T-Server for CSTA Connector Deployment Guide

T-Servers 8.1.1

12/30/2021

Table of Contents

T-Server for CSTA Connector Deployment Guide

Use this guide to learn about the concepts, terminology, and procedures relevant to T-Servers in general and provides detailed reference information about T-Server for CSTA Connector. The reference information includes configuration options, limitations, and switch-specific functionality. See the summary of the highlighted topics below:

About T-Server

Find out about the T-Server:

Overview

New in This Release

Feature Configuration

Find out about the supported features that include these topics:

Agent Substitution

Business-Call Handling

all topics>>

T-Library Support

Find out about T-Library Support that include these topics:

Private Service and Events

T-Library Functionality

all topics>>

Configuration Options

Find out about the configuration options:

Common Configuration Options

T-Server Common Configuration Options

T-Server Specific Configuration Options

all topics>>

T-Server Deployment

Find procedures to configure and install the T-Server that include these topics:

T-Server Deployment Fundamentals

Multi-Site Support

all topics>>

Overview

Welcome to the *T-Server for CSTA Connector Deployment Guide*. These topics introduce you to the concepts, terminology, and procedures that are relevant to T-Server for CSTA Connector.

About T-Server for CSTA Connector

Genesys T-Server for CSTA Connector belongs to the Framework Media Layer, which enables Genesys solutions to communicate across media, including traditional telephony systems, voice over IP, e-mail, and the Web. It depends on CSTA Connector for BroadSoft Broadworks for providing switch CTI translations to Genesys standard CSTA.

New in This Release

The following general changes have been implemented in the 8.1 release of CSTA Connector:

- Support for the new Broadsoft Release 17 SP4 feature: Call Recording.
- Multiple connections from T-Server for CSTA Connector to BroadWorks Connector.
- Support on Red Hat Enterprise Linux 6 32- and 64-bit platforms.
- Limited display of sensitive information: In logs, new options enable sensitive data in logs to be marked for post-processing by the user, such as deletion, replacement, or hiding. See the Genesys 8.1 Security Deployment Guide for details.
- Compliance with FIPS: TLS as implemented by Genesys meets the Federal Information Processing Standards (FIPS).

Feature Configuration

Supported Features

The following table lists the functionality supported by T-Server for CSTA Connector:

- Account Codes
- Agent Substitution for Monitored Agents
- Business-Call Handling
- Call Recording
- Call Release Tracking
- Call Type Prediction
- Emulated Agents
- Failed Route Notification
- Hot-Standby HA
- Hunt Groups
- Keep-Alive Feature Handling
- Link Bandwidth Monitoring
- No-Answer Supervision
- Partitioned-Switch Configuration
- Request Handling Enhancements
- T-Server Error Messages

Account Codes

T-Server distinguishes between two situations for the Account Code feature:

- Account codes that are entered during a call, or during After-Call Work (ACW) when the released call is left, are treated as account codes.
- Account codes that are entered while the agent is idle are interpreted as walk-away codes.

Any account codes entered during a call are treated by T-Server as call account codes. T-Server reports such account codes using attached user-data with configurable keys. Optionally, T-Server can report an account code as an `Extensions` attribute key, instead of an `UserData` attribute key, to minimize interference with the other components, such as ISCC and other user applications.

While Call Concentrator can pick up `Extensions` attribute events, the same as the `UserData` attribute, Stat Server can only work with the `UserData`.

Indexing by Key Name

In scenarios where multiple account codes are required, it is possible to turn on key name indexing. When indexing is enabled, T-Server should attach each subsequent account code and increment the index part of the key.

The index is an incremental integer attached to the configured key name after an underscore, starting with 1—for example: `AccountCode_1`, `AccountCode_2`, and so on). T-Server only attaches unique codes that are not yet attached. T-Server keeps non-indexed key—for example: `AccountCode`, updated with the last received value irrespective of whether indexing is enabled or not.

In case multiple calls exist on the device, T-Server attaches the code to the last active call. For this reason, T-Server has to keep a historically ordered stack of active calls on the device so that last active call can be easily and reliably identified.

The data key name is set by the configuration option, accode-name. If the configured name is different from `AccountCode`, then the name for multiple account codes is also changed and represented as `"<value of "accode-name">_<N>"`.

Related Configuration Options

The following configuration options support the Account Code feature:

accode-data

accode-data

Default Value: none
Valid Values:
none—T-Server does not map the switch account codes to the call user data.
udata—T-Server attaches reported account codes as user data, using the key defined by the accode-name option. T-Server then sends requests to set account codes to the switch, when such user data keys are used in client requests AttachUserData or UpdateUserData.
ext—T-Server attaches user data as extensions to all call events and does not intercept user data update requests with the reserved keys.
Changes Take Effect: Immediately
Related Feature: Account Codes

Specifies whether T-Server has to map the switch account codes to call user data (value udata), to extensions (value ext) or will not map switch account codes (value none).

Note: T-Server uses the reserved keys sent in any call-related client-request Extensions attribute, regardless of the value of this option. The only exception is when the configuration option is set to udata and the user data in the request contains the account code.

accode-name

accode-name

Default Value: AccountCode
Valid Values: Any valid key name
Changes Take Effect: Immediately
Related Feature: Account Codes

Specifies the data key name under which T-Server attaches the account code to the call, as either user data or extensions.

accode-privateservice

accode-privateservice

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately Related Feature: Account Codes

Enables or disables the use of `TPrivateService` and `EventPrivateInfo` for handling the Account Code feature.

acw-retain-call

acw-retain-call

Default Value: `false`
Valid Values:`true, false`
Changes Take Effect: Immediately
Related Feature: Account Codes

Instructs T-Server to retain the last agent business call while the agent is in an After-Call Work (ACW) period and allows user data updates to be added after the call has been released. This allows the account code to be attached to the previous call. When set to true, T-Server sends the account code in the `EventUserEvent` message, rather than the `EventAttachedDataChanged` message, to avoid confusing existing desktop applications.

Note: To enable the Standard Account Code functionality in T-Server, both this option and `acw-retain-lock` must be enabled.

acw-retain-lock

acw-retain-lock

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: Immediately
Related Feature: Account Codes

Specifies the period of time, in seconds, for the call to remain locked in Call Concentrator after the call has been released. When this option is enabled, T-Server sends an `EventUserEvent` event with the `Extension` attribute key, `LockCall` and the value set by the option. Typically, this value should be greater than the After-Call Work (ACW) value.

Note: To enable the Standard Account Code functionality in T-Server, both this option and the `acw-retain-call` option must be enabled. In addition, the `acw-retain-lock` option must be set to a value equal to, or greater than, the value set on the PBX for the Account Code timeout period.

Agent Substitution

An agent can be monitored in the same way as a device of type `ACD Station` and T-Server accordingly adjusts the device and call event reporting. The Agent ID value is reported in place of the device ID in the `thisDN` field of the event. When the Agent Substitution feature is activated (normal operation), T-Server sends all call-related events on the ACD-authorized device when an agent is logged in. This means that T-Server clients only need to register for the ACD-authorized device and not the agent device.

Although T-Server reports all events for the agent on the ACD-authorized device extension, calls must still be made to the agent and not to the ACD-authorized device.

When the agent is monitored, the switch typically reports call events using the `AgentID` as the event device. T-Server needs to replace this event device with the agent device found in T-Library reporting.

T-Server then performs the following steps:

1. Checks the device identifier of the call events that are sent to it.
2. Checks to see whether the device identifier matches the id of a currently logged in agent that has monitoring enabled.

If there is a match, T-Server uses the agent's associated device for the `ThisDN` field in the reported Genesys T-Library event(s) and the Agent ID for the `AgentID` field.

Configuration

To enable the Agent Substitution feature, `AgentID` has to be configured in the `Agent Logins` tab of the `Switch` object, and monitoring has to have started on the `AgentID`.

T-Server monitors `AgentID`, if the following conditions are met:

- The `AgentID` value consists only of digits.
- No other DN with the same digits as `AgentID` is configured in the configuration environment.
- The `TServer`-level configuration option, `monitor-agents`, or the `Agent`-level configuration option, `monitor`, are set to enable `AgentID` monitoring.
- `AgentID` is not configured for use as an Emulated Agent (for more information, see the `Agent`-level configuration option, `emulate-login`).

For more information, see the Related Configuration Options topic.

Note: For normal operation, a monitored `AgentID` should be provisioned as a hoteling guest in BroadSoft BroadWorks and DNs (that the agent is logged into) should be provisioned as hoteling hosts in BroadSoft BroadWorks.

Related Configuration Options

The following configuration options support the Agent Substitution for Monitored Agents feature:

monitor

monitor

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

Specifies whether the switch should monitor the agent. The value of the `monitor` configuration option overrides any value of the `monitor-agents` configuration option set at the `Application`-level. Set this option in the `TServer` section of the `AgentID Annex` tab.

monitor-agents

monitor-agents

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

Specifies whether T-Server should monitor all agents specified in the `Agent Logins` tab. This value can be overridden by the agent `monitor` or `emulate-login` Annex tab options. T-Server monitors the number as a device and substitutes events on that device with the position number that the agent is logged on. Set this option in the `TServer` section on the `Options` tab of the T-Server `Application` object.

Note: Use this option when all `AgentIDs` are planned for monitoring. For more selective `AgentID` monitoring, use the Agent-specific Override option, `monitor`.

Business-Call Handling

This section describes how T-Server handles different types of calls. Based on the call assignment, T-Server applies the appropriate business-call handling after the call is released.

T-Server Call Classification

T-Server automatically assigns every call to one of the four following categories:

- Business
- Work Related
- Private
- Unknown

According to which type is assigned, T-Server applies the appropriate business call handling after the call is released. T-Server reports the business call type in the call related events by using the `BusinessCall` key in the `Extensions` attribute, unless the business call type is *Unknown*.

Business Calls

By default, T-Server categorizes any call that is distributed to an agent or extension through a Routing Point, a Routing Queue, or an ACD Queue as a business call. This behavior can be modified by adding the `bsns-call-type` option to the distribution device's `Annex` tab. The `bsns-call-dev-types` configuration option determines whether a call on a distribution device is promoted to a business call type. Use the following configuration options to define what additional calls (to or from an agent) are classified as business calls:

- `inbound-bsns-calls`
- `outbound-bsns-calls`
- `internal-bsns-calls`
- `unknown-bsns-calls`

T-Server can be configured to categorize consultation calls that are made on behalf of a business call as business calls using the following option:

- `inherit-bsns-type`

See, the Related Configuration Options topic for more information on these configuration options.

Once a call is classified as a business call, this attribute remains with the call (connection ID) until it is ended. When an agent releases a call that T-Server has categorized as a business call, T-Server applies the automatic emulated wrap-up and legal guard times, if these features are configured. See, the Emulated After-Call Work (ACW) topic for more information.

Private Calls

T-Server categorizes any call that does not fall into the business or work-related categories as a private call. T-Server does not apply any automatic business-call handling after a private call. If emulated agents receive a direct private call while in wrap-up or legal-guard time, the emulated wrap-up or legal-guard timer is not interrupted.

Work-Related Calls

T-Server categorizes any non-business call that an agent makes while in an after-call work (ACW) as a work-related call. T-Server does not apply any automatic business-call handling after a work-related call.

Because emulated agents can make or receive a direct work-related call while in wrap-up time, T-Server pauses the emulated wrap-up timer for the duration of such a call.

If an agent receives a direct work-related call during legal-guard time, T-Server cancels the legal-guard timer and reapplies it at the end of the work-related call.

Unknown Calls

Any call that does not fall into any of the above categories is classified as an unknown call.

Business Call Type Configuration

Determining the Business Call Type

T-Server uses the following options to determine the business call type of a call, which are displayed in order of precedence, from highest to lowest:

- T-Server supports an Extensions attribute request to define the business call type upon call initiation or answer.
- T-Server uses the originator agent state to determine if the call is work related.
- The Configuration Manager Annex tab configuration option, bsns-call-type, specifies the business call type for calls that pass through or arrive at a distribution device.

If the call passes through a distribution device and there is no DN-level option present, the call is classified as a business call, as long as this is enabled by the bsns-call-dev-types option. Automatic classification of calls as business calls on distribution DNs can be disabled by the Application-level option, bsns-call-dev-types.

If the corresponding flag of this option is disabled, calls passing distribution DNs of that type do not change their respective business classification, but the Extensions attribute request and DN-level option are still affected.

The distribution devices include the following device types:

- Routing Point
- ACD Queue
- Routing Queue
- External Routing Point

T-Server supports options that are configured on the Application-level to define whether specific call types (inbound, outbound, internal, or unknown) are to be classified as business calls.

See, the Related Configuration Options topic for more information on the configuration options mentioned above.

Specifying the Business Call Type

To specify the business call type for the new call, the BusinessCallType Extensions attribute can be attached to the following requests:

- TMakeCall
- TInitiateTransfer

- TMuteTransfer
- TInitiateConference
- TMakePredictiveCall

The BusinessCallType Extensions attribute takes precedence over all other Configuration Manager business call type configuration options. This Extensions attribute can also be attached to the TAnswerCall request to specify the business call type for the answering party and call.

The DN-level option, bsns-call-type, specifies the business call type for calls that pass through or arrive at a distribution device (Routing Point, Route Queue or ACD Queue). If the call passes through a distribution device and there is no Annex tab option present, the call is classified as a business call. If the call passes through more than one distribution device, then the usual rules for assigning a business call type are followed. Once set, the business call type cannot be overridden unless it is changed to a business call.

When the following configuration options: inbound-bsns-calls, internal-bsns-calls, and outbound-bsns-calls are set at the Application-level, they control whether the call type of the associated calls are classified as business calls. T-Server does not classify the business type of the call using these options until the destination is known. Also, these options are not used to set the originating party's business type as business until after the Dialing event is reported. (This is to ensure that Genesys reporting is consistent, regardless of the switch-reported order of events).

The private request, TSetBusinessCall, allows T-Server clients to set the business call type of an existing call to business. T-Server responds to a successful request by distributing the private event, EventBusinessCallSet.

See, the Related Configuration Options topic for more information on the configuration options mentioned above.

Related Configuration Options

The following configuration options define what additional calls to or from an agent are classified as business calls:

bsns-call-dev-types

bsns-call-dev-types

Default Values: `+acdq +rp +rpq +xrp`
Valid Values: A set of space separated flags.

`+/-acdq`—Turns on/off the classification of the call type as business on an ACD Queue.
`+/-rp`—Turns on/off the classification of the call type as business on a Routing Point.
`+/-rpq`—Turns on/off the classification of the call type as business on a Routing Queue.
`+/-xrp`—Turns on/off the classification of the call type as business on an External Routing Point.

Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Specifies which types of distribution devices will be exempt from default business-call handling. By default, T-Server classifies any call arriving at a distribution device (ACD Queue, Routing Point, Routing Queue, and External Routing Point) as a business call. Using this option, you can disable automatic classification for calls to a particular type of distribution device—for example, if the value for this option is set to `-rp`, calls to Routing Point DNs are not automatically classified as `business`, allowing the routing strategy to use the `BusinessCallType` `Extensions` attribute.

Note: This option does not affect the application of the DN-level `bsns-call-type` option.

bsns-call-type

bsns-call-type

Default Value: none
Valid Values:

`business`—The call is classified as a business call.
`private`—The call is classified as a private call.
`ignore`—The distribution point has no effect on business call classification.

Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Specifies the business call type for calls that pass through or arrive at the associated device.

Note: This option takes precedence over the following options that are set at the `Application`-level: inbound-bsns-calls, inherit-bsns-type, and outbound-bsns-calls. This option may be over-ridden by the `BusinessCallType Extenstions` attribute.

inbound-bsns-calls

inbound-bsns-calls

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Specifies whether T-Server should consider all established inbound calls on an emulated agent as business calls.

inherit-bsns-type

inherit-bsns-type

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Determines whether a consult call that is made from a business primary call should inherit the `business call` attribute.

internal-bsns-calls

internal-bsns-calls

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Determines whether T-Server considers internal calls made from or to any agent as business calls.

outbound-bsns-calls

outbound-bsns-calls

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Specifies whether T-Server should consider all established outbound calls on a emulated agent as business calls after being established.

Call Recording

Call recording provides the functionality to digitally record calls on a requested connection. CSTA Connector supports the CSTA `RecordMessage` request that can be invoked on the behalf of the BroadWorks user, which starts recording messages on the requested connection.

T-Server supports the `TPrivateService` request (service number: `3013`) to invoke a CSTA `RecordMessage`:

- Upon receiving a CSTA Event Start `EventPrivateInfo` event, a `CallRecordingStarted` message (private message id: `3013`) is generated.
- Upon receiving a CSTA Event Stop `EventPrivateInfo` event, a `CallRecordingStopped` message (private message id: `3014`) message is generated.

Currently, it is impossible to stop recording for BroadSoft BroadWorks. T-Server processes the `TPrivateService` request (service number: `3014`) to stop the recording in progress, however, CSTA Connector returns an `Unsupported Operation` error.

T-Server reports the current recording status in the `Extensions` attribute for the `EventRegistered` and `EventAddressInfo` events using the `Extensions` attribute key value-pair, `RECORDING_STATE`.

See, the Private Services and Events topic for more information regarding the Call Recording Private Services and Events.

Limitations

- CSTA Connector for BroadSoft BroadWorks does not support stop operation for Call Recording.
- CSTA Connector for BroadSoft BroadWorks does not support Query Call Recording functionality on start-up.

Related Configuration Options

The following configuration option enables or disables the Call Recording feature:

broadworks-version

Default Value: `17.sp4`
Valid Values: The supported BroadWorks release version.
Changes Take Effect: Immediately
Related Feature: Call Recording

Specifies release version *17.sp4* in all CTI requests sent to the BroadWorks XSI server and provides backwards compatibility with previous CSTA Connector releases.

Call Release Tracking

T-Server now provides information about which party initiated the release of a call. This functionality is valuable for different applications to provide historical and real-time call reporting.

The following T-Library SDK call models can now be reported in this way:

- Normal call release.
- Abnormal call release.
- Call release from a conference.
- Rejection of an alerting call.
- Release for a failed or blocked call to a busy destination.

DN-Based Reporting

In DN-based reporting, information about the call release initiator is reported in the `Extensions` attribute using the `ReleasingParty` key-value pair in the `EventReleased` and `EventAbandoned` events, when those events are distributed.

