Configurations Options Reference Manual

Configuration Server Section

5/3/2025

Contents

Configuration Server Section

This section contains the configuration options of Configuration Server. The name of the section depends on the name of the Configuration Server `Application` object. On the first Configuration Server (named **confserv**), this section is named **confserv**. On other Configuration Servers being installed, this section has the same name as the Configuration Server object.

allow-empty-password

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

Specifies whether Configuration Server allows an empty (blank) password in a client connection request. If the option is set to `false` and the password in a request is not specified, Configuration Server rejects the request and generates a corresponding error message.

> ### Important
> The Tenant option **password-min-length** overrides the value of **allow-empty-password** for all users in the Tenant in which the latter option is configured. Genesys strongly recommends that you use **password-min-length** instead of **allow-empty-password**. The latter has been provided only for purposes of backward compatibility.

Refer to the User Passwords section of the *Genesys Security Deployment Guide* for more information about this option and how to use it.

allow-external-empty-password

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

This option is used only if external authentication is being used.

Specifies whether Configuration Server allows an empty (blank) password in a client connection request when these requests are authenticated externally. When set to `true` (default), Configuration Server will permit an unspecified password in an externally authenticated request.

> ### Important
> There might be instances where an LDAP server, instead of rejecting a blank password, might (depending on the LDAP Server configuration) interpret this to mean

that it should make an unauthenticated connection, giving the false impression that authentication has succeeded. To allow empty passwords in Configuration Server and still avoid this, set the **allow-external-empty-password** option to `false` so that configuration will enforce at least one character in a password sent to an external system.

If the option is set to `false` and the password in a request is not specified, Configuration Server rejects the request and generates a corresponding error message, regardless of the value of the two other options.

Refer to the User Passwords section of the *Genesys Security Deployment Guide* for more information about this option and how to use it.

allow-mixed-encoding

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

Specifies if Configuration Server checks if the encoding of user interface client applications at client registration matches the current encoding of Configuration Server. If set to `false` (the default), only those interface clients with the same encoding mode can connect to Configuration Server. If set to true, Configuration Server will not check, and the interface client can connect to Configuration Server regardless of its encoding mode.

Important

Be very careful if you are setting this option to true. If a client sends any string data that is encoded differently than the encoding used by Configuration Server, the behavior of Configuration Server will be undefined.

cfglib-connect-tmout

Default Value: `20`
Valid Values: Any integer from `0` to 65536 seconds
Changes Take Effect: After restart

Sets a timeout (in seconds) for this instance of Configuration Server to expect a TCP success or failure response from the remote Configuration Server to which it is connecting. If the connection has not been made when the timeout expires, all pending connection requests are cancelled.

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

The value of this parameter overrides that of the **-cfglib-connect-tmout** command-line parameter.

client-connect-timeout

Default Value: 40
Valid Values: Any positive integer from 1 to 65536
Changes Take Effect: After restart

Specifies the client connection timeout. The client should be authenticated before this timeout expires.

client-record-sync-timeout

Default Value: 0
Valid Values: Any positive integer from 0 to 20
Changes Take Effect: Immediately

Specifies a duration in seconds during which client records from Configuration Server (primary) or Configuration Server Proxy (primary) will be synched to their corresponding Backup Configuration Server in scenarios of switchover or shutdown in primary Configuration Server.

client-response-timeout

Default Value: 600
Valid Values: Positive integer up to 86400 (24 hours)
Changes Take Effect: Immediately

Limits the time, in seconds, during which Configuration Server retains prepared unsent data in its memory. If this timeout expires and the data is still unsent, Configuration Server disconnects the client and discards all the data related to it.

dbthread

Default Value: true
Valid Values: true, false

true	Uses internal database thread. This is the preferred method.
false	Uses separate DB Server, as in releases prior to 8.5.

Changes Take Effect: After restart

Specifies how Configuration Server accesses the Configuration Database.

If set to true, Configuration Server attempts to launch a database client process locally using the options specified in the Configuration Database section, but not the host and port options. This is the preferred method of accessing a database.

