Configurations Options Reference Manual

[security-authentication-rules] Section

5/8/2025

Contents

[security-authentication-rules] Section

This section contains configuration options for defining custom properties of user passwords and setting up and using passwords. The options in this section are configured at either the tenant level or the user level. Refer to the User Passwords chapter in the *Genesys Security Deployment Guide* for complete information about these options.

This section must be called **security-authentication-rules**.

Tenant-level Options

The following options are configured in the [**security-authentication-rules**] section in the annex of the Tenant object, as follows:

- `Tenant` object > `Options` tab > `Advanced View (Annex)`

account-expiration

Default Value: `0`
Valid Values: `0` to 365
Changes Take Effect: Rule validation occurs the next time an account belonging to this Tenant tries to log in or authenticate, or when a User object belonging to this Tenant is retrieved or changed

Specifies the maximum number of days for which an account can remain idle. After this time interval, the account will be considered expired and the user will not be able to log in until the account has been reactivated by the system administrator. Configuration Server checks for expired accounts when an account belonging to this Tenant tries to log in or authenticate, or when a User object belonging to this Tenant is retrieved or changed.

> **Important**
> Account expiration functionality does not work correctly if the Last Login feature is not configured. That is, the master Configuration Server and all Configuration Server Proxies must have the **last-login** and **last-login-synchronization** options both set to `true`. Calculations for the expiration of a particular account starts after the first login is recorded as a part of the Last Login feature; if the last login is not available, account expiration does not apply.

If set to `0` (the default), there is no expiration of idle accounts for any user.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

> **Important**
>
> - This option does not apply to the `Default` account, which does not expire.
> - This option does not apply to accounts that are externally authenticated if an external authentication Domain was configured.
> - This option can be overridden for individual users using the **override-account-expiration** option.

account-lockout-attempts-period

Default Value: `0`
Valid Values: `0–20`
Takes Effect: At the next occurrence of an unsuccessful login attempt

Specifies the length of time (in minutes) since the last unsuccessful login attempt in which another unsuccessful attempt will be counted toward the lockout threshold specified by **account-lockout-threshold**. If another unsuccessful attempt is recorded before this time interval expires, the time of this latest attempt becomes the basis from which this time period is calculated. In effect, this period is a sliding window.

If no additional unsuccessful attempts occur within this time period, the number of unsuccessful attempts is cleared, and previous attempts are not counted towards the lockout threshold.

This time period applies to all user accounts belonging to this Tenant unless overridden at the User level by the **account-override-lockout** option.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

account-lockout-duration

Default Value: `30`
Valid Values: `0–1440`
Takes Effect: Next time an account is locked out

Specifies the length of time (in minutes) that the lockout lasts after the lockout condition has been met.

Accounts already locked when this option is changed are released after the time specified by this option elapses, regardless of how long they were locked out originally.

This lockout duration applies to all user accounts belonging to this Tenant unless overridden at the User level by the **account-override-lockout** option.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

account-lockout-mode

Default Value: `0`
Valid Values: `0`, `1`
Takes Effect: Next time an account is locked out

Specifies whether an account will remain locked (after a user repeatedly enters incorrect authentication credentials) until the administrator unlocks it manually.

- If set to `1`, the **account-lockout-duration** option is ignored and the account remains locked until an administrator unlocks it.
- If set to `0` (the default), the account remains locked out for the time period configured using the **account-lockout-duration** option.

The administrator can unlock an account using any of the following methods:

- Changing the password for the user.
- Enabling force password reset for the user.
- Setting the **account-override-lockout** option to true at User-level, which overrides the account lockout for that user.

account-lockout-threshold

Default Value: `0`
Valid Values: `0` to `8`
Takes Effect: At next attempt to log in

Specifies the number of consecutive unsuccessful login attempts that a user account can make before being locked out. When set to the `0` (the default), no lockout will occur. This threshold applies to all user accounts belonging to this Tenant unless overridden at the User level by the **account-override-lockout** option.

force-password-reset

Default Value: `false`
Valid Values: `false`, `true`
Takes Effect: Immediately

Specifies whether all applications must prompt all of their users to change their passwords at first login. If set to true, all users for whom password reset is enabled (**Reset password** is checked on the user **Configuration** tab) will be unable to login unless they reset their password the next time that they log in. Any exceptions to the policy of changing passwords at first login (down-level applications or applications for which the **no-change-password-at-first-login** option is set to `true`) will not be permitted.The user will not be able to log in until he or she uses the correct application or the administrator clears the **Reset password** checkbox on the corresponding User object's **Configuration** tab.

For example, you might want to use this option to ensure that there are no exceptions to the policy of changing passwords at first login.

max-account-sessions

Default Value: `0`
Valid Values: `0` to 128
Takes Effect: At next attempt to connect to Configuration Server.

Specifies the number of simultaneous connections that each account can have with a single instance of Configuration Server. If an account tries to exceed the number of connections, login is denied.

