



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Administrator Extension Deployment Guide

Configuring GAX Properties

Configuring GAX Properties

After GAX starts for the first time, it generates the following files and folders in the installation directory:

- `conf/gax.properties`
- `webapp`
- `logs`
- `jsp`

You can configure GAX by editing the `gax.properties` file. The options specified in the `gax.properties` file are used by GAX before it connects to Configuration Server. To set additional configuration options, see [Configuration Options](#).

Tip

Read more general information about Java-based *.properties* files [here](#).

The following options can be configured:

Option	Description	Possible Values	Default Value
<code>accesslog_enabled</code>	Enables HTTP access logging	true, false	true
<code>accesslog_filename</code>	File name for the HTTP access log	Valid filename	<code>./logs/http-yyyy_mm_dd.log</code>
<code>accesslog_timezone</code>	Time zone for the HTTP access log	Any valid timezone code (see Time Zones for a list). Note: It is recommended to specify the time zone value in canonical format instead of three-letter time zone IDs. For example, Australia/Sydney, Asia/Kolkata, America/Los_Angeles, and so on.	GMT
<code>accesslog_append</code>	After GAX is restarted, specifies whether to append to existing HTTP access log	true, false	true
<code>accesslog_extended</code>	Specifies whether to include extended	true, false	false

Option	Description	Possible Values	Default Value
	information in the HTTP access log		
accesslog_cookies	Specifies whether to include cookies in the HTTP access log	true, false	false
accesslog_retaindays	Specifies number of days to retain the HTTP access log	integer	90
app	Specifies the GAX Application object	Existing Application object name	
backup_port	Specifies the backup Configuration Server Port	integer	
backup_host	Specifies the backup Configuration Server Host, written as a Fully Qualified Domain Name (FQDN) or IP address	Valid FQDN or IP address	
cache_control	Enables Cache-Control in the response header.	Any valid value accepted by Cache-Control HTTP header	no-cache, no-store, must-revalidate
disable_xframe_options	When its set to true in the gax.properties file, the response header will not have X-Frame-Options, and the GAX login page will load properly in new tab from other Genesys applications, such as Workspace Web Edition.	true, false	false
enable_web_notification	Enables real-time notification if the configuration object currently being modified has been updated by another user while the current user was modifying it; that is, since the object's properties window was opened. See Coordinating Simultaneous Changes to Data . Note: This feature is currently supported only in the Configuration	true, false	false

Option	Description	Possible Values	Default Value
	Manager view.		
host	Specifies the primary Configuration Server Host, written as a Fully Qualified Domain Name (FQDN) or IP address	Valid FQDN or IP address	
http_port	Defines the HTTP port	integer	8080
https_port	Defines the HTTPS port	integer	8443
input_deny_list	Enables configuration of patterns for input validation.	Space separated regex patterns. You can add more strings in space separated format. The following example has three strings: <code>.alert\(. (?i)img[\s<].?src\s?=. * .script</code>	
invalidate_session_on_login	Specifies whether GAX regenerates JSESSIONID immediately after user login and logout.	true, false	false
keystore_path	Specifies the keystore path.	Valid path, for example: Windows: <code>C:\OpenSSL-Win32\bin\keystore</code> Linux: <code>/opt/genesys/gax/conf/keystore</code>	
keystore_password	Specifies the keystore password	Note: The password is encrypted and must not be modified directly. Instead, refer to Step 4 of Setting up HTTPS for use with Genesys Administrator Extension .	
max_cfg_connection	Specifies the maximum number of connections to allow from GAX to Configuration Server. To allow unlimited connections, set the value to -1.	-1 or any positive integer	200
max_idle_time	Specifies the maximum idle time,	integer	1000*60*60

Option	Description	Possible Values	Default Value
	in milliseconds, for HTTP connection.		
port	Specifies the primary Configuration Server Port	integer	
root_url	Specifies the root URL (host:port/rootURL)		/gax
session_httponly	Specifies whether the HTTPOnly flag is set automatically on session cookie JSESSIONID.	true, false	true
session_securecookies	Specifies whether the secure flag is set automatically on session cookie JSESSIONID.	true, false	true
supported_protocol	Defines the protocol to use when communicating with the server	http/https/both	http
saml	Enables SSO login to GAX using SAML	true, false	false
saml_entityid	Specifies entity ID used by GAX metadata	Any value	
saml_external_userid	Defines the protocol to correlate to the External User ID in Genesys Person object. GAX must extract DSID from SAML assertion and query the user by using the external ID, then use the username to enable the user to log in.	Valid SAML attribute (DSID) value	
saml_idp_metadata	Specifies the path or URL of the IDP's metadata XML file	Valid path (or) URL	
saml_jksfilelocation	Specifies the location or path of custom JKS Keystore.	Valid path	
saml_jkspassword	Defines the custom JKS Keystore's password.	Any value (password entered during key store generation)	
saml_landingpage	Logout URL to redirect when users log out of SSO GAX.	URL	

Option	Description	Possible Values	Default Value
saml_signingkeyname	Defines the signing key name (alias provided during custom key store generation)	Any value (alias name given during key store generation)	
saml_signingkeypassword	Defines the signing key password	Any value (key password entered during key store generation)	