If set to false, Configuration Server attempts to use a remote DB Server, as specified in the Configuration Database section, including the host and port options. This was the only way to access a database in releases prior to 8.5. Genesys recommends that you use this method only with older Genesys applications.

decryption-key

Default Value: No default value
Valid Values: Valid path to decryption file
Changes Take Effect: After restart

Specifies the path to an external .pem file containing the RSA key used for decrypting the password to the Configuration Database. The presence of this option, plus **encryption** set to `true`, indicates that the password was encoded using an asymmetric algorithm, with an encryption key from an external file.

Configuration Server creates or updates the value of this option if the **-keys** parameter is specified in the command-line at startup.

Important

- This option is set automatically by Configuration Server. Do not change the value of this option manually, except in the following circumstance.
- If you want to switch back to using an unencrypted Configuration password, set the value of this option to empty (no value) and set the **encryption** option to false, then manually enter the unencrypted password into the Configuration Server configuration file. **Note:** You must have Write access to the Configuration Server configuration file to do this.
- If you then want to revert back to using symmetric encryption, set the value of this option to empty (no value), and restart Configuration Server from the command line using the `-p <name of Configuration Database section> <password>` parameter.

delay-reload-backup

Default Value: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: For the next reconnect to the master

Specifies the reload delay period (in seconds) for the backup Configuration Server Proxies or the master Configuration Server running in the backup mode. You can specify a higher delay period for the backup Configuration Server proxies to ease the load on the master Configuration Server after network outages when multiple clients need to reload data at the same time.

The configured reload delay period applies to the master Configuration Server when it needs to reload data while running in the backup mode or after being switched to backup mode upon a switchover.

This option does not delay initial data load after Configuration Server restart and it does not delay the attempt to restore the previous session to the master Configuration Server. This option takes effect only if an attempt to restore the previous session with the master Configuration Server fails.

> **Tip**
> Specify different delay reload settings for different proxies to establish the order in which proxies initiate reload. You can use this option in conjunction with the **proxy-load-max** option to further delay data reloading process for the proxies.

disable-vag-calculation

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

Specifies whether Configuration Server calculates Virtual Agent Groups for existing and newly-created objects for the application in which it is configured.

To manage the calculation of Virtual Agent Groups by primary and backup Configuration Servers before and after switchovers, add this option to both the primary and backup Configuration Servers, in the sections with the same name as the corresponding `Application` objects. If this option is set to `true`, Configuration Server does not calculate Virtual Agent Groups for existing and newly-created objects.

> **Important**
> You must set this option to the same value for both the primary and backup Configuration Servers. Then stop and restart both Configuration Servers. You must do this each time you change this option to retain the contents of the Virtual Agent Group.

decryption-padding

Default: If the password is encrypted, PKCS 1 padding is used
Valid Value: OAEP - password is encrypted using OAEP padding
Changes Take Effect: After restart

The presence of this option, together with **encryption** set to `true` and **decryption-key** options, indicates that the configuration database password is encrypted using an asymmetric algorithm with OAEP padding. Configuration Server creates or updates the value of this option when the password is encrypted as described in the section Encrypting the Configuration Database Password of the *Management Framework Deployment Guide*.

> **Important**
> This option is set automatically by Configuration Server. Do not change the value or remove this option manually, except when you are switching back to using an unencrypted configuration database password, as described for the encryption option.

enable-pre-812-security

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

If set to `true`, this option restores pre-8.1.2 security behavior as follows:

- Enables a user, who does not have Change permission on a folder, to move objects from that folder to another location.
- Enables a user, who does not have Change Permissions permission on an object, to change the object's permissions implicitly by moving the object with inherited permissions between folders with different permission.

If set to `false` (the default), both actions are disabled.

> **Important**
>
> To take effect, this option must be set to `true` in both the **confserv** section of the primary master Configuration Server, and in the corresponding main section of the backup master Configuration Server.

