Configurations Options Reference Manual

[authentication] Section

5/5/2025

Contents

[authentication] Section

This section is mandatory on the Server level to enable external authentication and is optional to configure certain features common for all authentication types. It can, however, appear in other locations as mentioned in Setting Configuration Options.

This section must be called *authentication*. The following are the [authentication] section options, common for all authentication types:

- **library**
- **enforce-external-auth**
- **enforce-internal-auth**
- **failure-alarm-***

Some of these options may be configured in the **[authentication]** section at different levels:

- application (Configuration Server Application object)
- tenant (Tenant object)
- user (Person object)

Refer to External Authentication Reference Manual for the options specific to each external authentication type.

library

Default value: No default value
Valid values: Depends on type configuration option, as follows:

`gauth_radius`	All
`gauth_ldap`	All
`gauth_radius, gauth_ldap`	Configuration Server, Configuration Server Proxy
`gauth_ldap, gauth_radius`	Configuration Server, Configuration Server Proxy
`internal`	Tenant, Person

Changes Take Effect: Upon restart of the object for which this option is set

Lists enabled external authentication type(s). The name(s) of corresponding section(s) that specifies the parameters for each external authentication type must match these values. This option is mandatory to enable external authentication, and its value is set automatically during installation, based on the selected external authentication type.

You can deploy both RADIUS and LDAP on the same Configuration Server or Configuration Server Proxy. If this Configuration Server or Configuration Server Proxy was previously configured for another type of authentication, add `gauth_radius` or `gauth_ldap` to the value of this option, separated by comma. When set to internal, all users associated with the object in which the object is set to this

value are validated internally.

When set to `internal`, all users associated with the object in which the object is set to this value are validated internally.

enforce-external-auth

Default value: `false`
Valid values: `true`, `false`
Changes Take Effect: Immediately

Optional. Enforces external authentication for every user. If you omit this parameter, LDAP AM performs authentication only if an External ID is specified in the Person object.

This option applies at the server level, and starting in release 8.5.1, also at the Tenant level.

If this option is configured at the server level as `true` in the database, but Configuration Server reads its configuration file and finds the option set to `false`, the value from the configuration file will override the value in the database, allowing all users of the Environment tenant to log in internally.

> **Warning**
> Do not set this option to `true` until you have configured all of the accounts in the configuration.

enforce-internal-auth

Default value: `false`
Valid values: `true`, `false`
Changes Take Effect: Immediately

Optional. Specifies if all users are to be authenticated internally.

This option is set in the options of the Application object. If set to `true`, all users are authenticated internally by Configuration Server or Configuration Server Proxy, regardless of having a value in the External ID field. If set to `false` (the default), only those users with a value in the External ID field are authenticated by the LDAP AM.

failure-alarm-*

These options are applicable to the entire Configuration Server application and should be configured only in the Configuration Server Application object **[authentication]** section.

Configuration Server can keep track of recent user login/authentication failures to generate Standard level log message when the number/rate of failures exceeds specified threshold.

The following events (further denoted as `auth` events) are tracked:

- user logins with `gui-type` applications
- user authentications, requested by applications
- user owned password changes, which require old password

These events are tracked for all client protocols (`cfglib`, `soap`) and authentication types (`internal`, `external`, `delegated to master`).

The alarm criterion threshold can be defined as a maximum count and/or percentage of authentication failures during specified last time interval. If both count and percentage criteria are specified, the alarm log message is generated whenever any of the criterion is met. Once the message is generated, the failure counter is reset. If the condition persists, the message would be generated again, once the condition is detected, starting with the reset counter.

If specified condition is met, the following log message is generated:

```
24150|STANDARD|GCTI_CONFSERV_AUTH_FAILURE_ALARM|Multiple authentication failures: %u failures over last %u minute(s) exceed predefined threshold of %u%s
```

The message can be associated with alarm condition/reaction using existing Management Layer alarming functionality.

The alarm can serve as an indication of:

- authentication subsystem failures/misconfiguration
- specific type of intrusion attempts

The feature is configured in the **[authentication]** section of the Configuration Server Application configuration object.

- **failure-alarm-period** – enables the feature and specifies time interval used to detect repeated auth failures
- **failure-alarm-count** – specifies the count criterion
- **failure-alarm-percent** and **failure-alarm-percent-threshold** – specify the percentage criterion. This is the percentage of failures to all auth attempts. failure-alarm-percent takes effect only if the total number of attempts exceeds failure-alarm-percent-threshold.

failure-alarm-period

Default value: `0`
Valid values:

`0`	Disables the failure tracking.
`positive integer`	Specifies the time interval in minutes.

Changes take effect: Immediately

Enables alarm for repeated auth failures and specifies time interval, used for detection criteria.

failure-alarm-count

Default value: `0`
Valid values:

`0`	Disables count criterion.
`positive integer`	Specifies the threshold count.

Changes take effect: Immediately

For repeated authentication failures, alarm specifies the threshold count of failures. If the number of failures during last failure-alarm-period exceeds this value, the alarm log message is logged. The corresponding alarm, if configured, is triggered.

failure-alarm-percent

Default value: `0`
Valid values:

`0`	Disables count criterion.
`1-100`	Specifies the percentage in %.

Changes take effect: Immediately

For repeated authentication failures, alarm specifies the threshold percentage of failures. If the percentage of failures (the ratio of the number of failures to the number of attempts) exceeds this value, the alarm log message is logged. The corresponding alarm, if configured, is triggered. This option is effective only if the total number of attempts during the last failure-alarm-period exceeds the failure-alarm-percent-threshold.

failure-alarm-percent-threshold

Default value: `10`
Valid values:
non-negative integer - specifies the threshold count
Changes take effect: Immediately

For repeated authentication failures, alarm specifies the total number of authentication attempts during the last failure-alarm-period at which the failure-alarm-percent starts to take effect.