Manager Wizard Manager
44	Solution Control Interface
51	Interaction Routing Designer
165	Genesys Administrator

For example, to specify values specific to Genesys Administrator, which has application type 165, define the registry subkey as follows:

HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\165

When selecting the security banner to display and use, the library first looks for a corresponding subkey, and then uses the default key if the subkey does not exist.

String entries can be entered as STRING or EXPANDABLE_STRING registry values. If they are entered as EXPANDABLE_STRING, environment variable strings enclosed in percent signs (%) are replaced with their values defined by the environment variables (located in **%HOMEDRIVE%%HOMEPATH%\default.htm**). Integer entries can be entered either as DWORD or STRING registry values, representing decimal numbers.

Configuring URLs

The URLs for the security banner and any associated error pages are configured in the following registry keys:

- For all applications: **HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\<seq_number>**
- For specific applications: **HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\<CgfAppType>\<seq_number>**

where **<seq_number>** is the sequence number for multiple URLs. Multiple URLs are tried in the order of their sequence number.

The URLs are specified by the registry options Error Page and URL.

Example

The following sample registry entries:

```
KEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\1\URL=http://MyServer1/
Banner.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\2\URL=http://MyServer2/
Banner.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\
URL=%SystemRoot%AdminContacts.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\ErrorPage=1
```

specify the following behavior:

The dialog attempts to retrieve **Banner.htm** from **MyServer1**. If it cannot retrieve that file, the dialog attempts to retrieve **Banner.htm** from . If it cannot retrieve that file, the dialog attempts to retrieve the custom error page located in the **system32** directory. And if that page cannot be retrieved, the default error page is displayed.

Security Banner Registry Entries

This section describes the registry options used to specify and customize the appearance and behavior of the security banner. These options are intended only for advanced users with registry access.

> **Important**
>
> Unless otherwise noted, the registry entries in this section are equivalent to the options presented when installing the security banner during application setup.

AckMandatory
Default Value: **0**
Valid Values: One of the following:

0	Proceed with the login, without acknowledgement of the contents of the security banner. The login dialog box is displayed.
1	Exit the application. The login dialog box is

	not displayed.

Changes Take Effect: After the application restarts

Specifies whether login to the application will be allowed if the document specified in the URL cannot be displayed for any reason.

> ## Warning
> Setting this option to **1** effectively disables access to the application when the document specified by the URL cannot be retrieved or rendered for any reason.

AckMode
Default Value: **0**
Valid Values: One of the following:

0	User can choose to hide the security banner for all subsequent logins, for all applications.
1	User can choose to hide the security banner for all subsequent logins to the current application only.
2	User cannot choose to hide the security banner; user must accept content of the banner whenever logging in to any application.

Changes Take Effect: After the application restarts

Specifies whether the user is presented with the option to hide the security banner, and therefore does not need to accept the security banner content, the next time an application is launched.

If this option is set to **0** or **1**, the **I Accept. Do not show this again.** check box appears in the security banner window. If the user selects this check box, they will not see the security banner at subsequent attempts to access either this (**0** or **1**) or any application (**1**) for which the security banner is configured.

> ## Important
> If option **0** or **1** is selected, the only way to have the security banner displayed again when logging in to this (**0** or **1**) or any application (**1**) is to manually remove this entry from the registry. This registry entry and its value is persistent across installations—it is not removed when uninstalling the application, nor is it cleared or reset when reinstalling the application.

If this option is set to **2**, the **I Acknowledge. Don't show this again.** check box does not appear in the security banner window, and the security banner is displayed every time anyone tries to access the application.

ErrorPage
Default Value: **0**
Valid Values:

0	The security banner is displayed.
1	An error page is displayed.

Changes Take Effect: After the application restarts

Required if you are using a custom error page. Specifies that the URL points to an error page or the security banner. If the error page is displayed, the window displays the **Exit** button in place of the **Accept** and **Reject** buttons. Use this setting to substitute the default error page with a customized error page.

Height
Default Value: No default value
Valid Values: Any positive integer greater than **180**
Changes Take Effect: After the application restarts

Width
Default Value: No default value
Valid Values: Any positive integer greater than **359**
Changes Take Effect: After the application restarts

Optional; these two options specify the dimensions (in pixels) of the document area of the security banner and error page window. If neither of these values is specified (the default), the window is sized to fit the complete content of the document specified by the URL. At no time does the window exceed the work area of the screen. The document retains its size between logins, and once displayed, can be resized using standard IE tools.

> ### Important
>
> If the exact screen size for the security banner documents cannot be determined or estimated, Genesys recommends that the height and width parameters be specified.

NoCompleteTimeout
Default Value: **2000**
Valid Values: Any non-negative integer
Changes Take Effect: After the application restarts

Specifies the timeout (in milliseconds) for receiving download progress or status notifications from the WebBrowser control. To download and render the document, the security banner dialog uses components of IE in the form of WebBrowser control. In some cases, for security reasons, the WebBrowser control does not provide the client with the means to detect navigation cancellation. This timeout is used to detect and properly process these cases.

The absence of progress or status notifications from the WebBrowser control for a period exceeding this timeout is considered a failure to retrieve the document. If this timeout expires, the attempt to retrieve the document specified by the current URL is aborted, and the dialog attempts to retrieve the next URL from the URLs list. If this happens with the last URL in the list, the System error **0x80004004: Operation aborted** error message is reported to the user.

If this option is set to zero (**0**), progress and status notifications are not used to detect download failure or cancellation.

> ### Important
>
> **NoCompleteTimeout** is intended only for advanced users with access to the registry. It has no equivalent option in the process of installing the security banner during application setup, and its default value is considered adequate in these situations.

ShowUpTimeout
Default Value: **3000**
Valid Values: Any non-negative integer
Changes Take Effect: After the application restarts

Specifies the timeout (in milliseconds) within which the security banner window attempts to load the document specified by the URL. If the timeout expires before the content is displayed, an intermediate window (**Downloading terms of use... Please wait...**) is displayed. During this time, the user can close the window by clicking **Cancel**; the terms can only be accepted when the content is fully displayed.

If the document cannot be retrieved, the behavior of the window depends on the value of AckMandatory, as follows:

- If **AckMandatory=0**, the window closes automatically (if it is open), and the login dialog box appears. The user can then log in to the application.
- If **AckMandatory=1**, the error page included with the software is displayed, showing the error code. For HTTP errors, refer to the HTTP specification. For system errors, refer to Microsoft technical documentation. The login dialog box is not displayed, so the user cannot log in.

Title
Default Value: No default value
Valid Values: Any string, or blank
Changes Take Effect: After the application restarts

Optional; specifies the title that appears in the title bar of the security banner window. If no value is specified for this option, the title is derived from the following:

- If the security banner is an HTML file, the **<title>** element.
- If the security banner is an HTML file but has no **<title>** element, the URL address.
- If the security banner is not an HTML file, the URL address.

In all cases, the application name follows the title in the title bar.

> Important
>
> Note: If rebranding resources are present, the corresponding rebranding resource overrides this entry.

URL
Default Value: No default value, for backward compatibility
Valid Values: A URL address that can be resolved by the installed IE application and displayed as an active page within the IE window
Changes Take Effect: After the application restarts

Required; specifies the URL of the document displayed in the security banner window. If this value is not specified, all other options are ignored, and:

- If an old security banner bitmap is configured, it is displayed.
- Otherwise, no security banner is displayed.

> Important
>
> If you uninstall an application for which the security banner was configured, the configuration parameters of its security banner are not removed from the registry. To clear these parameters, you must reinstall the application without enabling the security banner.