> **Warning**
>
> Use this option only in exceptional cases, and only as a temporary measure.

encoding

Default Value: `UTF-8`
Valid Values: `UTF-8, UTF-16, ASCII, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8, ISO-8859-9, ebcdic-cp-us, ibm1140, gb2312, Big5, koi8-r, Shift_JIS, euc-kr`
Changes Take Effect: After restart

Sets the UCS (Universal Character Set) transformation format (such as UTF-8, UTF-16, Shift_JIS, and so on) that Configuration Server uses when exporting configuration data into an XML (Extensible Markup Language) file. The Configuration Import Wizard (CIW) must initiate the export operation. If the operating system settings do not support the specified value, Configuration Server uses the default value.

Specify the UTF-8 encoding format unless you are using wide-character codesets (such as Chinese, Japanese, Korean).

> **Important**
>
> In single-language format on UNIX platforms, the value of this option must match the value defined by the LANG environment variable (or derived from the values of the LC_ALL and LC_CTYPE environment variables as specified in the vendor documentation). On the Solaris platform, you might be required to set the environment variable GCTI_TRANSLOCALCP to the value that represents the current local system encoding name (returned by the `iconv -l` command). You must set this Genesys-specific variable only if, in your environment, the value returned by the command does not match the codepage name specified in system locale settings (`LANG, LC_ALL, or LC_CTYPE`) on Solaris.

encryption

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

When set to `true`, the values of the password options in all Configuration Database sections are interpreted as being encrypted. Configuration Server decrypts the value when reading its configuration file at startup, accesses the Configuration Database using the decrypted value, and prints an encrypted string of characters as the password value into the log.

This option is set to `true` automatically by Configuration Server when the **-p** parameter is specified in the startup command line.

> **Important**
>
> - This option is set automatically by Configuration Server. Do not change the value of this option manually, except in the following circumstance.
> - If you want to switch back to using an unencrypted Configuration password, set the value of this option to `false` and set the **decryption-key** option to empty (no value), then manually enter the unencrypted password into the Configuration Server configuration file. Note: You must have Write access to the Configuration Server configuration file to do this.

fix_cs_version_7x

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

Use this option when using a master Configuration Server running release 8.0.3 (or later) with a Configuration Server Proxy running release 8.1.1 (or earlier). Setting this option to true enables the master Configuration Server to treat Configuration Server Proxy as running an equivalent schema.

This prevents Configuration Server Proxy from using an incorrect schema and reading configuration data incorrectly.

> **Important**
>
> If you are trying to run a Configuration Server Proxy release 8.1.1 (or earlier) with a Master Configuration Server 8.x, make sure that this option is set to `true` before setting up the connection between the two servers. Otherwise, the configuration schema of Configuration Server Proxy will be incorrect, and you will have to reinstall Configuration Server Proxy. However, note that Genesys strongly recommends that Configuration Server and Configuration Server proxy be running the same version of software. The only exception is during migration, in which case the servers can run different version but only until migration is complete.

force-md5

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

Specifies whether Configuration Server uses the MD5 hashing algorithm to hash user passwords. MD5 was the default algorithm prior to Management Framework 8.1.2, when it was replaced by the SHA256 algorithm. If set to `false` (the default), all new and changed passwords will be hashed using SHA256. If set to `true`, all new and existing passwords will be hashed using MD5.

Use this option if you are running Configuration Server Proxy 8.1.0 (or earlier) that supports MD5, and a master Configuration Server8.1.1 (or later) that supports SHA256. In this case, the two servers can be running together long enough to encounter password requests. Because they use two different hashing algorithms, the master Configuration Server will be unable to process the requests. You must force Configuration Server to use MD5 by setting the **force-md5** option to `true` in the **confserv** section of the master Configuration Server.

> **Important**
>
> Genesys does not recommend that you run a newer version of Configuration Server with an earlier version of Configuration Server Proxy. However, this situation is allowed for a short time during migration.

Refer to the User Passwords section of the *Genesys Security Deployment Guide* for more information about this option and how to use it.

langid

Default Value: No default value
Valid Values: Valid integer from list of LCID to language mappings
Changes Take Effect: After restart

This option is mandatory for Configuration Server operating in single-language mode with Configuration Database in 8.5 format, and specifies the language used by Configuration Server. This option is ignored by Configuration Server in multi-language mode, or when working with Configuration Database in 8.1 format.