One of the following values is reported in the `ReleasingParty` key-value pair:

- `1 Local`—The call is released because the `ThisDN` value in the `EventReleased` requested the release.
- `2 Remote`—The call is released because the other party (which is remote to `ThisDN`) in the `EventReleased` or `EventAbandoned` events requested the release operation.
- `3 Unknown`—The call is released, but T-Server cannot determine the release initiator.

Call-Based Reporting

Independently of DN-based reporting, T-server provides the call release initiator in `AttributeCtrlParty` attribute for `EventCallPartyDeleted` and `EventCallDeleted` events. For scenarios where T-Server cannot provide the release initiator, the `AttributeCtrlParty` attribute does not appear in the event reporting.

T-Server provides reporting for the `AttributeCtrlParty` attribute (for the party that initiated the call release) either when:

- The call is released using a `GCTI` request and T-Server is aware of the result of the requested operation, or;
- The PBX CTI protocol provides reliable information about the identity of party that is released.

Related Configuration Options

The following configuration option enables or disables the Call Release Tracking feature:

releasing-party-report

Default Value: `false`
Valid Values:`true, false`
Changes Take Effect: Immediately
Related Feature: Call Release Tracking

Specifies whether T-Server reports the `ReleasingParty Extensions` attribute in `EventReleased` and `EventAbandoned` events to indicate which party initiated the call release.

Call Type Prediction

T-Servers use CTI-provided information to assign a call type to a call. On occasions when the CTI information is either insufficient or arrives too late for T-Server to assign a definite call type, T-Server can now use a call type prediction procedure to assign a call type on a *best possible guess* basis.

When this feature is enabled by the `call-type-by-dn` configuration option, T-Server analyzes other DNs in the call and goes through the following steps (in a specific order) to decide whether other DNs are internal or external:

1. T-Server uses the Configuration Manager DN configuration to verify whether the DN is configured in the configuration environment. DNs configured in Configuration Manager are considered as internal.
2. T-Server verifies whether the `otherDN` value is included in the DN range configured on the configuration environment switch. If the `otherDN` value falls within the configured DN range, then it is considered as internal.
3. T-Server verifies whether the `otherDN` value is included in the same `dn-scope` T-Server monitoring scope. Calls placed between DNs from the same scope are considered as internal.
4. T-Server verifies whether the DN is monitored on the PBX (see, the Unregistered DNs topic). Unregistered DNs that are still monitored on the PBX DN are still considered as internal.
5. T-Server performs a digit analysis if the `call-type-rules` section contains a valid set of rules.
6. If none of above steps return a positive result, then T-Server uses the existing (if any) algorithm to assign the call type.

The rules for *digit analysis* are specified in the `rule-<n>` configuration option found in the `call-type-rules` configuration section. The call-type rules specify the number of dialing plans related to the external, internal, and unknown DNs. When these rules are provided, the `otherDN` value fits into any of pre-configured rules and then the configured call type (internal, external, or unknown) is assigned.

Call Type Prediction is only effective if the T-Server specific common option, `dn-scope`, is not configured. If this option is configured, the call type assignment follows the rules enforced by that option.

The following table shows how T-Server assigns predictive call types in different scenarios:

Call Type Prediction

Call Direction/ OtherDN	External	Internal	Unknown
Incoming	`CallTypeInbound`	`CallTypeInternal`	`CallTypeUnknown`
Outgoing	`CallTypeOutbound`	`CallTypeInternal`	`CallTypeUnknown`

Call Type Rules Example

An example of the configured call type rules is as follows:

- The operator console, `00`, is internal.
- The abbreviated dialling number `10` is unknown.
- All numbers consisting of four digits are internal.
- All numbers consisting of seven digits are external.
- All numbers that start with 2 are internal.
- The rest of the numbers are external.

These requirements correspond to the following set of rules in the configuration:

- rule-1= `pattern=00, value=internal`—the operator console, `00`, is internal
- rule-2= `pattern=10, value=unknown`—the abbreviated dialing number `10` is unknown
- rule-3= `pattern=AAAA, value=internal`—all numbers consisting of four digits are considered as internal
- rule-4= `pattern=AAAAAAA, value=external`—all numbers consisting of seven digits are considered as external
- rule-5= `pattern=[2]A*B, value=internal`—all numbers that start with 2 are considered as internal
- rule-6= `pattern=[0-9]A*B, value=external`—all numbers that start with a lead digit from `0` (zero) to 9 are processed by T-Server as external numbers. (This rule is the default fallback rule. When no other rules match, this rule is used for all numbers that start with a positive digit value).

Related Configuration Options

TServer Section

You can configure the Call Type Prediction feature in T-Server using the following `TServer` section options set at the `Application`-level:

call-type-by-dn

call-type-by-dn

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Call Type Prediction

Enables or disables the setting of call type based on dialing plan analysis (when configured) and on the DN configuration in the Configuration Layer.

See `call-type-rules` for dialling plan analysis configuration.

call-type-rules

call-type-rules

Default Value: none
Valid Values: Name for the configuration section where the digit analysis rules are defined.
Changes Take Effect: Immediately
Related Feature: Call Type Prediction

Specifies name for configuration section where digit analysis rules are defined.

Note: This configuration option is required if the configuration section named.

Call-Type-Rules Section

You call also configure this feature using the following `Call-Type-Rules` section option:

rule-<n>

Default Value: none
Valid Values: Any valid string in the following format :
`pattern=<input pattern>; value=<internal|external|unknown>`
Changes Take Effect: Immediately
Related Feature: Call Type Prediction

Defines a rule to be applied to an inbound number, where `n=1-N`. Multiple rules can be created and number will be matched against all patterns for those rules. As soon as first match is found then result specified in the value part of the option is used for call type assignment.

Emulated Agents

T-Server emulates the following functionality for agents in situations where the PBX does not support it:

When this feature is used, T-Server emulates the following functionality:

- Login and logout
- Agent set ready
- Agent set not ready (using various work modes)
- Automatic after call work (ACW)
- After call work in idle
- Automatic legal-guard time to provide a minimum break between business related calls

Depending on the PBX capability T-Server can emulate none, some or all of these features.

Emulated Agent Login/Logout

You can configure T-Server to perform emulated login either always, never, or on a per-request basis. See, the emulate-login option for more information.

Agent Logout on Client Unregistering from DN

In some scenarios (such as a power failure/disconnection or when a desktop stops responding), agents may still receive calls but be unable to handle them. To prevent this problem, T-Server can be configured to automatically logout the agent in such circumstances.

When a client desktop or application disconnects from T-Server while an agent is still logged in, T-Server receives a notification that the application is unregistering from the agent's DN. Also, T-Server is able to uniquely identify the client application which sends a T-Library request, including `TAgentLogin` and `TRegisterAddress`.

T-Server can associate the client application (the one that sends the initial `TAgentLogin` request) with the agent and automatically log that agent out when the client application unregisters the agent DN while the agent is still logged in. (The initial`TAgentLogin` request is the one which first logs the agent in). See, the Related Configuration Options topic for more information.

HA Considerations

If T-Server is running in HA mode, a client connecting to one T-Server will be connected to both with the same session ID. Therefore the client's session ID must be used as part of the association data to ensure consistency across the primary and backup T-Servers. The primary T-Server will send an HA

synchronization message to the backup when there is a change in client associations.

Emulated Agent Ready/NotReady

Emulated agents can perform an emulated Ready or NotReady request regardless of whether they are on a call, subject to the rules governing work modes.

T-Server also reports any change in agent modes requested by the agent while remaining in a NotReady state (*self-transition*).

Note: The *Genesys Events and Models Reference Manual* and the *Platform SDK 8.x .NET (or Java) API Reference* define which agent state/agent mode transitions are permissible.

Emulated After-Call Work (ACW)

T-Server can apply emulated wrap-up (after-call work or ACW) for agents after a business call is released, unless the agent is still involved in another business call (see Business Call Handling).

See, the Related Configuration Options topic for more information about the configuration options for this feature.

Timed and Untimed ACW

T-Server applies emulated ACW for an agent after any business call is released from an established state. T-Server automatically returns the agent to the Ready state at the end of a timed ACW period. The agent must return to the Ready state manually when the ACW period is untimed.

Events and Extensions

T-Server indicates the expected amount of ACW for an agent in `EventEstablished` event using the `WrapUpTime` `Extensions` attribute. It is not indicated in the `EventRinging` event because the value may change between the call ringing and the call answer. Untimed ACW is indicated by the string value, `untimed`, otherwise the value indicates the expected ACW period in seconds.

T-Server reports ACW using the `EventAgentNotReady` event with the `AgentAfterCallWork` agent work mode and indicates the amount of ACW it will apply using the `WrapUpTime` `Extensions` attribute.

T-Server sends the`EventNotReady(ACW)` before the `EventReleased` at the end of the business call.

Emulated ACW Period

The amount of emulated ACW that T-Server applies (when required) after a business call is determined by the value in the `wrap-up-time` configuration option.

The `untimed-wrap-up-value` configuration option determines which specific integer value of `wrap-up-time` indicates the untimed ACW. To specify the untimed ACW in `Extensions` or `UserData` attribute requests, you should use the string `untimed` instead. All positive integer values are treated as indicating timed ACW (in seconds). For backwards compatibility, the default value of `untimed-wrap-up-value` is `1000`.

Note: Changing the value of untimed ACW should be done with care, because may affect the interpretation of all integer values of the `wrap-up-time` option in Configuration Manager. If lowered, it may change the timed ACW to untimed, or disable ACW altogether. If raised, it may change the untimed or disabled ACW to timed ACW. The use of the new option (string) value, `untimed`, is encouraged whereever possible to minimize the impact of any future changes to the value of the

untimed-wrap-up-value option.

Pending ACW

An agent can request emulated ACW, or override the period of (emulated) ACW to be applied to themselves, while on an established call. T-Server applies the emulated ACW when the call is released. The agent sends a TAgentSetReady request with workmode = 3 to request pending ACW while on an established call. The WrapUpTime Extensions attribute indicates the amount of ACW that T-Server applies, using the following parameters and rules:

- Extension missing - untimed ACW
- Value = 0 - ACW is disabled
- Value greater than 0 - period of timed ACW in seconds
- Value = untimed - untimed ACW
- Invalid value - request is rejected

If the request is successful, T-Server sends an EventAgentReady message with workmode = 3 (ACW). T-Server will also indicate that the agent is in a pending ACW state by adding the ReasonCode Extensions attribute with the new value PendingACW. It will also indicate the period of ACW to be applied using the WrapUpTime Extensions attribute.

An agent may alter the period of pending ACW by sending a new TAgentSetReady request with workmode = 3, using a different value for the WrapUpTime Extensions attribute. If the request is successful, T-Server sends another EventAgentReady event, indicating the new value in the WrapUpTime Extensions attribute.

Note: To enable this feature the agent desktop the WrapUpTime Extensions attribute must be enabled on the agent desktop.

Emulated ACW In Idle

An agent can activate wrap-up time on request when idle, by issuing a TAgentSetNotReady request with workmode = 3 (AgentAfterCallWork) to request emulated ACW while idle.

Extending ACW

An agent can request an extension to the amount of emulated ACW for a call while in emulated ACW or in the legal-guard state.

The agent requests an Extensions attribute to ACW by sending a TAgentSetNotReady request with workmode = 3 (AgentAfterCallWork). T-Server determines the period of the extended ACW from the WrapUpTime Extensions attribute, as follows:

- Value = `0` - No change to ACW period, but T-Server reports how much ACW time remains.
- Value greater than `0` - T-Server adds the given number of seconds to the timed ACW period. Untimed ACW remains unaffected.
- Value = `untimed` - T-Server applies untimed ACW.

T-Server sends an `EventAgentNotReady` message with `workmode` = 3 (AgentAfterCallWork), reporting the newly extended amount of ACW using the `WrapUpTime Extensions` attribute. If the agent was in the emulated legal-guard state, T-Server places the agent back into emulated ACW state.

The agent may extend the period of ACW as many times as desired. At the end of the extended timed ACW period, T-Server applies legal guard if any is configured. No legal guard is applied if the emulated ACW was untimed.

Note: To enable this feature the agent desktop the `WrapUpTime Extensions` attribute must be enabled on the agent desktop.

Emulated Legal-Guard Time

T-Server applies emulated legal-guard time for agents before they are about to be automatically set ready after any period of timed ACW or after the last business call is released where there is no ACW to be applied. It is a regulatory requirement in many countries to guarantee that agents have a break of a few seconds before the next call can arrive. No legal-guard time is applied if the ACW period was not timed or if the agent is not being placed into the Ready state.

T-Server reports legal guard using an `EventAgentNotReady` event with `workmode` = 2 (LegalGuard). If an agent requests to be logged out during emulated legal-guard time, T-Server immediately logs the agent out.

If the agent requests to go to a `Not` Ready or Ready state during legal-guard time, T-Server terminates legal guard and transitions the agent to the requested state. If the agent requests to return to the ACW state, T-Server re-applies legal guard at the end of ACW, provided that the agent still requires it according to the above criteria.

The period of legal guard is determined by the configuration option, `legal-guard-time`. See, the Related Configuration Options topic for more information.

HA Synchronization

On startup and link re-establishment, the Hot Standby backup T-Server requests the primary T-Server to send details of all agents. The primary T-Server replies with all the information required for switchover, including all emulated and switch-based data.

From this point on, the primary T-Server also sends a similar synchronization message whenever an emulated agent's state changes.

This means that a higher level of synchronization between the two T-Servers is maintained at all times.

Related Configuration Options

Enabling or Disabling the Emulated Agent Login

The following configuration options enable or disable the emulated agent login/logout functionality:

agent-emu-login-on-call

agent-emu-login-on-call

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server allows an emulated agent login or logout on a device where there is a call in progress.

This option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The `TServer` section of the `Annex` tab of the `Agent Login` object.
2. The `TServer` section of the `Annex` tab of a device.
3. The `TServer` section of the application.

The value can also be set by using the `AgentEmuLoginOnCall` `Extensions` attribute in the `TAgentLogin` or `TAgentLogout` requests. The value specified by the extension, where present, takes precedence over the settings configured in the Configuration Layer.

agent-strict-id

agent-strict-id

Default Value: `false`
Valid Values: `true, false, passwd`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server allows:

- Any Agent ID to be used during login (value false)
- Only Agent IDs configured in the Configuration Layer to be used during login (value true)
- Only Agent IDs that match an Agent ID configured in the Configuration Layer and that also have a matching password (value passwd)

emulate-login

emulate-login

Default Value: on-RP
Valid Values:

- true—T-Server performs an emulated login.
- false—T-Server passes a login request to the PBX.
- on-RP—T-Server checks the Agent Group associated with the login request. If the Agent Group is a standard Routing Point, then the emulated login request succeeds. This value can only be set at the Application-level, and is available for backwards compatibility.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server performs an emulated agent login when the login device is configured in the Configuration Layer as a device of type extension.

This value can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next highest level, and so on.

1. In the TAgentLogin request, using the EmulateLogin key of the Extensions attribute.
2. In the TServer section of the Annex tab of the Agent Login object.
3. In the TServer section of the Annex tab of the login device object.
4. In the device representing an Agent Group object, on the Annex tab.
5. In the T-Server Application object, in the Tserver section.
6. Using an Agent Group corresponding to an object that is configured in the Configuration Layer as a device of type Routing Point.

emulated-login-state

emulated-login-state

Default Value: ready
Valid Values:

- not-ready—T-Server distributes EventAgentNotReady after EventAgentLogin.
- ready—T-Server distributes EventAgentReady after EventAgentLogin.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

When T-Server performs an emulated agent login and the client specifies an agent work mode other than ManualIn or AutoIn, T-Server uses this option to determine which event to distribute.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the Agent Login object on the Annex tab.
2. In the agent login device on the Annex tab.
3. In the login device representing an Agent Group object during login, on the Annex tab.
4. In the T-Server Application object in the Tserver section.

sync-emu-acw

sync-emu-acw

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server synchronizes emulated ACW for native agents.

This option can be set in Configuration Manager in the following places in order of precedence (highest to lowest):

1. In the TServer section in the Annex tab of an Agent Login object.
2. In the TServer section in the Annex tab of a device.
3. In the TServer section of the application.

The SyncEmuACW Extensions attribute of the TAgentLogin request overrides the value configured for this option.

Enabling or Disabling the Automatic Agent Logout

The following configuration options enable or disable the automatic logout of the agent:

agent-logout-on-unreg

agent-logout-on-unreg

Default Value: `false`
Valid Values:

- `true`—T-Server logs out emulated and native agents on unregister.
- `false`—T-Server does not log out emulated or native agents on unregister.
- `emu-only`—T-Server logs out only emulated agents on unregister.

Changes Take Effect: At the next agent login session
Related Feature: Emulated Agents

Specifies whether T-Server performs an automatic logout of an agent whenever their client application unregisters the DN from T-Server. This happens whenever a client application disconnects from T-Server.

The option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The `TServer` section in the `Annex` tab of the device representing the agent's group (such as an `ACD queue`).
2. The `TServer` section of the `Annex` tab of the `Agent Login` object.
3. The`TServer` section of the `Annex` tab of a device.
4. The `TServer` section of the application.

The Configuration Layer configuration setting may be overridden by adding the `AgentLogoutOnUnregister` `Extensions` attribute to the `TAgentLogin` request.

Any subsequent self-transition `TAgentLogin` request can override the current agent association by adding the `AgentLogoutOnUnregister` `Extensions` attribute with a value of `true.`

Similarly a `TRegisterAddress` request can override the current agent association by adding the `AgentLogoutOnUnregister` `Extensions` attribute with a value of `true.`

agent-logout-reassoc

agent-logout-reassoc

Default Value: `false`
Valid Values:

- `true`—T-Server automatically associates a new client application with the agent.
- `false`—T-Server does not automatically associate a new client application with the agent.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server automatically associates as a new client application with the agent, when the application either:

- Registers on the agent DN, or;
- Sends a login request while T-Server is currently waiting to log the agent out due to the previously associated client disconnecting.

Note: The new client application must have the same application name as the previously disconnected client.

The option can be set in the Configuration Layer in the `TServer` section of the application.

Enabling or Disabling the Emulated ACW Period

The following configuration options enable or disable the emulated ACW period functionality:

override-switch-acw

override-switch-acw

Default Value: `true`, `false`
Valid Value: `false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether or not the T-Server emulated ACW overrides the switch ACW for calls distributed through a Routing Point.