In configurations with multiple Tenants, if this option is missing from the Tenant in which the account is logging in, the value set in the Parent up to the inheritance node for this Tenant applies. See Passwords in Configurations with Multiple Tenants for more information.

If this option is set to `0` (the default), there are no limits.

This option can be overridden for individual users by setting this option, with the same valid values, in the annex of the particular User object.

> **Important**
>
> Sessions restored and authenticated through existing sessions are not included in the count of sessions for this option.

object-deletion-rate

Default Value: `0`
Valid Values: Any positive integer
Takes Effect: Immediately

Specifies the maximum number of objects that a user can delete within the interval configured in the **object-deletion-rate-interval** option.

When a user tries to delete beyond the configured limit, then Configuration Server rejects the request and generates a corresponding error message.

When set to `0` (zero), this feature is disabled.

object-deletion-rate-interval

Default Value: `1440` minutes
Valid Values: Any positive integer
Takes Effect: Immediately

Specifies the maximum amount of time (in minutes) in which a user can delete the number of objects configured in the **object-deletion-rate** option. Once the specified time expires, this option is reset to `0` and the user can continue to delete the objects until the next timeout.

When set to `0` (zero), this feature is disabled.

password-expiration

Default Value: `0`
Valid Values: `0` to 365
Takes Effect: Immediately

Specifies the number of days from when the user password was created and after which the password is considered expired and cannot be used. If set to `0` (the default), the password will not expire.

This option does not apply to empty passwords, nor to the password for the default account that never expires.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

password-expiration-notify

Default Value: `0`
Valid Values: `0` to 364
Takes Effect: Immediately

Specifies the number of days before a user password expires that a notice will be displayed to the user warning that his or her password will expire. To take effect, the specified value must be less than the number of days left before the password expires. If set to `0` (the default), no notification is sent.

This option applies only if the **password-expiration** option is configured at the Tenant level.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

password-min-length

Default Value: No default value
Valid Values: `0` to 64
Takes Effect: Immediately

Optional. Specifies the minimum length (in characters) of a password used by all users in the Tenant in which the option is defined. If this option is present, it overrides the **allow-empty-password** option in Configuration Server or Configuration Server Proxy.

If this option is set to `0`, an empty password is permitted (regardless of the value of **allow-empty-password**). If this option is set to a value greater than the maximum allowed value (64), the maximum value is used.

> **Important**
>
> - This option applies only to passwords used with internal authentication, however during person object creation, the password criteria must match with configuration irrespective

of whether external or internal authentication is used. This is because if external authentication is disabled, then it must fall back to internal authentication.

- This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the minimum length requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
- Genesys recommends you use this option instead of the **allow-empty-password** option, which is provided only for purposes of backward compatibility.

password-no-repeats

Default: `0`
Valid Values: `0` to `30`
Changes Take Effect: At the next password creation or change

Specifies the number of password changes that must occur (that is, the number of old passwords) before a prior password can be reused. If set to `0` (the default), no history of used passwords is kept, and a password can be reused as desired.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

password-req-alpha

Default: `false`
Valid Values: `false`, `true`
Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one US-ASCII alphabetic character (a-z, A-Z). If set to true, and a password being created or changed does not contain one or more alphabetic characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

Important

- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
- This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the alphabetic requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.

password-req-mixed-case

Default: `false`
Valid Values: `false`, `true`
Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one uppercase character (A-Z) and one lowercase character (a-z) from the US-ASCII character set. If set to true, and a password is created or changed does not contain one or more uppercase characters and one or more lowercase characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

> **Important**
>
> - The password must contain at least one upper-case (A-Z) and one lower-case (a-z) ASCII character.
> - This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
> - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the mixed-case requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.

password-req-number

Default: `false`
Valid Values: `false`, `true`
Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one numeric character (0-9). If set to true, and a password being created or changed does not contain one or more numeric characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

> **Important**
>
> - This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
> - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the numeric the requirement is not rejected during

login; however, when the user tries to change one of these passwords, the new password will be subject to this option.

password-req-punctuation

Default: `false`
Valid Values: `false`, `true`
Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one punctuation character from the US-ASCII character set. If set to true, and a password being created or changed does not contain one or more punctuation characters, Configuration Server will not save the changes. The following punctuation characters are permitted:

- ! “ # $ % &’ ( ) * + , - . /
- : ; < = > ?
- [\ ] ^ _ `
- { | } ~

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See Passwords in Configurations with Multiple Tenants for more information.

Important

- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
- This option applies only to passwords that are set after this option has been configured. Existing valid passwords that do not meet the punctuation requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.

shortcut-add-restriction-count

Default: `0`
Valid Values:Any positive integer
Changes Take Effect: Immediately

The maximum number of objects that can be moved by a User per change object request. Also the maximum number of shortcuts that can be added into an object group by a user per change request.

When a user tries to move objects or add shortcuts beyond the configured limit, then Configuration Server rejects the request and generates a corresponding error message.