Set this option in the configuration file of Configuration Server. If Configuration Server Proxies are configured, set this option in only the master Configuration Server; the proxy servers determine the language used in a single-language environment automatically, based on the response they receive from the master Configuration Server to which they are connected.

When Configuration Server and the Configuration Database are installed using the default (English) initialization scripts, this option must be set to 1033 (English, ENU) in the configuration file. If any Configuration Server Language Packs are applied to the single-language Configuration Database, the value of this option value be changed to match the value of one of the Language Packs, as given in the following table.

Language	Value of languid
English (ENU)	1033
Chinese (Simplified) (CHS)	2052
French (France) (FRA)	1036
German (DEU)	1031
Korean (KOR)	1042
Japanese (JPN)	1041
Portuguese (Brazil) (PTB)	1046
Spanish (Mexico) (ESM)	2058

For more information about installing and using Language Packs for the Configuration Database, refer to the Configuration Database section of the *Framework Deployment Guide*.

last-login

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

Specifies whether the Last Logged In Display feature is to be used. If set to `true`, the feature is used for this Configuration Server. Last Logged In information is sent to its clients, and is stored and displayed by Genesys graphical user interfaces that support this feature.

If set to `false` (the default), this feature is not used for this Configuration Server.

For more information about the Last Logged In Display feature and this option, see the “Last Logged In Display” topic in the *Genesys Security Deployment Guide*.

last-login-synchronization

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

Specifies whether Last Logged In information is synchronized between this Configuration Server or Configuration Server Proxy and others in the environment. If set to `true`, this Configuration Server or Configuration Server Proxy sends notifications about changes in Last Logged In information to others in the configuration.

If set to `false` (the default), Last Logged In information is not synchronized between this Configuration Server or Configuration Server Proxy and others in the configuration.

This option is ignored if the last-login option is set to `false`.

For more information about the Last Logged In Display feature and this option, see the "Last Logged In Display" topic in the *Genesys Security Deployment Guide*.

locale

Default Value: No default value
Valid Values: Any valid locale name or abbreviation
Changes Take Effect: After restart

Specifies the locale setting that Configuration Server uses for date/time/currency format (where applicable). It also affects encoding that is selected by Configuration Server in single-language mode when transforming configuration object information from internal representation for export to an XML file. If you do not specify the option, Configuration Server uses the default operating system setting.

Genesys recommends that you rely on operating system settings for locale selection, instead of this Genesys option. If you do have to set it up here, select values for this option from the official Microsoft locale list. For example, for English, specify `english` or `eng`; for Japanese, specify `japan` or `jpn`; and so on. For UNIX, consult the vendor documentation for your operating system.

The specified locale value must be supported by your operating system, and must match the value that is defined by the LANG environment variable (or derived from the values of the `LC_ALL` and `LC_CTYPE` environment variables, as specified in the vendor documentation). When this option is set, its value must also be aligned with the **encoding** option; that is, the locale in use must activate the same encoding as specified by that option.

> **Important**
>
> On the Solaris platform, you might be required to set the environment variable `GCTI_TRANSLOCALCP` to the value that represents the current local system encoding name (returned by the **iconv -li** command). You must set this Genesys-specific variable only if, in your environment, the value returned by the command does not match the codepage name specified in system locale settings (`LANG`, `LC_ALL`, or `LC_CTYPE`) on Solaris.

management-port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port that management software uses to monitor and control the operation of

Configuration Server. If not specified, management agents cannot monitor and control the operation of Configuration Server. You cannot set this option to the value specified for the **port** option.

max-client-output-queue-size

Default Value: `1024`
Valid Values:

`0`	No limit
Any positive integer	Threshold value (in KB)

Changes Take Effect: Immediately

Specifies the threshold on the amount of memory (in KB), used by prepared unsent data for a single client, at which Configuration Server defers processing requests from that client.