This option can be set in the following places, in order of precedence (highest to lowest):

1. In the `TServer` section of the `Annex` tab of DNs of type `Routing Point`.
2. In the `TServer` section of the `Options` tab of the T-Server `Application` object.

untimed-wrap-up-value

untimed-wrap-up-value

Default Value: `1000`
Valid Value: Any positive integer or `0` (zero)
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the time threshold in seconds at which the timing of ACW stops and manual intervention is required (untimed ACW).

wrap-up-threshold

wrap-up-threshold

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the minimum period (in seconds) that a business call must last before emulated ACW is applied at the end of the call.

wrap-up-time

wrap-up-time

Default Value: `0` (zero)
Valid Value: Any positive integer, `untimed`

`0` (zero)	ACW is disabled. Exception: If this option is set in the Annex tab of the `Agent Login` object, a value of `0` (zero) means that T-Server processes from Step 4 in the processing order of precedence below.

A value greater than 0 (zero), but less than the value set for the untimed-wrap-up-value option.	The number of seconds of timed ACW, after which T-Sever returns the agent automatically to the Ready state.
A value equal to the value set for the untimedwrap-up-value option.	ACW is untimed and the agent must manually return to the Ready state.
A value greater than the value set for the untimed-wrap-up-value option.	Disables ACW.
untimed	ACW is untimed and the agent must manually return to the Ready state. **Note:** This value cannot be set on the Annex tab of an Agent Login object.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the amount of wrap-up time (ACW) allocated to emulated agents at the end of a business call.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the WrapUpTime Extensions attribute key of the TAgentPendingACW request (applies to this agent only).
2. In the WrapUpTime Extensions attribute key of the TACWInIdle request (applies to this agent only).
3. In the call, in the WrapUpTime UserData attribute (limited to ISCC scenarios).
4. In a DN configuration object of type ACD Queue or Routing Point, on the Annex tab in the TServer section.
5. In the WrapUpTime Extensions attribute key of the TAgentLogin request, (applies to this agent only).
6. In the Agent Login configuration object, on the Annex tab in the TServer section (but not including the untimed value).
7. Using an Agent Group corresponding to an object configured in the Configuration Layer as a device of type ACD Queue.
8. In the T-Server Application object, on the Options tab in the TServer section.

Enabling or Disabling Pending ACW Functionality

The following configuration options enable or disable the pending ACW functionality:

acw-in-idle-force-ready

acw-in-idle-force-ready

Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether, after timed manual wrap-up (when you have set the value of the `timed-acw-in-idle` to `true`), T-Server forces the agent to the Ready state. If this value is set to `false`, T-Server returns the agent to the agent's previous state prior to requesting manual wrap-up.

timed-acw-in-idle

timed-acw-in-idle

Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server applies the automatic wrap-up timer (using the `wrap-up-time` parameter) when an agent sends a `TAgentNotReady` request.

If the value of this option is set to `false`, T-Server does not automatically end manual wrap-up—the agent must return manually from ACW.

Note: For compatibility with the previous T-Server release, you can use the name `timed-cwk-in-idle` for this option as an alias.

Determining the Period of Legal Guard Time

The following configuration options determine the period of legal guard time:

legal-guard-reason

legal-guard-reason

Default Value: `LegalGuard`
Valid Value: Any string
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the value of the `Extensions` attribute key used by T-Server to indicate that the agent is in legal guard mode. T-Server adds the `ReasonCode` `Extensions` attribute with a value of `LegalGuard` to the `EventAgentNotReady` event, signalling the start of legal guard. If this option is set to a null string, then no extension is added.

legal-guard-time

legal-guard-time

Default Value: `0` (zero)
Valid Value: Any integer from `0-30`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies a legal-guard time (in seconds) for emulated agents to postpone the transition to the Ready state after a business call. T-Server always considers a routed call a business call.

Handling Calls in Emulated ACW

T-Server's handling of an agent who is making or receiving a call while the agent is in emulated ACW is governed by the `backwds-compat-acw-behavior` configuration option.

backwds-compat-acw-behavior

Default Value: `false`
Valid Value: `true`, `false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether pre-8.0 behavior after-call work is enabled (value = `true`) or disabled (value = `false`), for backward compatibility.

If the value is set to `true` and an agent receives or makes a business call while in emulated ACW, T-Server does the following:

1. Stops the ACW timer.
2. Forces the agent to the Ready state.
3. Restarts ACW (and the legal-guard timer) after the new business call is released.

If an agent makes or receives a work-related call while in ACW, T-Server does the following:

- Suspends the ACW, but leaves the agent in the `ACW` state.
- Resumes the ACW timer once the work-related call is released.

Note: A work-related call is one made by an agent while in ACW, or a consultation call where the main call is either a business call or a work-related call.

After the ACW and any configured legal-guard time have been completed, the agent is forced to the Ready state.

- If an agent makes or receives a private call during ACW, no action is taken and the ACW timer keeps running.
- If the value is set to `false`, pre-8.0 behavior is used. In this case, T-Server forces the agent to the Ready state after the after-call work and legal-guard timer have been applied.

Error Messages

The following tables present the complete set of error messages T-Server distributes with the `EventError` event.

T-Server-Defined Errors

T-Server-Defined Errors

Code	Description
50	Unknown error
51	Unsupported operation for the switch
52	Internal error
53	Invalid attribute
54	Switch not connected
98	Cannot complete transfer
119	Invalid password
177	Target DN invalid
714	Invalid Call_ID

ISCC Errors

ISCC (Inter Server Call Control) Errors

Code	Description
1000	Invalid or missing server location name
1001	Remote server disconnected
1002	Remote server has not processed request
1003	Wrong protocol version
1004	Remote link disconnected
1005	External routing feature not initiated
1006	No free CDNs
1007	No access number
1008	TCS feature is not initiated

Code	Description
1009	Invalid route type
1010	Invalid request
1011	No primary server was found on location
1012	Location is invalid or missing
1013	Timeout performing requested transaction
1014	No configured access resources are found
1015	No registered access resources are found
1016	Client is not authorized
1017	Invalid transaction type
1018	Invalid or missing transaction data
1019	Invalid location query request

Code	Description
1020	Invalid origin location

Switch-Specific Errors

Switch-Specific Errors

Code	Description
109	Link down or bad link specified
231	DN is busy
232	No answer at DN
233	Call rejected
1102	Badly structured APDU
1110	Duplicate invocation (packet missed)
1131	Unexpected error response
1132	Unrecognized error
1141	Request incompatible with object

Code	Description
1143	Object not known
1147	Request caused privilege violation on device
1153	Invalid call destination
1154	Invalid feature requested
1156	Invalid cross-reference identifier
1161	Invalid object state
1162	Invalid Connection ID
1173	Resource is out of service
1181	Object monitor limit exceeded
1190	Unspecified security error

Failed Route Notification

T-Server supports a variety of alarm messages for unsuccessful routing scenarios.

When this feature is enable, a failed route timer is set using the interval defined in the route-failure-alarm-period configuration option. Each routing failure reported during this period is added to a counter. If this counter exceeds a *high water mark* threshold value defined by the route-failure-alarm-high-wm configuration option, T-Server sets a route failure alarm condition, and resets the counter.

The alarm condition is cleared when fewer route failures than what is configured in the route-failure-alarm-low-wm configuration option are recorded and, also, there is no more than the number of route failures configured in the `route-failure-alarm-high-wm` option in one complete period (configured in the `route-failure-alarm-period` option).

Setting the value of the `route-failure-alarm-period` option to `0` (zero) disables this feature.

LMS Messages

High alarm

Text: `STANDARD Route Failure: Exceeds [%d1] failures within [%d2] seconds; Last Route ConnID[%s], ErrorCode(%d3 )`

Description: T-Server sends a warning that the number of allowable failed route requests during the set time period is exceeded.

Attributes:

- `%d1` represents the number of failed route requests during this time period
- `%d2` represents the period of time (in seconds) in which the failures occurred
- `%d3` represents the error code generated, within this time period, in the `EventError` message for the last failed route

Low alarm

Text: `STANDARD Route Failed: Below high water mark`

Description: The reported condition has ended.

Attributes: None

HA Considerations

Only the primary T-Server maintains the failed routing counter. The backup T-Server does not run the `route-failure-alarm-period` option timer, so it keeps the routing failure alarm in the canceled state.

- On switchover from the primary role to the backup role, T-Server stops the `route-failure-alarm-period` option timer and clears any alarm internally, without sending any LMS message.
- On switchover from the backup role to the primary role, T-Server starts the `route-failure-alarm-period` option timer and starts counting routing requests and routing failures.

Related Configuration Options

The following configuration options support the Failed-Route Notification feature:

route-failure-alarm-high-wm

route-failure-alarm-high-wm

Default Value: `10`
Valid Values: Any positive integer for an absolute value or a floating point number followed by a `%` (percent) symbol—for example: `10%, 2.25%, 5E-2%`.
Changes Take Effect: Immediately
Related Feature: Failed-Route Notification

Defines the high water mark which must be reached in order for a route failure alarm to be triggered, within the period configured in the `route-failure-alarm-period` option.

route-failure-alarm-low-wm

route-failure-alarm-low-wm

Default Value: `1`
Valid Values: Any positive integer for an absolute value or a floating point number followed by `%` (percent) symbol—for example: `10%, 2.25%, 5E-2%`.
Changes Take Effect: Immediately
Related Feature: Failed-Route Notification

Defines the low water mark which must be reached, while under the route failure alarm condition, within the period configured in the `route-failure-alarm-period` option.

route-failure-alarm-period

route-failure-alarm-period

Default Value: `0` (zero)
Valid Values: Any positive integer

Changes Take Effect: Immediately
Related Feature: Failed-Route Notification

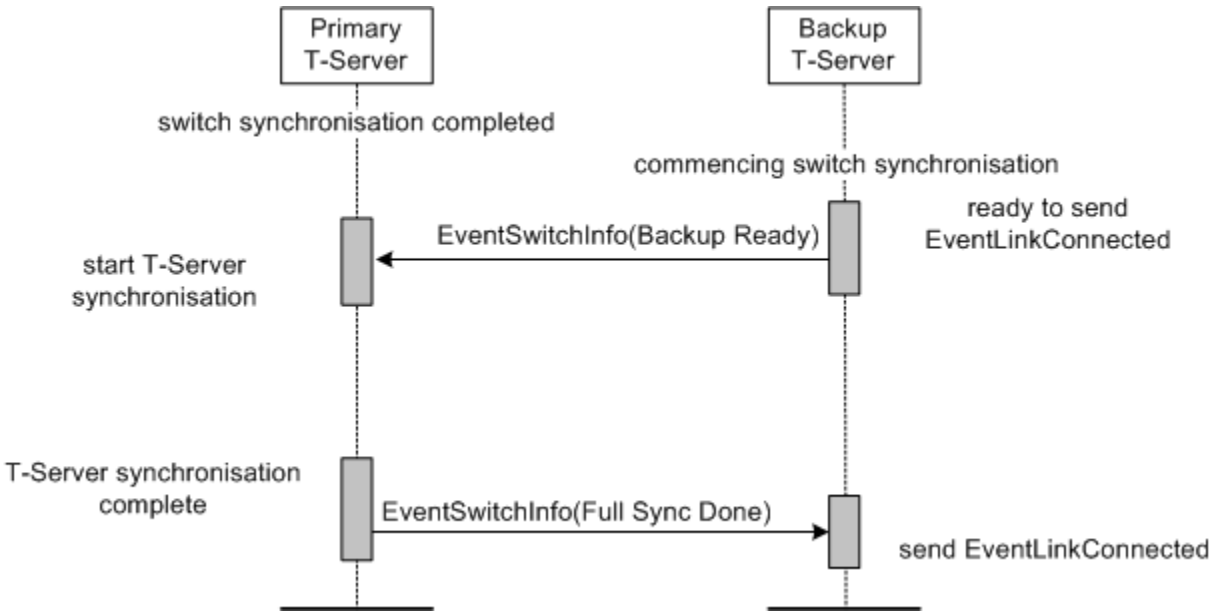
Defines the interval (in seconds) in which the number of failed route requests is totaled, in order to determine either a possible route failure alarm or the cancellation of an alarm, based on the failed route counter reaching the relevant high or low water mark.

Note: This option also specifies the minimum time between alarm setting and alarm clearing.

Hot-Standby HA

This section describes how T-Server supports the `hot-standby` high-availability (HA) synchronization.

The following figure shows the process of a successful detection of T-Server synchronization. The primary T-Server is assumed to have successfully completed the switch synchronization.



Hot-Standby (HA) T-Server Synchronization

If the Primary T-Server is Still in the Start-up Phase

If the primary T-Server is still in the process of switch synchronization when it receives a `Backup Ready`message from the backup T-Server, the primary T-Server sends the `Full Sync Done` message immediately. This allows the backup T-Server to send an `EventLinkConnected` message and become available. The Management Layer then sets the backup T-Server as the new primary, and vice versa. Once the old primary T-Server finishes switch synchronization, it initiates T-Server synchronization with the new primary T-Server as shown in the table above.

If the Primary T-Server's Link with the Switch is Down

If the primary T-Server has lost communication with the switch when it receives a `Backup Ready` message from the other T-Server, it sends the `Full Sync Done` message immediately. It can be assumed to have lost synchronization with the switch itself and there is no guarantee that it will recover communication with the link, which the backup T-Server currently has.

If the Backup T-Server Fails During Synchronization

If the backup T-Server fails while waiting for synchronization, the primary T-Server stops the synchronization process.

If the Primary T-Server Fails During Synchronization

If the primary T-Server fails while waiting for synchronization, the backup T-Server immediately sends an `EventLinkConnected` message.

Call Synchronization Between T-Servers

An integral part of T-Server synchronization is the synchronization of the Connection IDs of the calls between T-Servers. It is the Connection IDs of calls created by the backup T-Server during the switch synchronization phase that differ from those in the primary T-Server—those created afterwards are synchronized by the normal HA mechanism. When the primary T-Server receives the `Backup Ready` message from the backup T-Server, it tags all current calls. Once all tagged calls have been released, the primary T-Server can be certain that the Connection IDs for all current calls have been synchronized with the backup T-Server because they were created after the backup T-Server completed its startup phase. If no further T-Server synchronization is required, the primary T-Server sends the `Full Sync Done` message to the backup T-Server.

Using the EventSwitchInfo Event

T-Servers use the HA synchronization `EventSwitchInfo` messages for T-Server synchronization during the start-up phase of the backup T-Server. A new message attribute is defined to identify certain `EventSwitchInfo` events as specific only for backup synchronization. Two further attributes are required to distinguish between the `Backup Ready` event by the backup and the `Full Sync Done` event sent by the primary.

If the Backup T-Server Sends a EventSwitchInfo Message

The backup T-Server sends an `EventSwitchInfo` message to the primary T-Server indicating that it will become available as soon as the primary T-Server notifies it that the full synchronization is complete.

The backup T-Server sends a Standard level message to Message Server. This provides an indication that the backup T-Server is available for a forced fail-over (by stopping the primary) should this be needed. The format for the message is as follows, no parameters are required:

`Backup T-Server is now ready, starting wait for full synchronization.`

If the Primary T-Server Sends a EventSwitchInfo Message

The primary T-Server sends an `EventUserEvent` message to the backup T-Server once it has completed the full synchronization. Once the backup T-Server receives the event from the primary T-Server, it sends an `EventLinkConnected` message and becomes available for a managed fail-over.

The primary T-Server sends a Standard level message to Message Server. This provides an indication that it is completely safe to fail-over to the backup T-Server in situations where the `EventLinkConnected` message is sent immediately by the backup T-Server. The format for the message is as follows, no parameters are required:

```
Primary T-Server has detected full synchronization of backup T-Server.
```

Related Configuration Options

The following configuration option enables control of the `hot-standby` high-availability (HA) synchronization feature:

ha-sync-dly-lnk-conn

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: At T-Server start/restart
Related Feature: Hot-Standby HA

Determines whether the backup T-Server delays sending an `EventLinkConnected` message until it has been notified that the T-Server synchronization is complete:

- If the option is set to `true`, the backup T-Server sends an `EventLinkConnected` message once it has completed switch synchronization (that is, after all calls are cleared in the primary T-Server).
- If the option is set to `false`, there is no delay in sending an `EventLinkConnected` message and synchronization takes place the same as for pre-7.1 T-Servers.

Hot Desking

Hot-desking provides the capability of sharing a workspace. In a telephony context, hot-desking is a feature where a telephone device and/or address can be shared and/or re-used. See, the Hot Desking topic in the *CSTA Connector for BroadSoft BroadWorks Deployment Guide* for more information.

T-Server for CSTA Connector is able to support hot-desking reporting when used with a specific CSTA Connector, if the following conditions apply:

- The host device must be monitored as a device with the type `Extension` with the CSTA Connector.
- The guest device must be monitored as a device with the type `Extension` with the CSTAConnector.

Note: The guest devices must be either configured in the configuration environment or registered as a device that is not configured in Configuration Manager with the type `Extension`. It is not necessary to register the host device.

Guest/Host Association Before Startup

T-Server performs an internal query when a device of type `Extension` is registered with the switch. If the query returns that the `Extension` is associated with the host, T-Server reports the `Extension` attribute key, `HOST_DN` in the `EventRegistered` and `EventAddressInfo` events that correspond to the guest device. The value of the `Extension` attribute key denotes a host device number that is associated with the current device. See the Private Services and Events topic for more information about the the `Initiate hot-desking` and `Cancel hot-desking` Private Services.

Guest/Host Association After Startup

T-Server receives a notification if the association is after T-Server start-up. See, the Private Services and Events topic for more information about the the `Hot-desking established` and `Hot-desking cancelled` Private Events.

Hunt Groups

T-Server supports the BroadWorks Hunt Groups with different distribution modes (Circular, Regular) and HG overflow.

Keep-Alive Feature

T-Server may not always receive timely notification when the CTI link stops functioning. In order for T-Server to detect link failure and initialize alarm and recovery procedures, T-Server usually needs to actively check the link's integrity. This is referred to as Keep-Alive or *KPL* functionality.

Keep-alive functionality involves sending a KPL request which elicits either a positive or negative response from the CTI link. The responses are counted in four cumulative counters. If the relevant counter reaches the maximum configured limit, T-Server either:

- Decrements the relevant warning/failure KPL tolerance counter
- Attempts to reconnect to the link
- Sends a warning message to Message Server

Related Configuration Options

The following configuration options enable or disable the Keep-Alive feature:

kpl-interval

kpl-interval

Default Value: `10`
Valid Value: Any integer from `0-600`
Changes Take Effect: Immediately
Related Feature: Keep-Alive Feature Handling

Specifies a *keep-alive* interval (in seconds). To check network connectivity, T-Server issues a dummy CTI request at the interval specified when there is no other activity on the link. A value of `0` (zero) disables this feature. See, the `kpl-tolerance` option.

