Genesys Administrator Extension Deployment Guide

security Section

5/1/2025

security Section

Contents

This section must be called `security`, and is configured in the Genesys Administrator Extension Server Application object of type **Genesys Administrator Server**.

The options in this section relate to security features in Genesys Administrator Extension.

enable_un_cookie

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After restart

Specifies if the encrypted usernames are stored in the browser cookies. If set to `true`, GAX stores the encrypted username in browser cookies for a period of 30 days. If set to `false`, GAX does not store the username in the browser cookies and it also removes the existing username (un) cookies.

host_whitelist

Default Value: Empty
Valid Values: URLs of hosts trusted by this GAX instance, separated by semi-colons (`;`); for example `132.56.54.34;host1;34.32.12.8`
Changes Take Effect: After restart

Specifies the host URLs that can be whitelisted. This option only takes effect when **host_whitelist_enabled** is set to `true`.

host_whitelist_enabled

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After restart

Specifies if host whitelisting is enabled in GAX. If this option is not set or set to `false` (the default), then host whitelisting is disabled and all hosts are allowed by GAX.

If set to `true`, only those hosts specified in the option **host_whitelist** can appear as:

- values of the parameters **logout_success_url**, **logout_failure_url**, and **logout_url** when logging in remotely

- list of hosts from which to select **UNC Path to Mounted CD or Directory**, **UNC Path to an Existing Administrator Repository**, and **UNC Path to Zipped IPs** when uploading IPs.