When the amount of unsent data drops below that threshold, Configuration Server restarts processing incoming requests from the client in the order that they were originally received.

max-output-queue-size

Default Value: `0` Valid Values:

`0`	No limit
Any positive integer	Threshold value (in MB)

Changes Take Effect: Immediately

Specifies the threshold on the total amount of memory (in MB), used by prepared unsent data, at which Configuration Server defers processing of all incoming requests. While processing of the incoming requests is deferred, Configuration Server continues to receive and store incoming requests for further processing.

When the amount of unsent data drops below that threshold, Configuration Server restarts processing incoming requests.

> **Important**
> Use this option with extreme care. Reaching the threshold specified by this option effectively halts Configuration Server until the size of outgoing buffers drops below the specified value. This option is intended to be a last resort defense against unexpected termination due to memory starvation.

multi-languages

Default Value: `false`
Valid Values: `false, true`
Changes Take Effect: At first start of Configuration Server; subsequent changes not permitted

Specifies if Configuration Server supports UTF-8 encoding internally.

> **Important**
> You can only set this option to `true` if you are using a multi-language version of the Configuration Database initialization scripts.

objects-cache

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

Specifies if Configuration Server uses internal caching. When set to true, Configuration Server caches objects requested by client applications. This is the default behavior of Configuration Server in previous releases. When this option is set to `false`, the objects are not cached, reducing the amount of memory used by Configuration Server.

> **Important**
> Disabling the cache may increase the load on Configuration Server during client application registration. Use this option with care.

packet-size

Default Value: `1024000`
Valid Values: 1–2147483648
Changes Take Effect: After restart

Specifies, in bytes, the target maximum size of the packet in a single message.

> **Important**
> Do not change this option unless instructed by Customer Care.

password-change

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

Specifies whether Configuration Server allows users to change his or her own password, if the user does not have Change permission for his or her own object. If set to false, the user can change his or her own password only if he or she has Change permissions on his or her own object. If this option is

set to true (default), Configuration Server allows the user to change the password regardless of the Change permission.

> **Important**
>
> This option does not apply if the System Administrator has configured the Force Password at Next Login feature.

For more information about this option and how to use it in your password system, refer to the User Passwords section of the *Genesys Security Deployment Guide*.

peer-switchover-tmout

Default Value: 30
Valid Values: 10–600
Changes Take Effect: After restart

Specifies the time interval (in seconds) that a Configuration Server, when switching to primary, waits for the other Configuration Server in the HA pair to close its side of the connection between the two servers. The servers cannot switch over if one server has the connection open. If the specified time expires before the connection is closed, the switchover request is ignored and the server mode does not change.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port that Configuration Server clients use to connect to this server.

> **Important**
>
> The **port** option is used only during the first start of Configuration Server with an initialized database. Upon subsequent restarts, Configuration Server reads the port information from its Application object in the Configuration Database and ignores the setting of the port option in the configuration file.

primary-master-response-timeout

Default Value: 600
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the time interval, in seconds, the backup Configuration Server and Configuration Server Proxy waits for a response from the primary master Configuration Server while loading data from it. If

this timeout expires, connection to the primary master Configuration Server is closed and then reconnection and data loading processes are reattempted from scratch.

For master Configuration Server, set this option in the main section of Configuration Server primary and backup to enable this functionality during startup. For the proxies, this option must be specified in the command line.

> **Important**
>
> The time measured to determine the timeout condition includes the time needed to completely receive a response for each request. Some responses may contain a significant portion of the entire configuration database. Setting this option too small for large databases can cause false timeouts and results in consistent failure to load data.

primary-startup-tmout

Default Value: `30`
Valid Values: 1—MAXINT
Changes Take Effect: After restart

Specifies the time interval (in seconds) that the backup Configuration Server waits for the primary Configuration Server to finish starting up and run as primary before continuing its own startup.

When two Configuration Servers in an HA pair start at the same time and detect each other's presence before either has completed its initialization, this option effectively determines which server starts as primary and which starts as backup. In this case, the server configured as primary continues its startup and initialization to completion to run as the primary Configuration Server. The server configured as backup, delays its initialization and waits for the primary server to start up and open its ports. After the time specified by this option, the backup Configuration Server attempts to connect to the now-running primary Configuration Server, and if successful, continues its start-up as backup.