The value of this option may need to be increased to avoid false restarts, if the switch is slow to respond—for example, during busy periods.

kpl-tolerance

kpl-tolerance

Default Value: `3`
Valid Value: Any integer from `0-10`
Changes Take Effect: Immediately
Related Feature: Keep-Alive Feature Handling

Specifies the threshold number of accumulated failed keep-alive requests that T-Server permits before considering the CTI link to be interrupted. When this threshold is reached, T-Server treats the CTI link as either:

- Lost—T-Server tries to reconnect to the CTI link.
- Unstable—T-Server issues a warning message.

See, the `kpl-interval` option.

Link Bandwidth Monitoring

T-Server provides bandwidth monitoring on a CTI link and can notify the Genesys Management Layer when the Configuration Layer limits are exceeded.

When configured high or low thresholds are reached, T-Server sends either of the following alarm messages, as appropriate:

- `MSG_TS_COMMON_LINK_ALARM_HIGH` LMS
- `MSG_TS_COMMON_LINK_ALARM_LOW` LMS

High and Low Watermarks

- The link-alarm-high option, specified as a percentage of the `max-bandwidth` value, defines an upper threshold bandwidth value which when breached raises a `MSG_TS_COMMON_LINK_ALARM_HIGH` LMS message.
- The link-alarm-low option, specified as a percentage of the `max-bandwidth` value, defines a lower threshold bandwidth value which when breached raises a `MSG_TS_COMMON_LINK_ALARM_LOW` LMS message.

Alarm Set Algorithm

T-Server measures requests sent to the CTI link, and whenever there is a 99.7% probability that a high or low watermark threshold has been crossed, an appropriate LMS message is generated.

If the link-alarm-high option is set to `0` (zero), no high alarm is generated.

Note: A high or low watermark LMS message is only generated when there is at least a 99.7% probability that the requisite threshold has been crossed. Therefore, if the `link-alarm-low` option is set to `0` (zero), it cannot be crossed and no low alarm can be generated. Since a subsequent high alarm LMS message is only generated after a low watermark message, no further alarms can be raised.

LMS Messages

High alarm

```
STANDARD Link bandwidth: %d1 requests per second exceeds alarm threshold %d2 requests per second on CTI link ID %d3
```

Attributes:

- %d1 represents estimated requests rate
- %d2 represents link-alarm-high * max_bandwidth / 100
- %d3 represents the CTI Link ID

Low alarm

```
STANDARD Link bandwidth: %d1 requests per second dropped below alarm threshold %d2
requests per second on CTI link ID %d3
```

Attributes:

- %d1 represents estimated requests rate
- %d2 represents link-alarm-low * max_bandwidth / 100
- %d3 represents the CTI Link ID

Setting the `link-alarm-low` option to a value of `0` (zero) will not create a link alarm low LMS message. The link bandwidth must drop below the set low alarm level in order to create the low watermark message. For a high watermark, the bandwidth recorded must exceed the set high alarm watermark to create the high watermark LMS message. The consequence of setting the low alarm watermark to `0` (zero) is that T-Server will only generate one high watermark LMS message since a low watermark LMS message is never created. Therefore, T-Server will remain in high watermark alarm state indefinitely and will never generate a subsequent LMS high watermark message.

If the `link-alarm-low` option is set to a value higher than the value of the `link-alarm-high` option, then the two values are swapped. However, the values are not swapped if either value is set to `0` (zero).

See the LinkLoad `Extensions` attribute for more information about the link bandwidth feature.

HA Considerations

If the primary T-Server is at the high watermark prior to a switchover, its state is not transferred to the backup T-Server.

Related Configuration Options

The following configuration option are used to set bandwidth monitoring on a CTI link:

link-alarm-high

link-alarm-high

Default Value: `0` (zero)
Valid Values: `0-100`
Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the percentage of the `use-link-bandwidth` option when the `MSG_TS_COMMON_LINK_ALARM_HIGH` LMS message is triggered.

A value of `0` (zero) disables this feature.

link-alarm-low

link-alarm-low

Default Value: `0` (zero)
Valid Values: `0-100`
Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the percentage of `use-link-bandwidth` option when the `MSG_TS_COMMON_LINK_ALARM_LOW` LMS message is triggered.

use-link-bandwidth

use-link-bandwidth

Default Value: `auto`
Valid Values: `0-999, auto`

Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the maximum number of requests per second throughput to be used by T-Server to calculate the link alarm messages. A value of `0` (zero) disables this feature.

Multiple Configured Links

T-Server now supports multiple configured links to different CSTA Connectors. T-Server verifies the link availability and selects the active link by using the link priority defined in the link configuration and uses this link for all computer telephony integration (CTI) communication.

Connection Procedure

On initial start-up, the standalone or primary T-Server opens all configured CTI links. The backup T-Server opens only the CTI links with the highest provisioned priority. After the TCP/IP connection is accepted, T-Server then sends the computer-supported telecommunications applications (CSTA) call associated requests through all opened connections and waits for the the CSTA call associated responses. Each particular link is considered as established when the call associated response is received.

The CSTA Connector always sends the system status event right after the call associated response to T-Server. T-Server uses the system status event to validate whether the established link is operational. Use the `normal` value in the `SystemStatus` event argument parameter to set the validation check.

When this link is established, T-Server closes the non-operational links with the same or lower provisioned priority. T-Server makes this link active, if there are no more links waiting in the queue. The following LMS message (log number 35115) is then generated: `STANDARD CTI link %s with priority %d is selected`. The `Link Name` parameter corresponds to the CSTA Connector `Application` name. T-Server continues to use the active link for all CTI communications with CSTA Connector.

The connection time to the configured links is limited by the value specified in the T-Server `connect-tout` configuration option. If there are no operational links at that time, T-Server re-initiates the connection procedure.

If T-Server selected the link with the non-highest configured priority as an active link and this T-Server is assigned with the backup High-Availability (HA) role, it drops the current link and initiates the connection procedure to CTI links with the highest provisioned priority.

If more than one link is configured with the same priority, T-Server selects the link that is the first to report its System Status as `Normal`. This configuration allows the selection of the most responsive CSTA Connector for CTI operations.

Link Failure Handling

Upon detection of an active CTI link failure, an `EventLinkDisconnected` message is sent to all T-Servers clients. If T-Server is running in a High-Availability (HA) pair, the Management Layer switches this T-Server into the backup role. Reconnecting to the configured CTI links is initiated after the link restart timeout.

CTI Link Priority

T-Server supports the `priority` configuration parameter for each connection to a CSTA Connector. A higher parameter value indicates a higher priority.

- If a T-Server connection to a CSTA Connector is configured by adding a connection to the `Connections` tab of a T-Server application, the priority can be configured using the `priority` parameter in the `Application Parameters` field of this connection.
- If T-Server connection to a CSTA Connector is configured using the `link-%d-name` section, then the `priority` configuration option in this section is recognized.

Backward Compatibility

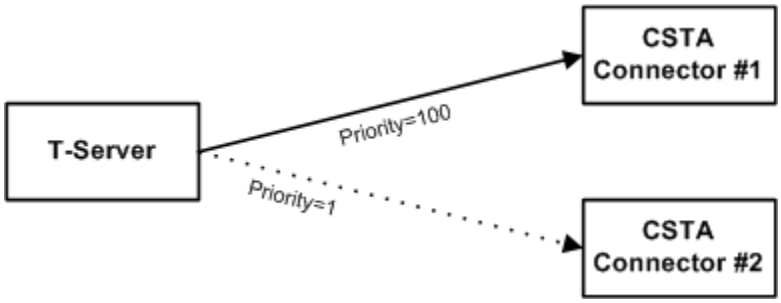
T-Server for CSTA Connector configured with a single link is fully backward compatible to earlier versions of T-Server.

High-Availability Examples

The following examples demonstrate different methods of how a standalone T-Server can operate in a high-availability (HA) configuration with redundant CSTA Connectors.

Example 1

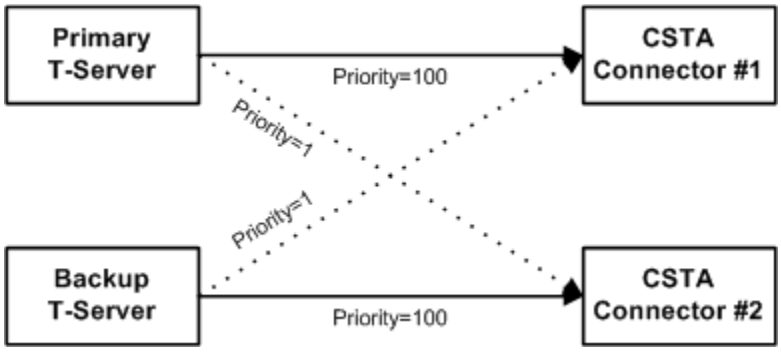
This example is similar to the HA `warm standby` redundant configuration for CSTA Connector, as illustrated below:



Warm-Standby (HA) Redundant Configuration

Example 2

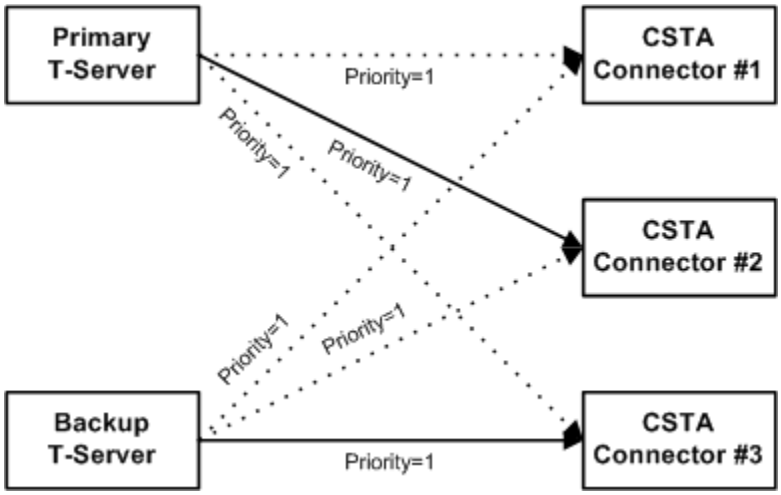
This example illustrates the seamless T-Server switchover in cases where the CSTA Connector fails. A failed CSTA Connector must be restarted to support the next CSTA Connector failover.



T-Server Switchover Where CSTA Connector Fails

Example 3

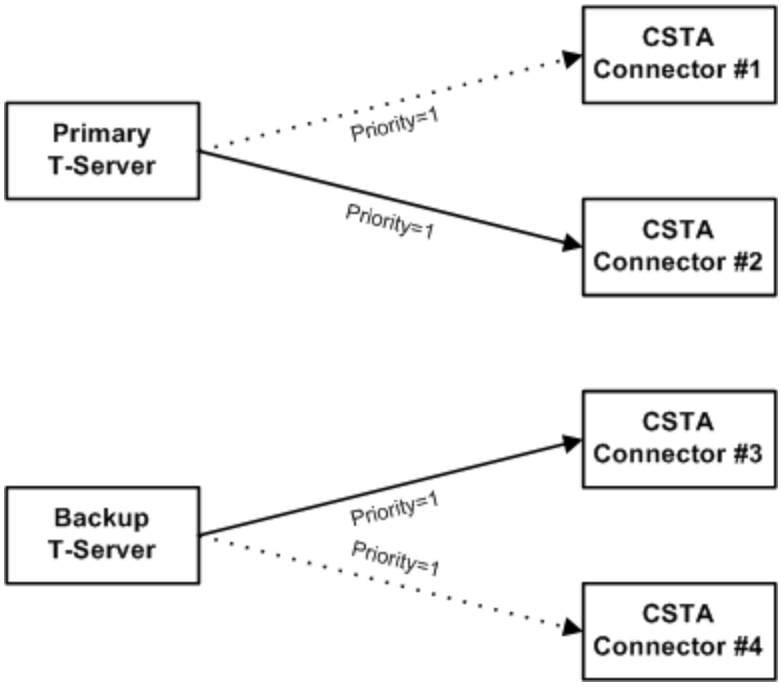
This example illustrates how the primary and backup T-Servers select the CSTA Connector with the shortest response time:



Primary and Backup T-Server Selection

Example 4

This example illustrates how the primary and backup T-Servers use different sets of CSTA Connectors to select the most responsive one:



Selecting the Most Responsive CSTA Connector

Related Configuration Options

connect-tout

Default Value: 2
Valid Values: Any positive integer from 1–1000
Changes Take Effect: On CTI link restart
Related Feature: Multiple Configured Links

Specifies the length of timeout, in seconds, T-Server waits for the CTI link with the highest priority to become operational.

Related Configuration Parameter

The `priority` application configuration parameter can be configured in two ways:

- for each link to the CSTA Connector
- in the link section where the CSTA Connector link is configured using the link-%s configuration option

priority

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: On CTI link reconnect
Related Feature: Multiple Configured Links

Specifies the priority for a given link to the CSTA Connector. A higher value means a higher link priority.

No-Answer Supervision

This section describes T-Server's No-Answer Supervision feature. See, the Related Configuration Options topic for a description of the configuration options mentioned below.

This feature implements no-answer supervision in T-Server that applies to any call that arrives on a device where there is an agent logged in.

T-Server supports the following types of no-answer supervision:

- Agent no-answer supervision
- Extension no-answer supervision
- ACD Position no-answer supervision

Agent No-Answer Supervision

This feature provides the following functionality:

- If an agent does not answer a call within a specified timeout, T-Server can divert the call to a sequence of overflow destinations. Alternatively, you can configure T-Server to return calls automatically to the last distribution device.
- If an agent fails to answer a call within a specified timeout, you can configure T-Server to either log out the agent or set the agent to `NotReady` to prevent further calls from arriving.

Extension No-Answer Supervision

The No-Answer Supervision feature includes devices of type `Extension`. If a call is not answered on an extension within a specified timeout, T-Server can divert the call to a sequence of overflow destinations. Alternatively, you can configure T-Server to return calls automatically to the last distribution device.

ACD Position No-Answer Supervision

The No-Answer–Supervision feature includes devices of type `ACD Position`. If a call is not answered on an ACD Position within a specified timeout, T-Server can divert the call to a sequence of overflow destinations. Alternatively, you can configure T-Server to return calls automatically to the last distribution device.

Device-Specific Overrides

T-Server provides three configuration options with which you can configure device-specific overrides for individual devices. You set the values for these options on the Annex tab of the TServer section of the individual device in the Framework Configuration Layer. These are the options:

- nas-private
- no-answer-overflow
- no-answer-timeout

Extensions Attributes for Overrides for Individual Calls

For all of the No-Answer Supervision options, you can specify the corresponding Extensions attribute in TRequestRouteCall requests to override the configured value for individual calls. This method allows the no-answer behavior to be determined in a routing strategy. The following are the three Extensions attributes:

- NO_ANSWER_ACTION
- NO_ANSWER_OVERFLOW
- NO_ANSWER_TIMEOUT

See, the Using the Extensions Attribute topic for the descriptions of these Extensions attributes.

Handling of Work-Related Calls

If an agent that is handling a business call initiates a consultation call to another agent, or an agent who is in ACW state, makes a call to another agent, this is considered as a work-related call by T-Server. From the point of view of the No-Answer Supervision feature, T-Server treats work-related calls like private calls; that is, no-answer supervision is not activated for such calls.

If a work-related call passes a distribution point, T-Server promotes this call to business call status. In this case, no-answer supervision is applied when the call arrives at its destination.

Handling of Transfer Scenarios

If a consultation call arrives at a destination as a work-related call, T-Server does not start no-answer supervision for that call on that destination. However, if the transfer is completed, T-Server then starts no-answer supervision, as the call that is now ringing on the new destination is now a business call. T-Server provides the information about the no-answer profile that is applied (according to the configuration) using the standard Extensions attributes in EventPartyChanged.

Private Calls

You can also apply No-Answer Supervision to private calls, using the `nas-private` configuration option.

Note: This this option is set in the `TServer` section, it defines the default value for all private calls. However, you can also set a value for this option on the `Annex` tab of DNs of type `Extension` or `Agent Login` in a section that is called `TServer`. When the is set there, it overrides the default value for the specific DN.

Recall Scenarios

There are scenarios where a call that was already established can start to ring again on a device, therefore, no-answer supervision must be re-applied. In such scenarios, T-Server suppresses the new ringing event and keeps reporting the call as held. In this case there is no event for T-Server to notify clients about the no-answer supervision to be applied, so T-Server sends a private event to notify the client applications that no-answer supervision will be applied. As soon as the PBX reports a delivered-recall (or its equivalent), T-Server sends the following private events and provides the information about the no-answer supervision profile applied in the standard `Extensions` attributes, described in the table below:

No-Answer Supervision Private Events

Attribute	Value	Description
EventNumber	`500`	`EventRingback`—sent in response to the ringback occurring on the device with no-answer supervision.
ThisDN	Ringback DN	The DN of the device.
Extensions attribute key	`NO_ANSWER_TIMEOUT`	Present always. Provides the details of the no-answer overflow and the timeout to be applied.
Extensions attribute key	`NO_ANSWER_ACTION`	Present only if there is an agent logged in. Provides the details of the no-answer action to be applied.

There are cases where the PBX recalls a call back to a device that the call already left—many PBXs recall blind transferred calls back to the transferring device in case they were not answered on the transfer destination. In this case, T-Server report an `EventRinging` event, therefore, T-Server does not send a private event to the clients.

The `recall-no-answer-timeout` configuration option allows you to configure the No-Answer Supervision feature for recall scenarios.

Reporting

The `nas-indication` configuration option allows you to configure the reporting of the `Extensions` attributes related to the No-Answer Supervision feature for reporting scenarios.

Related Configuration Options

Enabling or Disabling the Agent No-Answer Supervision Feature

T-Server provides the following three configuration options for defining the behavior of the Agent No-Answer Supervision feature:

agent-no-answer-action

agent-no-answer-action

Default Value: none
Valid Values:

- none—T-Server takes no action on agents when calls are not answered.
- notready—T-Server sets agents NotReady when calls are not answered.
- logout—T-Server automatically logs out agents when calls are not answered.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines T-Server's default action if a logged-in agent (real or emulated) fails to answer a call within the time defined in agent-no-answer-timeout. See, the NO_ANSWER_ACTION Extensions attribute in the Using the Extensions Attribute section for more information about how this option is used.