> **Important**
> If set to `0`, there is no restriction. Only if value >`0`, restriction is applied.

shortcut-remove-restriction-count

Default: `0`
Valid Values:Any positive integer
Changes Take Effect: Immediately

Specifies the maximum number of shortcut objects that a user can delete per change object request. When a user tries to delete beyond the configured limit, then Configuration Server rejects the request and generates a corresponding error message. When set to `0` (zero), this feature is disabled.

tenant-override-section

Default: `false`
Valid Values: `false`, `true`
Changes Take Effect: Immediately

Applies only in a configuration with multiple Tenants; specifies how Configuration Server interprets or applies values for options in the configuration option section **security-authentication-rules**, as follows:

- If this Tenant has values configured for one or more of these options, those values are applied. Values for the other options are assigned as described in the following two bullets, depending on the value of this option (**tenant-override-section**).
- If this Tenant has no values configured for any of these options, and this option (**tenant-override-section**) is either absent or set to `false`, values defined at the nearest ancestor Tenant are applied.
- If this Tenant has no values configured for any of these options, and this option (**tenant-override-section**) is set to `true`, default values are applied to all options. Values assigned in ancestor Tenants are ignored for this Tenant.

In effect, this option allows customization of these options for this Tenant and its child Tenants, if required, and applies to all options in the **[security-authentication-rules]** section in the same object.

User-level Options

These options are configured at the User-level. They either override settings made at the Tenant level or contain information about actions taken as a result of settings at the Tenant level or their overrides at the User level. Options in this section are configured in the **security-authentication-rules** section in the annex of the `User` object, as follows:

- `User` object > `Options` tab > `Advanced View (Annex)`

> **Important**
>
> The User configuration options described in this section are not a complete set of options available for a User. Refer to the documentation for Genesys applications that you are installing for additional User-level options that might be required.

account-override-lockout

Default Value: `false`
Valid Values: `false`, `true`
Takes Effect: At the next attempt to log in to any instance of Configuration Server

Specifies whether this user account can be locked out. If set to `true`, this user can override the lockout rules set at its Tenant level. A `true` value can also be used to unlock, or clear, a locked account if set before the **account-lockout-duration** option is set at the Tenant level. If set to `false` (the default), the lockout will expire as configured at the Tenant level.

last-expired-at

Specifies when the user account expired, for example:
`Sat Oct 13 12:42:52 2012`

This option is set automatically by Configuration Server or Configuration Server Proxy and appears in the annex of the User object. The value is read-only and is for reference purposes only.

last-locked-at

Specifies when the user account was locked by the instance of Configuration Server to which the client application, used to review Person object options, is currently connected. For example:
`09/12/09 10:445 PM @confserv`

This option is set automatically by Configuration Server or Configuration Server Proxy and appears in the annex of the User object. The value is read-only and is for reference purposes only.

override-account-expiration

Default Value: `0`
Valid Values:

`0`	Default. No override; the expiration value set at the Tenant level applies. Each time that this account tries to log in or authenticate or an attempt is made to read or change the User object, the idle time calculation restarts.
`1`	No check for account expiration is made when the user tries to log in or authenticate, or when the User object is retrieved; the value of the Tenant-level option account-expiration is ignored. If this

	account is marked as expired (**last-expired-at** is set to a valid date/time stamp), it is reactivated.
2	Check for idle time does not occur at the next login attempt. After the user has logged in successfully, idle time calculation restarts and the value of this option is reset to 0 (the default).

Takes Effect: At the next time the user tries to log in or authenticate, or an attempt is made to read or change the User object.

Specifies if account expiration, as defined by the Tenant-level option **account-expiration**, applies to a particular user account.

> **Important**
>
> - This option does not apply to the `Default` account, which does not expire.
> - This option does not apply to accounts that are externally authenticated.

override-shortcut-add-restriction

Default Value: `false`
Valid Values: `true`, `false`
Takes Effect: Immediately

Configuration object move restriction disabled if set as `true` on person Object.

> **Important**
>
> If set to `true`, then there is no restriction on object movement between folders or object groups. Also no restriction on the number of shortcuts that can be added to object group.

override-object-deletion-rate

Default Value: `false`
Valid Values: `false`, `true`
Takes Effect: Immediately

Specifies whether to restrict a user account from deleting the configuration objects. By default, this feature is enabled. If set to `true`, restriction to delete the configuration options is disabled.

If the password of the Person object is changed, this option is reset to the default value (`false`).

override-password-expiration

Default Value: `false`
Valid Values: `false`, `true`
Takes Effect: At the next attempt to log in or authenticate the user

Specifies whether a password of the user for which this option is configured can override the expiration policy specified at the Tenant level by the **password-expiration** option. If set to `true`, the user password for this user will not expire. If set to `false` (default), the user password will expire as configured at the Tenant level.

This option applies only if **password-expiration** is configured at the Tenant level.

override-shortcut-remove-restriction

Default Value: `false`
Valid Values: `false`, `true`
Takes Effect: Immediately

Specifies whether to restrict a user account from deleting the shortcuts from the object group. By default, this feature is enabled. If set to `true`, restriction to delete the group object shortcuts is disabled.