> **Important**
>
> - Genesys strongly recommends that, to avoid concurrency during startup, you start one Configuration Server at a time.
> - Do not use this option unless instructed to do so by Genesys Customer Care.

session-restore-auth

Default Value: `empty`
Valid Values: `empty, username, password`
Changes Take Effect: After restart

Specifies the authentication method to be used when the Client application restores its connection

with Configuration Server with the restoration request (MSGCFG_RESTORESESSION). You can set this option either in the Client application or Configuration Server application. However, the authentication method configured in the Client application takes precedence. You can set `empty`, `username` or `password` as authentication methods. By default, `empty` is set.

- **username** - during connection restoration, username with old cached session's username will be validated.
- **password** - during connection restoration, password and username with old cached session's username and password will be validated.
- **empty** - during connection restoration, no authentication occurs.

server

Default Value: No default value
Valid Values: Any character string
Changes Take Effect: After restart

Specifies the name of the Configuration Database section in the configuration file; see Configuration Database Section. You must specify a value for this option.

upgrade-mode

Default Value: `0`
Valid Values: `0, 1`
Changes Take Effect: After restart

Used during migration to specify if peer Configuration Servers are able to start up side-by-side without contacting each other. If set to `1`, this independent side-by-side startup is permitted. If set to `0` (zero, the default), the startup of one Configuration Server is communicated to the other. For more information about the requirement for migration with minimum downturn, refer to the *Management Framework Migration Guide*.

Configuring ADDP Between Primary and Backup Configuration Servers

Use the options in this section to configure Advanced Disconnect Detection Protocol (ADDP) between primary and backup Configuration Servers. Configure the options in the following sections:

- In the primary Configuration Server, set them in the **confserv** section.
- In the backup Configuration Server, set them in the section that has the same name as the backup Configuration Server `Application` name.

> **Important**

> If one or both Configuration Servers have not been started up for the first time, set the options in the configuration file of the appropriate servers.

protocol

Default Value: No default value
Valid Values: `addp`
Changes Take Effect: After restart

Specifies if ADDP is to be used between the primary and backup Configuration Servers. If set to `addp`, the ADDP protocol is implemented as defined by the configuration options `addp-timeout`, `addp-remote-timeout`, and `addp-trace` in the same configuration server section (**confserv**, or its equivalent in the backup Configuration Server) of the configuration file. If this option is set to any other value, or if it is not specified at all, ADDP is not used and the ADDP-related configuration options in this section are ignored.

addp-remote-timeout

Default Value: `0`
Valid Values: `0`–`3600`
Changes Take Effect: After restart

Specifies the time interval, in seconds, that Configuration Server in backup mode instructs the other Configuration Server in the redundant pair to use when polling to check the connection between the two servers. If set to zero (`0`), Configuration Server in backup mode does not send any such instruction. This option applies only if the value of the **protocol** option is `addp`.

> **Important**
> Because any Configuration Server can be in primary or backup mode, regardless of how it is configured, you must set this option to the same value in both the primary and backup Configuration Servers.

addp-timeout

Default Value: `0`
Valid Values: `0`–`3600`
Changes Take Effect: After restart

Specifies the time interval, in seconds, that Configuration Server in backup mode waits before polling the other Configuration Server in the redundant pair. If set to zero (`0`), Configuration Server in backup mode does not poll the other Configuration Server in the redundant pair. This option applies only if the value of the **protocol** option is `addp`.

> **Important**
>
> Because any Configuration Server can be in primary or backup mode, regardless of how it is configured, you must set this option to the same value in both the primary and backup Configuration Servers.

addp-trace

Default Value: `off` Valid Values:

false, no, off	Turns ADDP off.
true, yes, on, local	ADDP trace occurs on the side of the Configuration Server in backup mode.
remote	ADDP trace occurs on the side of the Configuration Server in primary mode.
both, full	ADDP trace occurs at both the primary and backup Configuration Servers.

Changes Take Effect: After restart

Determines whether ADDP messages are written to the primary and backup Configuration Servers log files. This option applies only if the value of the **protocol** option is addp.