Note: When you set a value for the no-answer-action option on the Annex tab of an Agent Login object in the Configuration Layer, that value overrides, for that agent, the value of the agent-no-answer-action option in the TServer section.

agent-no-answer-overflow

agent-no-answer-overflow

Default Value: No default value
Valid Values:

- none—T-Server does not attempt to overflow a call on an agent desktop when agent-no-answer-timeout expires. T-Server treats this value as the end of a list. Subsequent values are not executed.

- recall—T-Server returns the call to the last distribution device (the device reported in the ThisQueue attribute of the call) when agent-no-answer-timeout expires.
- release—T-Server releases the call.
- <number>—T-Server sends the call to the specified destination number.
- Any valid overflow destination—T-Server returns the call to the specified destination when agent-no-answer-timeout expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies a sequence of overflow destinations that T-Server attempts to overflow to when the time specified in the agent-no-answer-timeout option expires. T-Server attempts to overflow in the order specified in the list. If all overflow attempts fail, T-Server abandons the overflow. See also, NO_ANSWER_OVERFLOW Extensions attribute in the Using the Extensions Attribute section for more information about how this option is used.

If the list of overflow destinations contains the value recall and the call was not distributed, T-Server skips to the next destination in the list.

Note: When you set a value for the no-answer-overflow option on the Annex tab of an Agent Login object in the Configuration Layer, that value overrides, for that agent, the value of the agent-no-answer-overflow option in the TServer section.

agent-no-answer-timeout

agent-no-answer-timeout

Default Value: 15
Valid Value: Any integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the default time (in seconds) that T-Server allows for a logged-in agent (real or emulated) to answer a call before executing the actions defined in the agent-no-answer-overflow and agent-no-answer-action options. A value of 0 (zero) disables the Agent No-Answer Supervision feature. See also, the NO_ANSWER_TIMEOUT Extensions attribute in the Using the Extensions Attribute section for more information about how this option is used.

Notes:

- When you set a value for this option on the Annex tab of an Agent Login object in the Configuration Layer, that value overrides, for that agent, the value of this option set in the TServer section.
- Because this T-Server supports supervised routing, the value defined for option supervised-route-timeout overrides the value defined for agent-no-answer-timeout for supervised routed calls. If a call is delivered to a device using supervised routing, and the routing timeout expires, T-Server does not apply the specified no-answer overflow. If the call is routed to an agent, T-Server does apply the specified no-answer action after the supervised-routing timeout expires.

Enabling or Disabling the Agent No-Answer Supervision Feature for Devices of Type Extension

T-Server provides the following two configuration options for defining the behavior of No-Answer Supervision with devices of type Extension:

extn-no-answer-overflow

extn-no-answer-overflow

Default Value: No default value
Valid Values:

- none—T-Server does not attempt to overflow a call on an extension when the timeout value specified for the extn-no-answer-timeout configuration option expires. T-Server treats this value as the end of a list. Subsequent values are not executed.
- recall—T-Server returns the call to the last distribution device (the device reported in the ThisQueue attribute of the call) when the timeout value specified for the extn-no-answer-timeout configuration option expires.
- release—T-Server drops the call.
- Any valid overflow destination in a comma-seperated list—T-Server returns the call to the specified destination when the timeout value specified for the extn-no-answer-timeout configuration option expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies a sequence of overflow destinations that T-Server attempts to overflow to when the timeout value specified in the extn-no-answer-timeout option has expired.

T-Server attempts to overflow in the order specified in the list. If all overflow attempts fail, T-Server abandons the overflow. See, the NO_ANSWER_OVERFLOW Extensions attribute in the topic, Using the Extensions Attribute, for more information about how this option is used.

If the list of overflow destinations contains the value recall and the call was not distributed, T-Server skips to the next destination in the list.

Note: If you set a value for the no-answer-overflow option on the Annex tab of any Extension object in Configuration Manager, that value overrides, for that Extension, the value of extn-no-answer-overflow in the TServer section.

extn-no-answer-timeout

extn-no-answer-timeout

Default Value: 15
Valid Value: Any positive integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the default no-answer timeout (in seconds) that T-Server applies to any device of type Extension. When the timeout ends, T-Server executes the actions defined in the extn-no-answer-timeout option.

A value of 0 (zero) deactivates the no-answer supervision for devices of type Extension. See, the NO_ANSWER_TIMEOUT Extensions attribute in the topic, Using the Extensions Attribute, for more information about how this option is used.

Note: When you set a value for the no-answer-overflow option on the Annex tab of an Extension object in the Configuration Layer, that value overrides, for that Extension, the value of the extn-no-answer-overflow option set in the TServer section.

Enabling or Disabling the Agent No-Answer Supervision Feature for Devices of Type ACD Position

T-Server provides the following two configuration options for defining the behavior of No-Answer Supervision with devices of type ACD Position:

posn-no-answer-overflow

posn-no-answer-overflow

Default Value: No default value
Valid Values:

- none—T-Server does not attempt to overflow a call on an position when the timeout value specified for the posn-no-answer-timeout configuration option expires. T-Server treats this value as the end of a list. Subsequent values are not executed.
- recall—T-Server returns the call to the last distribution device (the device reported in the ThisQueue attribute of the call) when posn-no-answer-timeout expires.
- release—T-Server releases the call.
- Any valid overflow destination in a comma-seperated list—T-Server returns the call to the specified

destination when the timeout value specified for the extn-no-answer-timeout configuration option expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies a sequence of overflow destinations that T-Server attempts to overflow to when the timeout value specified in the extn-no-answer-timeout configuration option expires.

T-Server attempts to overflow in the order specified in the list. If all overflow attempts fail, T-Server abandons the overflow. See, the NO_ANSWER_OVERFLOW Extensions attribute in the topic, Using the Extensions Attribute, for more information.

If the list of overflow destinations contains the value, recall, and the call was not distributed, T-Server skips to the next destination in the list.

Note: If you set a value for the no-answer-overflow option on the Annex tab of any individual ACD Position object in Configuration Manager, that value overrides, for that ACD Position, the value of posn-no-answer-overflow in the TServer section.

posn-no-answer-timeout

posn-no-answer-timeout

Default Value: 15
Valid Value: Any positive integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the default no-answer timeout (in seconds) that T-Server applies to any device of type ACD Position. When the timeout ends, T-Server executes the actions defined in the posn-no-answer-timeout option.

A value of 0 (zero) deactivates the no-answer supervision for devices of type ACD Position. See, the NO_ANSWER_TIMEOUT Extensions attribute in the topic, Using the Extensions Attribute, for more information about how this option is used.

Note: When you set a value for the no-answer-overflow option on the Annex tab of an ACD Position object in Configuration Manager, that value overrides, for that ACD Position, the value of the posn-no-answer-overflow option set in the TServer section.

Enabling or Disabling the Agent No-Answer Supervision Feature for Device-Specific Overrides

T-Server provides the following three configuration options with which you can configure device-specific overrides for individual devices. You set the values for these options on the Annex tab of the TServer section of the individual device in the Configuration Layer:

nas-private

nas-private

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies whether No-Answer Supervision should be applied to private calls.

Note: When set in the TServer section, this option defines the default value for all private calls. However, you can also set a value for this option on the Annex tab of DNs of type Extension or Agent Login in the section called TServer. When this option is set there, this value overrides the default value for the specific DN.

no-answer-action

no-answer-action

Default Value: None
Valid Values:

- `none`—T-Server take no action on agents when business calls are not answered.
- `notready`—T-Server sets agents to NotReady when business calls are not answered.
- `logout`—T-Server automatically logs out agents when business calls are not answered.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

This option is defined in the Tserver section on the Annex tab of any Agent ID object in the configuration environment. The value set in the Annex tab is specific to this instance of an agent, and overrides the value for the same option set in the Options tab.

If an emulated or real PBX agent receives a T-Server business call and the agent fails to answer the

call within the time defined in the agent-no-answer-timeout option, the no-answer-action option determines the action T-Server performs on this agent.

Note: If a call is abandoned before one of the timeouts specified for the agent-no-answer-timeout, no-answer-timeout, or supervised-route-timeout expires (depending on which timer is applicable), T-Server performs no action on this agent.

no-answer-overflow

no-answer-overflow

Default Value: No default value
Valid Values:

- none—T-Server does not attempt to overflow a call on an agent desktop when agent-no-answer-timeout expires. T-Server treats this value as the end of a list. Subsequent values are not executed.
- recall—T-Server returns the call to the last distribution device (the device reported in the ThisQueue attribute of the call) when agent-no-answer-timeout expires.
- release—T-Server releases the call.
- default—T-Server stops execution of the current overflow sequence and continues with the T-Server default overflow sequence defined by the relevant overflow option in the mainTServer section.
- Any valid overflow destination—T-Server returns the call to the specified destination when agent-no-answer-timeout expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

The value of the option overrides any of the following T-Server configuration options set at the Application-level for the object where it has been set (depending on the type of configuration object):

- agent-no-answer-overflow, if defined for an Agent Login object.
- extn-no-answer-timeout, if defined for an Extension object.

T-Server attempts to apply the overflow in the order that is listed. If the first overflow destination fails, then T-Server attempts the next one in the list. If all overflow destinations in the list fail, then T-Server abandons overflow. If the list of overflow destinations contains the value recall and the call was not distributed, T-Server skips to the next destination in the list.

no-answer-timeout

no-answer-timeout

Default Value: Same as the value in the corresponding option set at the `Application`-level
Valid Value: Any integer from `0-600`
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time (in seconds) that T-Server waits for a call to be answered that is ringing on the device in question. When the timer expires, T-Server applies the appropriate overflow, and, in the case of agents, the appropriate `logout` or `NotReady` action.

A value of `0` (zero) deactivates the no-answer supervision for this device.

When set, this option overrides any of the following T-Server configuration options set at the `Application`-level for the object where it has been set (depending on type of configuration object):

- `agent-no-answer-timeout`, if defined for an `Agent Login` object.
- `extn-no-answer-timeout`, if defined for an `Extension` object.

recall-no-answer-timeout

recall-no-answer-timeout

Default Value: 15
Valid Values: Any positive integer from `0-600`
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time that T-Server waits for a call to re-appear on a device as a result of a recall—for example: a ringback waiting to be answered. When the timer expires, T-Server executes the actions defined by the relevant overflow option, as well as the action option for cases where an agent is logged in.

There is no No-Answer Supervision for such calls, if the value is set to `0` (zero).

This option can be defined either in the main `Tserver` section or in a section called `TServer` on the Annex tab of any of the following configuration object types in Configuration Manager:

- `Extension`
- `ACD Position`
- `Voice Treatment Port`
- `Agent Login`

Enabling or Disabling the Agent No-Answer Supervision Feature for Reporting

The `nas-indication` option enables or disables No-Answer Supervision for reporting:

nas-indication

Default Value: `none`
Valid Values:

- `none`—No `ReasonCode` attribute or `Extensions` attribute is provided in the `EventReleased` event.
- `ext`—The `NO_ANSWER_TIMEOUT` `Extensions` attribute is supplied in the `EventReleased` event.
- `rsn`—The `NO_ANSWER_TIMEOUT` `ReasonCode` attribute is supplied in the `EventReleased` event.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies the reporting action in the `EventReleased` event when No-Answer Supervision overflows a call. See, the `no-answer-timeout` option for more information.

Partitioned-Switch Configuration

There are no special configuration requirements to support partitioned-switch configuration on T-Server for CSTA Connector.

Request Handling Enhancements

T-Server has two enhancements to handle queues: request conflict resolution and a new device queue.

Requests submitted by different clients are treated no differently to requests submitted by the same client. For this reason, having multiple clients controlling the same device can result in unexpected behavior.

Note: While this configuration is supported, it should be recognized that there is no special handling for multiple clients.

Related Configuration Options

The following configuration options control the request handling enhancements:

call-rq-gap

call-rq-gap

Default Value: `250`
Valid Value: Any integer from `0-1000`
Changes Take Effect: Immediately

Specifies (in milliseconds) the length of delay applied to a request issued against a busy call (a call that has another request working on it already). This prevents race conditions on the different call legs.

Set the value of this option to a time longer than the usual response time for a request from the switch.

correct-connid

correct-connid

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

If the value of this option is set to `true`, T-Server corrects the wrong `ConnectionID` provided by the application in CTI requests. If the value of this option is set to `false,` this feature is disabled.

correct-rqid

correct-rqid

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

If the value of this option is set to `true,` T-Server corrects the wrong CTI client request. If the value of this option is set to `false`, this feature is disabled.

device-rq-gap

device-rq-gap

Default Value: `250`
Valid Value: Any integer from `0-1000`
Changes Take Effect: Immediately
Related Feature: Request Handling Enhancements

Specifies (in milliseconds) the length of delay applied to a request issued against a busy call (a call that has another request working on it already). This prevents race conditions on the different call legs.

Set the value of this option to a time longer than the usual response time for a request from the switch.

rq-conflict-check

rq-conflict-check

Default Value: `true`
Valid Value: `true`, `false`
Changes Take Effect: Immediately
Related Feature: Request Handling Enhancements

Specifies whether request conflict resolution is enabled. Request conflict resolution intelligently resolves any conflicting client requests.

Unregistered DNs

You can request registration on DNs that are not registered in the configuration environment. The Disconnect Detection Protocol (DDP) is designed to accept unknown switch-specific types that are configured in the configuration environment. You are able to override the default value for a switch-specific type by using the `SwitchSpecificType` key in the `Extensions` attribute provided in the `TRegisterAddress` request.

The `AttributeAddressType` in the `TRegisterAddress` request replaces the DN-specific information that is obtained from the configuration environment. If this DN-specific information is missing, T-Server uses the values taken from the configuration options or applies the default values where ever possible.

T-Server does not accept `TRegisterAddress` requests in the following scenarios:

- T-Server does not have enough information to create a DN and perform the registration with the PBX.
- There is a request for registration on a reserved DN.
- There is a request for registration on a device where the registration in Configuration Manager is disabled in the configuration environment.
- The PBX device is not compatible with the device type requested for registration.

T-Server initiates the DN registration procedure on the PBX level after accepting the `TRegisterAddress` request from the first client on that DN when the PBX communication protocol requires this type of registration. The registration procedure at the PBX level could include following steps:

1. Monitor requests on a specified DN
2. Snapshot calls on the DN
3. Query device features on DN

Consecutive `TRegisterAddress` requests for the same DN do not re-initiate the registration procedure.

Supported Configuration

The following table displays the supported set of device types that are not configured in the Configuration Layer, but that T-Server can register by using the `AttributeAddressType` `Extensions` attribute from the client's `TRegisterAddress` request:

Supported T-Library Device Types in Client Requests

T-Library Type	Configuration Layer Device Type
AddressTypeDN	Extension

AddressTypeQueue	ACD Queue
AddressTypeRouteDN	Routing Point
AddressTypeRouteQueue	Routing Queue

Unsupported `AddressType` values received by T-Server in `TRegisterAddress` requests are processed in the same way as `TRegisterAddress` requests with the value of the `AttributeControlMode` `Extensions` attribute equal (`=`) to `RegisterLocal`.

Related Configuration Options

The following configuration options control the unregistered DNs:

accept-dn-type

accept-dn-type

Default Value: `+acdqueue +announcement +data +extension +position +routedn +routequeue +trunk +voicemail`
Valid Values:
`+/-acdqueue`—Accepts or rejects registration on DN of type `ACD Queue` (`AddressTypeQueue`)
`+/-announcement`—Accepts or rejects registration on DN of type `Music Port` (`AddressTypeAnnouncement`)
`+/-data`—Accepts or rejects registration on DN of type `Modem` (`AddressTypeDataChannel`)
`+/-extension`—Accepts or rejects registration on DN of type `Extension` (`AddressTypeDN`)
`+/-position`—Accepts or rejects registration on DN of type `Position` (`AddressTypePosition`)
`+/-routedn`—Accepts or rejects registration on DN of type `Routing Point` (`AddressTypeRouteDN`)
`+/-routequeue`—Accepts or rejects registration on DN of type `Route Queue` (`AddressTypeRouteQueue`)
`+/-trunk`—Accepts or rejects registration on DN of type `trunk` or `tie line` (`AddressTypeTrunk`)
`+/-voicemail`—Accepts or rejects registration on DN of type `Voice Mail` (`AddressTypeVoiceChannel`)
Changes Take Effect: Immediately

Defines the supported set of device types that are not configured in the Configuration Layer, but that T-Server can register.

Note: All possible values are listed here, however, this set is T-Server specific.

acd-position

acd-position

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `ACD Position` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `ACD Position` (`AddressTypePosition`) that are not configured in the Configuration Layer.

acd-queue

acd-queue

Default Value: 0 (zero)
Valid Value: Switch-specific types for DN of type ACD Queue supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type ACD Queue (AddressTypeQueue) that are not configured in the Configuration Layer.

data

data

Default Value: 0 (zero)
Valid Value: Switch-specific types for DN of type Data Channel (Modem in the configuration environment) supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type Modem (AddressTypeDataChannel) that are not configured in the Configuration Layer.

default-dn-type

default-dn-type

Default Value: none, extension, position
Valid Values:

- acdqueue—T-Server uses the AddressTypeQueue value
- announcement—T-Server uses the AddressTypeAnnouncement value
- data—T-Server uses the AddressTypeDataChannel value
- extension—T-Server uses the AddressTypeDN value
- none—T-Server assigns the DN type using the PBX-provided information
- position—T-Server uses the AddressTypePosition value
- trunk—T-Server uses the AddressTypeTrunk value

- voicemail—T-Server uses the AddressTypeVoiceChannel value

Changes Take Effect: Immediately

Defines the value that T-Server applies for the AttributeAddressType attribute when the client does not provide it or provides the value, AddressTypeUnknown, instead.

Note: All possible values are listed here, however, this set is T-Server specific.

dn-del-mode

dn-del-mode

Default Value:idle
Valid Values: never, idle, force, Timeout Value Format

- never—T-Server does not unregister the DN with the PBX and the device-related information is never deleted from the T-Server memory.
- idle—T-Server unregisters the DN with the PBX and the device-related information is deleted from the T-Server memory as soon as there are no more calls on this device.
- force—T-Server unregisters the DN with the PBX and the device-related information is deleted from the T-Server memory regardless of whether any calls exist on that DN.
- Timeout Value Format—T-Server applies a defined delay before unregistering the DN after the last call has left that DN. The valid value, idle is equivalent to setting the Timeout Value to 0 (zero).

Changes Take Effect: Immediately

Defines how T-Server handles device and device-related information when the DN is not configured in the Configuration Layer and there are no clients registered on that DN.

extension

extension

Default Value: 0 (zero)
Valid Value: Switch-specific types for DN of type Extension supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type Extension (AddressTypeDN) that are not configured in the Configuration Layer.

music

music

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Music Port` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Music Port` (`AddressTypeAnnouncement`) that are not configured in the Configuration Layer.

reg-delay

reg-delay

Default Value: `1000` milliseconds
Valid Values: `0-5000`
Changes Take Effect: Immediately

Defines the time (in milliseconds) that T-Server waits for the `DN Created` notification from Configuration Server before it starts processing the registration request from the client as a request for a DN not configured in the Configuration Layer.

reg-silent

reg-silent

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

- If this option is set to a value of `true`, T-Server reports `EventRegistered` for *on-demand* registration with the PBX when the procedure is completed.
- If this option is set to a value of `false`, T-Server reports `EventRegistered` as early as possible during the PBX registration procedure.

routing-point

routing-point

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Routing Point` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Routing Point` (`AddressTypeRouteDN`) that are not configured in the Configuration Layer.

routing-queue

routing-queue

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Routing Queue` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Routing Queue` (`AddressTypeRouteQueue`) that are not configured in the Configuration Layer.

trunk

trunk

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Routing Point` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Trunk` or `Tie Line` (`AddressTypeTrunk`) that are not configured in the Configuration Layer.

voicemail

voicemail

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Voice Mail` supported by T-Server

Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Voice Mail` (`AddressTypeVoiceChannel`) that are not configured in the Configuration Layer.

T-Library Support

The following topics describe the T-Library functionality supported by T-Server for CSTA Connector:

About Private Services and Events

Find out about the private services and events.

Private Services and Events

About Smart OtherDN Handling

Find out about the Smart OtherDN Handling feature.

Smart OtherDN Handling

About T-Library Functionality

Find out about the T-Library Functionality.

T-Library Functionality

About User Data Keys

Find out about the User Data Keys.

[[CSTADataKey|User Data Keys]

About Using the Extensions Attribute

Find out about the Using the Extensions Attribute.

Using the Extensions Attribute

Private Services and Events

The following tables represent describe the private services and events for different supported features:

Account Codes

Account Codes

Service	Attribute	Value	Description
Set Account Code	Event Number	501	The account code set on the device.
	ThisDN	This device.	
	ConnID	Connection ID of the call.	
	PrivateID	0 (zero)	
	Extensions attribute	Must have a key name defined by the accode-name option.	

Call Recording

Call Recording

Private Services

Service	Attribute	Value	Description
Initiate a call recording	Service Number	3013	Initiates a call recording (CSTA Record)
	ThisDN	Device requested to start the call recording	
	Connection ID	Connection ID of the call to be recorded	
	Extensions attribute key	None	
Stop a call recording	Service Number	3014	Stops a call recording when the call recording is active on the DN (CSTA Stop)
	ThisDN	Device requested to stop the call recording	

Service	Attribute	Value	Description
	Connection ID	Connection ID of the recorded call	
	`Extensions` attribute key	None	
Suspend a call recording	Service Number	`3015`	Suspend a call recording when the call recording is active on a DN (CSTA Suspend)
	`ThisDN`	Device requested to suspend the call recording	
	Connection ID	Connection ID of the recorded call	
	`Extensions` attribute key	None	
Resume a call recording	Service Number	`3016`	Resumes a call recording when the call recording is suspended on a DN (CSTA Resume)
	`ThisDN`	Device requested to resume the call	

Service	Attribute	Value	Description
		recording	
	Connection ID	Connection ID of the recorded call	
	Extensions attribute key	None	

Private Events

Service	Attribute	Value	Description
Start a private event call recording	Event Number	3013	Private event call record started
	ThisDN	Monitored DN	
	Connection ID	Connection ID of the call that finished recording	
	Extensions attribute key	None	
Stop a private event call recording	Service Number	3014	Private event call recording stopped

Service	Attribute	Value	Description
	ThisDN	Monitored DN	
	Connection ID	Connection ID of the call that finished recording	
	Extensions attribute key	None	
Suspend a private event call recording	Service Number	3015	Private event call recording suspended
	ThisDN	Monitored DN	
	Connection ID	Connection ID of the recorded call	
	Extensions attribute key	None	
Resume a private event call recording	Service Number	3016	Private event call recording suspended
	ThisDN	Monitored DN	
	Connection ID	Connection ID of	

Service	Attribute	Value	Description
		the recorded call	
	Extensions attribute key	None	

Hot Desking

Hot Desking

Private Services

Service	Attribute	Value	Description
Initiate hot-desking	Service Number	1	Specifies the host device number as an HOST_DN Extensions attribute. T-Server sends a corresponding EventPrivateInfo message when the association is successfully performed. If the association is already present, or cannot be performed, T-Server distributes an EventError message instead.

Service	Attribute	Value	Description
	ThisDN	guest extension	
	Extension Attribute Key	HOST_DN	A string value that identifies the host DN. Associates the guest extension with a host device.
	Connector Function	escapeService / guestAssociatedExtension	CSTA Genesys specific private service
Cancel hot-desking	Service Number	2	T-Server sends the corresponding EventPrivateInfo event when the de-association is successfully performed. If an association is not present, or the de-association cannot be performed, T-Server distributes an EventError message.
	ThisDN	guest extension	De-associates the guest extension with the host device.

Service	Attribute	Value	Description
	Connector Function	`escapeService` / `guestAssociatedExtension`	CSTA Genesys specific private event.

Private Events

Event	Attribute	Value	Description
Hot-desking established	Event Number	1	Successful association between guest and host device was established. T-Server sends corresponding `EventPrivateInfo` when de-association occurs.
	`ThisDN`	guest extension	
	`OtherDN`	host extension	Host associated with the guest extension
	`AttributePrivateMsgID`	1	
	Connector Function	`privateEvent` / `guestAssociatedEvent`	CSTA Genesys specific private event

Event	Attribute	Value	Description
Hot-desking cancelled	Event Number	2	Association between guest and host device was terminated.
	`ThisDN`	guest extension	
	`OtherDN`	host extension	Host (if known) that was associated with the guest extension.
	`AttributePrivateMsgID`	2	
	Connector Function	`privateEvent / guestAssociatedEvent`	CSTA Genesys specific private event.

Smart OtherDN Handling

For T-Server clients that provide the Agent ID value as the OtherDN attribute in requests to T-Server, T-Server can convert this OtherDN value using its knowledge of the association between the Agent ID and the DN to ensure the correct execution of the request by the switch. For switches expecting an Agent ID in the place of a DN for a particular operation, T-Server can convert the OtherDN value supplied by client to the Agent ID value that the switch expects.

Note: The Extensions attribute key, ConvertOtherDN, is also provided to enable this feature to be applied on a call-by-call basis.

Supported Requests

The following table shows the requests that assume the use of the OtherDN value as a switch directory number, and can therefore support the Smart OtherDN Handling feature.

Requests That Support Smart OtherDN Handling

TRequest	Meaning of OtherDN Attribute	AgentID-to-DN Conversion	Reserved DN Conversion
TMakeCall	Call destination	Yes	Yes
TMakePredictiveCall <ref>TMakePredictiveCall assumes that the directory number should be outside the switch; however, this request could also support Smart OtherDN Handling.</ref>	Call destination	Yes	Yes
TRedirectCall	New destination for call	Yes	Yes
TInitiateTransfer	Call destination	Yes	Yes
TMuteTransfer	Call destination	Yes	Yes
TSingleStepTransfer	New destination	No	No
TInitiateConference	Call destination	Yes	Yes
TSingleStepConference	New destination for call	Yes	Yes

TRequest	Meaning of OtherDN Attribute	AgentID-to-DN Conversion	Reserved DN Conversion
TDeleteFromConference	Conference member to be deleted	Yes	Yes
TListenDisconnect	Request target	Yes	Yes
TListenReconnect	Request target	Yes	Yes
TCallSetForward	Request target	Yes	Yes
TGetAccessNumber <ref>T-Server cannot intercept these requests.</ref>	DN for which Access Number is requested	No	No
TSetCallAttributes <ref name="OtherDN">Only the listed route types are applicable for OtherDN conversion.</ref>	Not specified	No	No
TReserveAgentAndGetAccessNumber <ref name="OtherDN" />	DN for which Access Number is requested	No	No
TMonitorNextCall	Agent DN to be monitored	Yes	Not applicable
TCancelMonitoring	Agent DN that was monitored	Yes	Not applicable
TRouteCall <ref name="OtherDN" />	New destination for call		
* RouteTypeUnknown		Yes	Yes
* RouteTypeDefault		Yes	Yes
* RouteTypeOverwriteDNIS		Yes	Yes
* RouteTypeAgentID		Yes	Yes

<references/>

Related Configuration Options

The following configuration option supports the Smart OtherDN Handling feature:

convert-other-dn

convert-otherdn

Default Value: `+agentid +reserveddn +fwd`
Valid Values:

- `+/-agentid`—Turns on/off either the conversion of the `Agent ID` value provided in the `OtherDN` attribute to the DN associated with this Agent, or the DN value to `Agent ID` value (where appropriate).
- `+/-reserveddn`—Turns on/off the conversion of the `OtherDN` attribute for reserved DNs.
- `+/-fwd`—Turns on/off conversion of the `OtherDN` attribute in the `TSetCallForward` request.

Changes Take Effect: Immediately
Related Feature: Smart OtherDN Handling

Defines whether T-Server has to convert, if applicable, the value provided in the request's `AttributeOtherDN` attribute.

dn-for-undesired-calls

dn-for-undesired-calls

Default Value: No default value
Valid Values: Any valid switch DN
Changes Take Effect: Immediately
Related Feature: Smart OtherDN Handling

Specifies the DN that T-Server uses as the request destination if the client provides a reserved DN in the request.

Note: You can set a value for this option in the appropriate DN Annex tab in the `TServer` section. When set there, this value overrides the default value for the DN.

T-Library Functionality

The following table presents T-Library functionality supported in T-Server for Connector. The table entries use these notations:

- N—Not supported
- Y—Supported
- I—Supported, but reserved for Genesys Engineering
- E—Event only supported

This table reflects only the switch functionality used by Genesys software and might not include the complete set of events offered by the switch.

Note: Refer to the BroadWorks Connector Interoperability topic for the switch functionality supported by T-Server for CSTA Connector.

When a set of events is sent in response to a single request, the events are listed in an arbitrary order. An asterisk (*) indicates the event that contains the same Reference ID as the request. For more information, refer to the *Genesys Events and Models Reference Manual* and the *Platform SDK 8 .NET (or Java) API Reference*.

Certain requests in the table are reserved for Genesys Engineering and are listed here merely for completeness of information.

Notes describing specific functionality appear at the end of the table.

Supported T-Library Functionality

Feature Request	Request Subtype	Corresponding Event(s)	Supported
General Requests			
TOpenServer		EventServerConnected	Y
TOpenServerEx		EventServerConnected	Y
TCloseServer		EventServerDisconnected	Y
TSetInputMask		EventACK	Y
TDispatch		Not Applicable	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TScanServer		Not Applicable	Y
TScanServerEx		Not Applicable	Y
Registration Requests			
TRegisterAddress <ref>Every configured device is monitored as soon as the connection with the switch is established. Extensions are monitored by using the MonitorDeviceCalls (telephony events) and MonitorACDFeatures (agent states) functionality. Routing Points are monitored by using MonitorDevice and ACD Queues by using MonitorQueue.</ref>		EventRegistered	Y
TUnregisterAddress		EventUnregistered	Y
Call-Handling Requests			
TMakeCall <ref>Functions on digital phones without any human intervention.</ref>	Regular	EventDialing	Y
	DirectAgent		N
	SupervisorAssist		N
	Priority		N
	DirectPriority		N
TAnswerCall <ref>This function is not available for analog phones (Extension type 2).</ref>		EventEstablished	Y
TReleaseCall		EventReleased	Y
TClearCall		EventReleased	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
THoldCall		EventHeld	Y
TRetrieveCall		EventRetrieved	Y
TRedirectCall		EventReleased	Y
TMakePredictiveCall		EventDialing*, EventQueued	Y
Transfer/Conference Requests			
TInitiateTransfer		EventHeld, EventDialing*	Y
TCompleteTransfer		EventReleased*, EventReleased	Y
TInitiateConference		EventHeld, EventDialing*	Y
TCompleteConference <ref>Only three-party conferences are supported.</ref>		EventReleased*, EventRetrieved, EventPartyAdded	Y
TDeleteFromConference		EventPartyDeleted*, EventReleased	Y
TReconnectCall		EventReleased, EventRetrieved*	Y
TAlternateCall		EventHeld*, EventRetrieved	Y
TMergeCalls	ForTransfer	EventReleased*, EventPartyChanged	N
	ForConference	EventReleased*, EventRetrieved, EventPartyChanged, EventPartyAdded	N
TMuteTransfer		EventHeld, EventDialing*, EventReleased, EventReleased	Y
TSingleStepTransfer		EventReleased*,	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
		EventPartyChanged	
TSingleStepConference		EventRinging*, EventEstablished	N
Call-Routing Requests			
TRouteCall	Unknown	EventRouteUsed	Y
	Default		Y
	Label		N
	OverwriteDNIS		Y
	DDD		Y
	IDDD		Y
	Direct		N
	Reject		Y
	Announcement		N
	PostFeature		N
	DirectAgent		N
	Priority		N
	DirectPriority		N
	AgentID		N
	CallDisconnect		Y
Call-Treatment Request			

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TApplyTreatment	Unknown	(EventTreatmentApplied + EventTreatmentEnd)/EventTreatmentNotApplied	N
	IVR		N
	Music		Y
	RingBack		Y
	Silence		Y
	Busy		Y
	CollectDigits		Y
	PlayAnnouncement		Y
	PlayAnnouncementAndDigits		Y
	VerifyDigits		N
	RecordUserAnnouncement		N
	DeleteUserAnnouncement		N
	CancelCall		Y
	PlayApplication		N
	SetDefaultRoute		N
	TextToSpeech		N
	TextToSpeechAndDigits		N
	FastBusy		N
	RAN		N

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TGiveMusicTreatment		EventTreatmentApplied	Y
TGiveRingBackTreatment		EventTreatmentApplied	Y
TGiveSilenceTreatment		EventTreatmentApplied	Y
DTMF (Dual-Tone Multifrequency) Requests			
TCollectDigits		EventDigitsCollected	Y
TSendDTMF		EventDTMFSent	Y
Voice-Mail Requests			
TOpenVoiceFile		EventVoiceFileOpened	N
TCloseVoiceFile		EventVoiceFileClosed	N
TLoginMailBox		EventMailBoxLogin	N
TLogoutMailBox		EventMailBoxLogout	N
TPlayVoice		EventVoiceFileEndPlay	N
Agent & DN Feature Requests			
TAgentLogin	WorkModeUnknown	EventAgentLogin	Y
	ManualIn <ref>If a queue is configured with the WK (work mode) parameter, the agent state is NotReady after login.</ref>		Y
	AutoIn <ref>If a queue is configured with the WK (work mode) parameter, the agent state is Ready after login. However, you can set the agent state to NotReady.</ref>		Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
	AfterCallWork <ref>After an ACD call, an agent is automatically put into the AfterCallWork state.</ref>		Y
	AuxWork		Y
	WalkAway		Y
	ReturnBack		Y
	NoCallDisconnect		Y
TAgentLogout		EventAgentLogout	Y
TAgentSetIdleReason		EventAgentIdleReasonSet	N
TAgentSetReady <ref>Functions only if the queue is configured with the WK (work mode) parameter.</ref>		EventAgentReady	Y
TAgentSetNotReady	WorkModeUnknown	EventAgentNotReady	Y
	ManualIn		Y
	AutoIn		Y
	AfterCallWork		Y
	AuxWork		Y
	WalkAway		Y
	ReturnBack		Y
	NoCallDisconnect		Y
TMonitorNextCall	OneCall	EventMonitoringNextCall	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
	AllCalls		Y
TCancelMonitoring		EventMonitoringCanceled	Y
TCallSetForward	None	EventForwardSet	Y
	Unconditional		Y
	OnBusy		Y
	OnNoAnswer		Y
	OnBusyAndNoAnswer		N
	SendAllCalls		N
TCallCancelForward	None	EventForwardCancel	Y
	Unconditional		Y
	OnBusy		Y
	OnNoAnswer		Y
	OnBusyAndNoAnswer		N
	SendAllCalls		N
TSetMuteOff		EventMuteOff	N
TSetMuteOn		EventMuteOn	N
TListenDisconnect		EventListenDisconnected	N
TListenReconnect		EventListenReconnected	N
TSetDNDOn		EventDNDOn	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TSetDNDOff		EventDNDOff	Y
TSetMessageWaitingOn		EventMessageWaitingOn	N
TSetMessageWaitingOff		EventMessageWaitingOff	N
Query Requests			
TQuerySwitch	DateTime	EventSwitchInfo	N
	ClassifierStat		N
TQueryCall	PartiesQuery	EventPartyInfo	Y
	StatusQuery		N
TQueryAddress	AddressStatus	EventAddressInfo	Y
	MessageWaitingStatus		N
	AssociationStatus		N
	CallForwardingStatus		Y
	AgentStatus		Y
	NumberOfAgentsInQueue <ref>Only on the Agent Group, not the queue.</ref>		Y
	NumberOfAvailableAgentsInQueue <ref>Only on the Agent Group, not the queue. Ready/ Not Ready only.</ref>		Y
	NumberOfCallsInQueue <ref>Only on the queue, not on the Agent Group.</ref>		Y
	AddressType		Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
	CallsQuery		Y
	SendAllCallsStatus		N
	QueueLoginAudit		Y
	NumberOfIdleTrunks		N
	NumberOfTrunksInUse		N
	DatabaseValue		N
	DNStatus		Y
	QueueStatus		Y
TQueryLocation	AllLocations	EventLocationInfo	I
	LocationData		I
	MonitorLocation		I
	CancelMonitorLocation		I
	MonitorAllLocations		I
	CancelMonitorAllLocations		I
	LocationMonitorCanceled		I
	AllLocationsMonitorCanceled		I
TQueryServer		EventServerInfo	Y
User-Data Requests			
TAttachUserData		EventAttachedDataChanged	Y

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TUpdateUserData		EventAttachedDataChanged	Y
TDeleteUserData		EventAttachedDataChanged	Y
TDeleteAllUserData		EventAttachedDataChanged	Y
ISCC (Inter Server Call Control) Requests			
TGetAccessNumber		EventAnswerAccessNumber	Y
TCancelReqGetAccessNumber		EventReqGetAccessNumberCanceled	Y
Special Requests			
TReserveAgent		EventAgentReserved	I
TSendEvent		EventACK	I
TSendEventEx		EventACK	I
TSetCallAttributes		EventCallInfoChanged	Y
TSendUserEvent		EventACK	Y
TPrivateService		EventPrivateInfo	Y
Network Requests			
TNetworkConsult		EventNetworkCallStatus	N
TNetworkAlternate		EventNetworkCallStatus	N
TNetworkTransfer		EventNetworkCallStatus	N
TNetworkMerge		EventNetworkCallStatus	N
TNetworkReconnect		EventNetworkCallStatus	N

Feature Request	Request Subtype	Corresponding Event(s)	Supported
TNetworkSingleStepTransfer		EventNetworkCallStatus	N
TNetworkPrivateService		EventNetworkPrivateInfo	N

<references/>

Note: The footnote functionality is not working properly.

User Data Keys

T-Server supports the use of the `User Data` keys in the following table:

Describing the User Data Keys

Extension		Used In	Description
Key	**Type**		

`ACCOUNT_CODE`	string
	integer
		`TAttachUserData`
		`TUpdateUserData`
		`EventUserDataChanged`
			Alternative to the `ACCOUNT_CODE_<N>` key. The name of this extension is defined by the accode-name configuration option.

`LegalGuardTime`	integer	Call-related requests	Specifies the amount of emulated Legal Guard time allocated to the agent at the end of a business call.
`RecordingState`	string	`EventRegistered` `EventAddressInfo`	Provides the status of the Call Recording feature for the DN. The status can be one of following values: • `1 Started` • `2 Stopped` • `3 Suspended` (currently reserved)
`WrapUpTime`	integer	Call-related requests	Specifies the amount of emulated wrap-up time allocated to all agents at the end of the business call. This value is effective for the duration of this agent's login session.

Using the Extensions Attribute

T-Server supports the use of the Extensions attribute as documented in the *Genesys Events and Models Reference Manual* and the *Platform SDK 8 .NET (or Java) API Reference*.

Additionally, the Extensions described in the following table are also supported.

Use of the Extensions Attribute

Extension		Used In	Description
Key	**Type**		
ACCOUNT_CODE	string or integer	TPrivateService EventPrivateInfo	The requested or reported account code. The key name of this Extensions attribute is defined by the accode-name configuration option.
ReasonCode	string or integer	TAgentNotReady EventAgentNotReady	When an account code is used as a Walk-Away code, this Extensions attribute specifies the requested or reported account code while the agent is in NotReady state. The default method of reporting the Not Ready activation information.
NO_ANSWER_TIMEOUT	string	TRouteCall	If set, the value of this Extensions attribute overrides any value set in any of the following configuration options for the current call: • no-answer-timeout • agent-no-answer-timeout • extn-no-answer-timeout
NO_ANSWER_ACTION	string	TRouteCall	If set, the value of this Extensions attribute overrides any value set in any of the following configuration options for the current call: • no-answer-action • agent-no-answer-

Extension		Used In	Description
			action
NO_ANSWER_OVERFLOW	comma-separated list	TRouteCall	If set, the value of this Extensions attribute overrides any value set in any of the following configuration options for the current call: • no-answer-overflow • agent-no-answer-overflow • extn-no-answer-overflow
SUPERVISED_ROUTE	string	TRouteCall	Overrides the value in the supervised-route-timeout configuration option for individual calls.
ConvertOtherDN	string or integer	See Smart OtherDN Handling.	• A value of 0 (zero) disables all conversions for the call. • A value of 1 forces the relevant conversion for the call.
EmulateLogin	string	TAgentLogin	• If this option is set to a value of yes, T-Server performs an emulated login. • If this option is set to a value of no, T-Server attempt a real login.
	string	EventAgentLogin EventAddressInfo EventRegistered	If this option is set to a value of yes, it indicates that the T-Server has performed an emulated login.
WrapUpTime	integer	TAgentLogin	Specifies the amount of emulated wrap-up time (in seconds) allocated to this agent at the end of a business call. This value is effective for the duration of this login's

Extension		Used In	Description
			agent session. It can be overridden by the value in the `WrapUpTime` `Extensions` attribute in the `TAgentNotReady` request.
	integer	`TAgentNotReady` with work mode = 3	Specifies the amount of emulated wrap-up time (in seconds) allocated to this agent at the end of a business call. This value is effective only for the lifespan of this request.
	integer	`EventAgentNotReady` `EventAgentReady` `EventEstablished`	Indicates the amount of emulated wrap-up time (in seconds) allocated to this agent at the end of a business call.
BusinessCall	integer	Call-related events	Specifies the business type of a call. Valid values are: • `0`/`private`—Private call • `1`/`business`—Business call • `2`/`work`—Work-related call
BusinessCallType	string or integer	`TMakeCall` `TInitiateTransfer` `TMuteTransfer` `TInitiateConference` `TMakePredictiveCall` `TAnswerCall`	Specifies the call business type to be used by T-Server for the new call or the answering party. Valid values are: • `0`/`private`—Private call • `1`/`business`—Business call • `2`/`work`—Work-related call
AgentLogoutOnUnregister	string	`TAgentLogin` `TRegisterAddress`	Specifies whether T-Server performs an automatic logout of an agent whenever their client application unregisters its DN from T-Server. Valid values are: • `true`—T-Server logs out emulated and

Extension		Used In	Description
			native agents on unregister • `false`—T-Server does not logout emulated or native agents on unregister • `emu-only`—T-Server logs out emulated agents only on unregister
AssociateClientWithLogin	boolean	`TAgentLogin` `TRegisterAddress`	Specifies whether the client should be associated with the agent session.
	boolean	`EventAgentLogin` `EventRegistered` `EventPrivateInfo`	Specifies that the client has been associated with the agent session.
AgentEmuLoginOnCall	boolean	`TAgentLogin` `TAgentLogout`	Specifies whether T-Server allows an emulated agent login or logout from a device where there is a call in progress.
LegalGuardTime	integer	`TAgentLogin`	Specifies the amount of emulated legal guard time allocated to an agent at the end of a business call.
SyncEmuACW	integer	`TAgentLogin`	Specifies whether T-Server synchronizes emulated ACW and/or legal guard with the switch for native agents.
ReleasingParty	string	`EventReleased` `EventAbandoned`	Identifies which party was the initiator of the call release. Possible values are: • 1—Local • 2—Remote • 3—Unknown
LinkLoad	string	`EventRouteRequest`	A value of1 High indicates that T-Server is in a high watermark condition. The feature is disabled if the value of the use-link-bandwidth option is set to `0` (zero). Possible values are:

Extension		Used In	Description
			• 0—OK • 1—High
Association	string	TRegisterAddress	Specifies the association that T-Server uses when a created DN is not specified in the configuration environment. T-Server uses the value of none (an empty string) when the Extensions attribute is not provided.
SwitchSpecificType	string or integer	TRegisterAddress	Specifies the switch-specific type that T-Server uses when a created DN is not specified in the configuration environment. T-Server verifies the combination switch device type/switch-specific type in the same manner as for a DN that is configured in the configuration environment. **Note:** The Disconnect Detection Protocol (DDP) is designed usually to accept unknown switch-specific types that are configured in the configuration environment by processing that type as type 0 (zero). An unknown switch-specific type for the T-Server value in the SwitchSpecificType Extensions attribute key is processed in the same way.
sdn-licenses-in-use	integer	EventServerInfo	Specifies how many SDN licenses are currently in use.
sdn-licenses-available	integer		Specifies how many SDN licenses are currently available.
PICKUP	string	TMakeCall	The value of the PICKUP Extensions attribute can be anything. If the Extensions attribute is present in the TMakeCall request, T-Server picks up the call ringing on the device specified by OtherDN attribute in the request.
ASSIST	string	TInitiateConferece TInitiiateTransfer	The value of the ASSIST Extensions attribute can be anything. An agent can add a supervisor to a call in order to

Extension		Used In	Description
			receive assistance by passing the ASSIST Extensions attribute in either of the TInitiateConference or TInitiateTransfer requests and specifying the supervisor's device as an OtherDN in the request.
INTRUDE	string	TSingleStepConference	The value of the INTRUDE Extensions attribute can be anything. A device can intrude on a call on another device by passing the INTRUDE Extensions attribute in a TSingleStepConference request and specifying in the OtherDN attribute the device with the call to be intruded on.
OrigSV-n, NumOfOrigSVs	string	EventPartyChanged, EventPartyAdded	Indicates the supervisors monitoring the main call in a transfer/conference scenario. The NumOfOrigSVs Extensions attribute indicates the number of supervisors listening to the main call.
ConsultSV-n, NumOfConsultSVs	string	EventPartyChanged, EventPartyAdded	Indicates the supervisors monitoring the consultation call in a transfer/conference scenario. The NumOfConsultSVs Extensions attribute indicates the number of supervisors listening to the consultation call.
ReleaseController	string or integer	TReleaseCall (CSTA Clear Connection)	Allows overriding the settings of the enable-controller-release configuration option. • 0 (zero)—Corresponds to the option value false. • A positive integer—Corresponds to the option value true.
RPDistributeType	string (BWDistribute, BWTransfer)	TRoutePointDistributeCall	Specifies the method for routing from a Routing Point. If this Extensions attribute has a value of BWDistribute, that is supplied by T-Server, CSTA Connector uses a

Extension		Used In	Description
			`TPointDistributeCall` request as the preferred method for routing from a Routing Point. A value of `BWTransfer` instructs CSTA Connector to use the blind transfer method for routing. Any other values for this `Extensions` attribute are ignored. See the enable-rp-distribute configuration option for more information.

Configuration Options

You must configure the configuration objects and options described in the topics below in the Framework Configuration Layer:

About Common Configuration Options

Find out about the configuration options that are common to all Genesys server applications.

Common Configuration Options

About T-Server Common Configuration Options

Find out about the configuration options that are generally common to all T-Server types.

T-Server Common Configuration Options

About T-Server Specific Configuration Options

Find out how the T-Server components and applications works.

T-Server Specific Configuration Options

Common Configuration Options

Unless otherwise noted, the common configuration options that this section describes are common to all Genesys server applications and are applicable to any Framework server component. This section includes the following topics:

Setting Common Configuration Options

Unless otherwise specified, set the common configuration options in the `Options` section of the `Application` object, using one of the following navigation paths:

- In Genesys Administrator `Application` object > `Options` tab > `Advanced` view (`Options`)
- In Configuration Manager `Application` object > `Properties` dialog box > `Options` tab

Warning: Configuration sections names, configuration option names, and predefined option values are case-sensitive. Enter these option names and values in Genesys Administrator or Configuration Manager exactly as they are documented in the following topics.

Mandatory Options

You do not have to configure any common options to start any Server applications.

Timeout Value Format

The Timeout Value Format describes the values to use for those T-Server common options that set various timeouts. The current format allows you to use fractional values and various time units for timeout settings.

For timeout-related options, you can specify any value that represents a time interval, provided that it is specified in one of the following formats:

[[[*hours*:]*minutes*:]*seconds*][*milliseconds*]

or

[*hours* `hr`][*minutes* `min`][*seconds* `sec`][*milliseconds* `msec`]

A time unit name in italics (for example, *hours*) that is specified in the example above, should be replaced by an integer value for that time unit.

Integer values with no measuring units are still supported to keep compatibility with the previous releases of T-Server. If you do not specify any measuring units, the units of the default value apply. For example, if the default value equals `60 seconds`, specifying the value of `30` sets the option to 30 seconds.

Example 1

The following settings result in a value of 1 second, 250 milliseconds:

```
sync-reconnect-tout = 1.25sync-reconnect-tout = 1 sec 250 msec
```

Example 2

The following settings result in a value of 1 minute, 30 seconds:

```
timeout = 1:30timeout = 1 min 30 sec
```

common Section

This section must be called `common`.

enable-async-dns

enable-async-dns

Default Value: `off`
Valid Values:

`off`	Disables asynchronous processing of DNS requests.
on	Enables asynchronous processing of DNS requests.

Changes Take Effect: Immediately

Enables the asynchronous processing of DNS requests such as, for example, host-name resolution.

Warning: Use this option only when requested by Genesys Technical Support. Use this option only with T-Servers.

rebind-delay

rebind-delay

Default Value: `10`
Valid Values: `0—600`
Changes Take Effect: After restart
Specifies the delay, in seconds, between socket-bind operations that are being executed by the server. Use this option if the server has not been able to successfully occupy a configured port.

Warning: Use this option only when requested by Genesys Technical Support.

Debug Log Options

The options in this section enable you to generate Debug logs containing information about specific operations of an application.

x-conn-debug-all

x-conn-debug-all

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.
1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about open connection, socket select, timer creation and deletion, write, security-related, and DNS operations, and connection library function calls. This option is the same as enabling or disabling all of the previous x-conn-debug-<op type> options.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-api

x-conn-debug-api

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.

1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about connection library function calls.

Warning:: Use this option only when requested by Genesys Technical Support.

x-conn-debug-dns

x-conn-debug-dns

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.
1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about DNS operations.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-open

x-conn-debug-open

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.

1	Log records are generated.

Changes Take Effect: After restart
Generates Debug log records about *open connection* operations of the application.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-security

x-conn-debug-security

Default Value: `0` (zero)
Valid Values:

`0`	Log records are not generated.
1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about security-related operations, such as Transport Layer Security and security certificates.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-select

x-conn-debug-select

Default Value: `0` (zero)
Valid Values:

`0`	Log records are not generated.

1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about *socket select* operations of the application.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-timers

x-conn-debug-timers

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.
1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about the timer creation and deletion operations of the application.

Warning: Use this option only when requested by Genesys Technical Support.

x-conn-debug-write

x-conn-debug-write

Default Value: 0 (zero)
Valid Values:

0	Log records are not generated.

1	Log records are generated.

Changes Take Effect: After restart

Generates Debug log records about the *write* operations of the application.

Warning: Use this option only when requested by Genesys Technical Support.

log Section

This section must be called `log`.

See the following topics for more information:

- Log Output Options
- Log File Extensions
- Examples

buffering

buffering

Default Value: `true`
Valid Values:

`true`	Enables buffering.
`false`	Disables buffering.

Changes Take Effect: Immediately

Turns on/off the operating system file buffering. This option is applicable only to the `stderr` and `stdout` output. Setting the value of this option to `true` increases the output performance.

Warning: When buffering is enabled, there might be a delay before log messages appear at the console.

check-point

check-point

Default Value: `1`
Valid Values: `0`—`24`
Changes Take Effect: Immediately

Specifies, in hours, how often the application generates a `check point` log event, to divide the log into sections of equal time. By default, the application generates this log event every hour. Setting the value of this option to `0` (zero) prevents the generation of `check-point` events.

compatible-output-priority

compatible-output-priority

Default Value: `false`
Valid Values:

`true`	The log of the level specified by Log Output Options is sent to the specified output.
`false`	The log of the level specified by Log Output Options, and higher levels, is sent to the specified output.

Changes Take Effect: Immediately

Specifies whether the application uses 6.x output logic—for example, you configure the following options in the `log` section for a 6.x application and for a 7.x application:

```
[log]
verbose = all
debug = file1
standard = file2
```

- The log file content of a 6.x application is as follows:
  - `file1` contains Debug messages only.
  - `file2` contains Standard messages only.
- The log file content of a 7.x application is as follows:
  - `file1` contains Debug, Trace, Interaction, and Standard messages.
  - `file2` contains Standard messages only.

If you set the value of the `compatible-output-priority` option to `true` in the 7.x application, its log file content is the same as for the 6.x application.

Warning: Genesys does not recommend changing the default value of this option unless you have specific reasons to use the 6.x log output logic—that is, to mimic the output priority as implemented

in releases 6.x. Setting this option to `true` affects the log consistency.

expire

expire

Default Value: `false`
Valid Values:

`false`	No expiration; all generated segments are stored.
`<number> file or <number>`	Sets the maximum number of log files to store. Specify a number from `1—1000`.
`<number> day`	Sets the maximum number of days before log files are deleted. Specify a number from `1—100`.

Changes Take Effect: Immediately

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file.

Warning: If an option's value is set incorrectly to out of the range of valid values, it is automatically reset to `10`.

keep-startup-file

keep-startup-file

Default Value: `false`
Valid Values:

`false`	No startup segment of the log is kept.
`true`	A startup segment of the log is kept. The size of the segment equals the value of the `segment` option.
`<number> KB`	Sets the maximum size, in kilobytes, for a startup segment of the log.
`<number> MB`	Sets the maximum size, in megabytes, for a startup segment of the log.

Changes Take Effect: After restart

Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to `true` or to a specific size. If set to `true`, the size of the initial segment is equal to the size of the regular log segment defined by the `segment` option. The value of this option is ignored if the segmentation is turned off (that is, if the `segment` option set to `false`).

Warning: This option applies only to T-Servers.

memory

memory

Default Value: No default value
Valid Values: `<string>` (memory file name)
Changes Take Effect: Immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this (see, Log Output Options). The new snapshot overwrites the previously written data. If the application terminates abnormally, then this file contains the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

Warning: If the file specified as the `memory` file is located on a network drive, an application does not create a snapshot file (with the extension `*.memory.log`).

memory-storage-size

memory-storage-size

Default Value: 2 MB Valid Values:

<number> KB or <number>	The size of the memory output, in kilobytes. The minimum value is 128 KB.
<number> MB	The size of the memory output, in megabytes. The maximum value is 64 MB.

Changes Take Effect: When the memory output is created.

Specifies the buffer size for log output to the memory, if configured. See, Log Output Options.

messagefile

messagefile

Default Value: As specified by a particular application
Valid Values: <string>.lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

Warning: An application that does not find its *.lms file at startup cannot generate application-specific log events and send them to Message Server.

message_format

message_format

Default Value: `short`
Valid Values:

`short`	An application uses compressed headers when writing log records in its log file.
`full`	An application uses complete headers when writing log records in its log file.

Changes Take Effect: Immediately

Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size.

With the value set to `short`:

- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to `Std`, `Int`, `Trc`, or `Dbg`, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix `GCTI` or the application type `ID`.
- A log record in the full format looks like this:
  - `2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started`
- A log record in the short format looks like this:
  - `2002-05-07T18:15:33.952 Std 05060 Application started`

Warning: Whether the full or short format is used, time is printed in the format specified by the `time-format` option.

print-attributes

print-attributes

Default Value: `false`

Valid Values:

`true`	Attaches extended attributes, if any exist, to a log event sent to log output.
`false`	Does not attach extended attributes to a log event sent to log output.

Changes Take Effect: Immediately

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to `true` enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to *Genesys 8.0 Combined Log Events Help* to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

segment

segment

Default Value: `false`
Valid Values:

`false`	No segmentation is allowed.
`<number> KB or <number>`	Sets the maximum segment size, in kilobytes. The minimum segment size is `100 KB`.
`<number> MB`	Sets the maximum segment size, in megabytes.

`<number> hr`	Sets the number of hours for the segment to stay open. The minimum number is 1 hour.

Changes Take Effect: Immediately

Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a log file.

spool

spool

Default Value: The application's working directory
Valid Values: `<path>` (the folder, with the full path to it)
Changes Take Effect: Immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

time_convert

time_convert

Default Value: `Local`
Valid Values:

`local`	The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.

`utc`	The time of log record generation is expressed as Coordinated Universal Time (UTC).

Changes Take Effect: Immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch time (00:00:00 UTC, January 1, 1970).

time_format

time_format

Default Value: `time`
Valid Values:

`time`	The time string is formatted according to the `HH:MM:SS.sss` (hours, minutes, seconds, and milliseconds) format.
`locale`	The time string is formatted according to the system's locale.
`ISO8601`	The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

Changes Take Effect: Immediately

Specifies how to represent, in a log file, the time when an application generates log records. A log record's time field in the ISO 8601 format looks like this:

- `2001-07-24T04:58:10.123`

verbose

verbose

Default Value: `all`
Valid Values:

`all`	All log events (that is, log events of the Standard, Trace, Interaction, and Debug levels) are generated.
`debug`	The same as `all`.
`trace`	Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
`interaction`	Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
`standard`	Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
`none`	No output is produced.

Changes Take Effect: Immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug. See also Log Output Options.

Warning: For definitions of the Standard, Interaction, Trace, and Debug log levels, refer to the *Framework 8.x Management Layer User's Guide*, *Framework 8.x Genesys Administrator Help,* or to

Framework 8.x Solution Control Interface Help.

Log Output Options

To configure log outputs, set the following log level options listed below to the following desired types of log output: `stdout`, `stderr`, `network`, `memory`, and/or `[filename]`, for log file output.

You can use:

- One log level option to specify different log outputs.
- One log output type for different log levels.
- Several log output types simultaneously, to log events of the same or different log levels.

You must separate the log output types by a comma, when you are configuring more than one output for the same log level. See the topic, Examples.

Notes:

- If you direct log output to a file on the network drive, an application does not create a snapshot log file (with the extension `*.snapshot.log`) in case it terminates abnormally.
- Directing log output to the console (by using the `stdout` or `stderr` settings) can affect application performance. Avoid using these log output settings in a production environment.

Warning: The log output options are activated according to the setting of the verbose configuration option.

all

all

Default Value: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).

network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
memory	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

For example:

- all = stdout, logfile

Warning: To ease the troubleshooting process, consider using unique names for log files that different applications generate.

alarm

alarm

Default Value: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	og events are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately
Specifies the outputs to which an application sends the `Alarm`-level log events. The log output types must be separated by a comma when more than one output is configured.

For example:

- `standard = stderr, network`

debug

debug

Default Value: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the `Standard`, `Interaction`, `Trace`, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

For example:

- `debug = stderr, /usr/local/genesys/logfile`

Warning: Debug-level log events are never sent to Message Server or stored in the Log Database.

interaction

interaction

Default Value: No default value
Valid Values (log output types):

stdout	Log events are sent to the Standard output (stdout).
stderr	Log events are sent to the Standard error output (stderr).
network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
memory	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

For example:

- interaction = stderr, network

standard

standard

Default Value: No default value

Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Standard` level. The log output types must be separated by a comma when more than one output is configured.

For example:

- `standard = stderr, network`

trace

trace

Default Value: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Trace` level and higher (that is, log events of the `Standard`, `Interaction`, and `Trace` levels). The log outputs must be separated by a comma when more than one output is configured.

For example:

- `trace = stderr, network`

Log File Extensions

You can use the following file extensions to identify log files that an application creates for various types of output:

- `*.log`—assigned to log files when you configure output to a log file—for example, if you set `standard = confservlog` for Configuration Server, it prints log messages into a text file called `confservlog.<time_stamp>.log.`
- `*.qsp`—assigned to temporary (spool) files when you configure output to the network but the network is temporarily unavailable—for example, if you set `standard = network` for Configuration Server, it prints log messages into a file called `confserv.<time_stamp>.qsp` during the time the network is not available.
- `*.snapshot.log`—assigned to files that contain the output snapshot when you configure output to a log file. The file contains the last log messages that an application generates before it terminates abnormally—for example, if you set `standard = confservlog` for Configuration Server, it prints the last log message into a file called `confserv.<time_stamp>.snapshot.log` in case of failure.

Warning: Provide the `*.snapshot.log` files to Genesys Technical Support when reporting a problem.

- `*.memory.log`—assigned to log files that contain the memory output snapshot when you configure output to memory and redirect the most recent memory output to a file—for example, if you set `standard = memory` and `memory = confserv` for Configuration Server, it prints the latest memory output to a file called `confserv.<time_stamp>.memory.log`.

Examples

This section presents examples of a `log` section that you might configure for an application when that application is operating in production mode and in the following two lab modes: debugging and troubleshooting.

Production Mode Log Section

- [log]
- `verbose = standard`
- `standard = network, logfile`

With this configuration, an application only generates the log events of the `Standard` level and sends them to Message Server, and to a file named `logfile`, which the application creates in its working directory. Genesys recommends that you use this or a similar configuration in a production environment.

Warning: Directing log output to the console (by using the `stdout` or `stderr` settings) can affect application performance. Avoid using these log output settings in a production environment.

Lab Mode Log Section

- [log]
- verbose = all
- all = stdout, /usr/local/genesys/logfile
- trace = network

With this configuration, an application generates log events of the `Standard`, `Interaction`, `Trace`, and Debug levels, and sends them to the standard output and to a file named `logfile`, which the application creates in the `/usr/local/genesys/` directory. In addition, the application sends log events of the `Standard`, `Interaction`, and `Trace` levels to Message Server. Use this configuration to test new interaction scenarios in a lab environment.

Failure-Troubleshooting Log Section

- [log]
- verbose = all
- standard = network

- all = memory
- memory = logfile
- memory-storage-size = 32 MB

With this configuration, an application generates log events of the `Standard` level and sends them to Message Server. It also generates log events of the `Standard`, `Interaction`, `Trace`, and `Debug` levels, and sends them to the memory output. The most current log is stored to a file named `logfile`, which the application creates in its working directory. Increased memory storage allows an application to save more of the log information generated before a failure.

Warning: If you are running an application on UNIX, and you do not specify any files in which to store the memory output snapshot, a core file that the application produces before terminating contains the most current application log. Provide the application's core file to Genesys Technical Support when reporting a problem.

log-extended Section

This section must be called `log-extended`.

level-reassign-disable

level-reassign-disable

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

When this option is set to `true`, the original (default) log level of all log events in the `[log-extended]` section are restored. This option is useful when you want to use the default levels, but not delete the customization statements.

level-reassign-<eventID>

level-reassign-<eventID>

Default Value: Default value of log event `<eventID>`
Valid Values:

`alarm`	The log level of log event `<eventID>` is set to `Alarm`.
`standard`	The log level of the `<eventID>` log event is set to `Standard`.
`interaction`	The log level of the `<eventID>` log event is set to `Interaction`.
`trace`	The log level of the `<eventID>` log

	event is set to Trace.
debug	The log level of the <eventID> log event is set to Debug.
none	The <eventID> log event is not recorded in a log.

Changes Take Effect: Immediately

Specifies a log level for the <eventID> log event that is different than its default level, or disables the <eventID> log event completely. If no value is specified, the log event retains its default level. This option is useful when you want to customize the log level for selected log events. These options can be deactivated using the level-reassign-disable option.

Warning:

- Use caution when making these changes in a production environment.
- Depending on the log configuration, changing the log level to a higher priority may cause the log event to be logged more often or to a greater number of outputs. This could affect system performance.
- Likewise, changing the log level to a lower priority may cause the log event to be not logged at all, or to be not logged to specific outputs, thereby losing important information. The same applies to any alarms associated with that log event.

Notes: In addition to the preceding warnings, take note of the following:

- Logs can be customized only by release 7.6 or later applications.
- When the log level of a log event is changed to any level except none, it is subject to the other settings in the [log] section at its new level. If set to none, it is not logged and is therefore not subject to any log configuration.
- Using this feature to change the log level of a log changes only its priority; it does not change how that log is treated by the system. For example, increasing the priority of a log to Alarm level does not mean that an alarm will be associated with it.
- Each application in a High Availability (HA) pair can define its own unique set of log customizations, but the two sets are not synchronized with each other. This can result in different log behavior depending on which application is currently in primary mode.
- This feature is not the same as a similar feature in Universal Routing Server (URS) release 7.2 or later. In this Framework feature, the priority of log events are customized. In the URS feature, the priority of debug messages only are customized. Refer to the Universal Routing Reference Manual for more information about the URS feature.
- You cannot customize any log event that is not in the unified log record format. Log events of the Alarm, Standard, Interaction, and Trace levels feature the same unified log record format.

Example:

This is an example of using customized log level settings, subject to the following log configuration:

```
[log]
verbose=interaction
all=stderr
interaction=log_file
standard=network
```

Before the log levels of the log are changed:

- Log event 1020, with default level `standard`, is output to `stderr` and `log_file`, and sent to Message Server.
- Log event 2020, with default level `standard`, is output to `stderr` and `log_file`, and sent to Message Server.
- Log event 3020, with default level `trace`, is output to `stderr`.
- Log event 4020, with default level `debug`, is output to `stderr`.

Extended log configuration section:

```
[log-extended]
level-reassign-1020=none
level-reassign-2020=interaction
level-reassign-3020=interaction
level-reassign-4020=standard
```

After the log levels are changed:

- Log event 1020 is disabled and not logged.
- Log event 2020 is output to `stderr` and `log_file`.
- Log event 3020 is output to `stderr` and `log_file`.
- Log event 4020 is output to `stderr` and `log_file`, and sent to Message Server.

log-filter Section

The `log-filter` section contains configuration options used to define the default treatment of filtering data in log output. This section contains one configuration option, `default-filter-type`. Refer to the *Hide Selected Data in Logs* chapter in the *Genesys 8.1 Security Deployment Guide* for complete information about this option.

log-filter-data Section

The `log-filter-data` section contains configuration options used to define the treatment of filtering data in log output on a key-by-key basis. This section contains one configuration option in the form of <key name>. Refer to the *Hide Selected Data in Logs* chapter in the *Genesys 8.1 Security Deployment Guide* for complete information about this option.

security Section

The `security` section contains configuration options used to specify security elements for your system. In addition to other options that may be required by your application, this section contains the configuration option `disable-rbac`, which is used to enable or disable Role-Based Access Control for an application. Refer to the *Role-Based Access Control* chapter in the *Genesys 8.1 Security Deployment Guide* for complete information about this option.

sml Section

This section must be called `sml`.

heartbeat-period

heartbeat-period

Default Value: None
Valid Values:

`0`	This method of detecting an unresponsive application is not used by this application.
`3-604800`	Length of timeout, in seconds; equivalent to 3 seconds—7 days.

Changes Take Effect: Immediately

Specifies the maximum amount of time, in seconds, in which heartbeat messages are expected from an application. If Local Control Agent (LCA) does not receive a heartbeat message from the application within this period, it assumes the application is not responding and carries out corrective action.

This option can also be used to specify the maximum heartbeat interval for threads registered with class zero (`0`). This thread class is reserved for use by the Management Layer only.

If this option is not configured or is set to `0` (zero), heartbeat detection is not used by this application.

Warning: Use this option with caution, and only with those applications that support this functionality. Failure to use this option properly could result in unexpected behavior, from ignoring the options to an unexpected restart of the application.

heartbeat-period-thread-class-<n>

heartbeat-period-thread-class-<n>

Default Value: None
Valid Values:

0	Value specified by the heartbeat-period in the application that is used.
3-604800	Length of timeout, in seconds; equivalent to 3 seconds—7 days.

Changes Take Effect: Immediately

Specifies the maximum amount of time, in seconds, in which heartbeat messages are expected from a thread of class, <n> registered by an application. If a heartbeat message from the thread is not received within this period, the thread is assumed to be not responding, and therefore, the application is unable to provide service.

If this option is not configured or is set to 0 (zero), but the application has registered one or more threads of class, <n>, the value specified by the value of the heartbeat-period for the application is also applied to these threads.

Refer to the application-specific documentation to determine what thread classes, if any, are used.

Warning: Use this option with caution, and only with those applications that support this functionality. Failure to use this option properly could result in unexpected behavior, from ignoring the options to an unexpected restart of the application.

hangup-restart

hangup-restart

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

If the value of the option is set to true (the default value), specifies that LCA restarts the unresponsive application immediately, without any further interaction from Solution Control Server. If the value of the option is set to false, specifies that LCA only generates a notification that the application has stopped responding.

Warning: Use this option with caution, and only with those applications that support this functionality. Failure to use this option properly could result in unexpected behavior, from ignoring the options to an unexpected restart of the application.

suspending-wait-timeout

suspending-wait-timeout

Default Value: `10`
Valid Values: `5-600`
Changes Take Effect: Immediately

Specifies a timeout (in seconds) after the Stop Graceful command is issued to an application during which the status of the application should change to `Suspending`, if the application supports a graceful shutdown. If the status of the application does not change to `Suspending` before the timeout expires, it is assumed that the application does not support a graceful shutdown, and it is stopped ungracefully.

Use this option if you are unsure whether the application supports a graceful shutdown.

Warning: Genesys recommends that you do not set this option for any Management Layer component (Configuration Server, Message Server, Solution Control Server, or SNMP Master Agent) or any DB Server. These components, by definition, do not support graceful shutdown, so this option is not required.

T-Server Common Configuration Options

This section describes the configuration options that are generally common to all T-Server types, with some exceptions noted. This section contains the following topics:

Setting Configuration Options

Unless specified otherwise, set T-Server common configuration options in the `Options` of the `Application` object, using one of the following navigation paths:

- In Genesys Administrator—`Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—`Application` object > `Properties` dialog box > `Options` tab

Mandatory Options

Except as noted for certain environments, the configuration of common options is not required for basic T-Server operation.

Security Section

The `Security` section contains the configuration options that are used to configure secure data exchange between T-Servers and other Genesys components. Refer to the *Genesys 8.0 Security Deployment Guide* for complete information on the security configuration.

Timeout Value Format

This section of the document describes the values to use for those T-Server common options that set

various timeouts. The current format allows you to use fractional values and various time units for timeout settings.

For timeout-related options, you can specify any value that represents a time interval, provided that it is specified in one of the following formats:

[[[*hours*:]*minutes*:]*seconds*][*milliseconds*]

or

[*hours* hr][*minutes* min][*seconds* sec][*milliseconds* msec]

Where a time unit name in italic (such as *hours*) is to be replaced by an integer value for this time unit.

Integer values with no measuring units are still supported, for compatibility with previous releases of T-Server. When you do not specify any measuring units, the units of the default value apply. For example, if the default value equals `60 sec`, specifying the value of `30` sets the option to 30 seconds.

Example 1

The following settings result in a value of 1 second, 250 milliseconds:

```
sync-reconnect-tout = 1.25sync-reconnect-tout = 1 sec 250 msec
```

Example 2

The following settings result in a value of 1 minute, 30 seconds:

```
timeout = 1:30timeout = 1 min 30 sec
```

agent-reservation Section

The `agent-reservation` section contains the configuration options that are used to customize the T-Server Agent Reservation feature. See the Agent Reservation section for details on this feature.

Warning: The Agent Reservation functionality is currently a software-only feature that is used to coordinate multiple client applications. This feature does not apply to multiple direct or ACD-distributed calls.

collect-lower-priority-requests

collect-lower-priority-requests

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

Specifies whether an agent reservation request is collected, depending on its priority during the time interval specified by the `request-collection-time` configuration option. When set to `false`, during the `request-collection-time` interval T-Server collects reservation requests of the highest priority only, rejecting newly submitted requests that have a lower priority or rejecting all previously submitted requests if a request with a higher priority arrives. When set to `true` (the default), agent reservation requests are collected as they were in pre-8.x releases.

request-collection-time

request-collection-time

Default Value: `100` milliseconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval, in milliseconds, that the agent reservation requests are collected before a reservation is granted. During this time interval, the agent reservation requests are delayed, in order to balance the successful reservations between client applications—for example: Universal Routing Servers).

reject-subsequent-request

reject-subsequent-request

Default Value: `true`
Valid Values:

`true`	T-Server rejects subsequent requests.
`false`	A subsequent request prolongs the current reservation made by the same client application for the same agent.

Changes Take Effect: Immediately

Specifies whether T-Server rejects subsequent requests from the same client application, for an agent reservation for the same `Agent` object that is currently reserved.

Warning: Genesys does not recommend setting this option to `false` in a multi-site environment in which remote locations use the Agent-Reservation feature.

reservation-time

reservation-time

Default Value: `10000` milliseconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately
Specifies the default time interval for which an Agent DN is reserved. During this interval, the agent cannot be reserved again.

backup-sync Section

The backup-synchronization section contains the configuration options that are used to support a high-availability (HA) `hot standby` (redundancy type) configuration.

Warning: These options apply only to T-Servers that support the `hot standby` redundancy type.

addp-remote-timeout

addp-remote-timeout

Default Value: `0` (zero)
Valid Values: Any positive integer from `0`—`3600`
Changes Take Effect: Immediately

Specifies the time interval that the redundant T-Server waits for a response from this T-Server after sending a polling signal. The default value of `0` (zero) disables the functionality of this option. To establish an appropriate timeout, specify a value other than the default. This option applies only if the `protocol` option is set to `addp`.

addp-timeout

addp-timeout

Default Value: `0` (zero)
Valid Values: Any positive integer from `0`—`3600`
Changes Take Effect: Immediately

Specifies the time interval that this T-Server waits for a response from another T-Server after sending a polling signal. The default value of `0` (zero) disables the functionality of this option. To establish an appropriate timeout, specify a value other than the default. This option applies only if the `protocol` option is set to `addp`.

addp-trace

addp-trace

Default Value: `off`
Valid Values:

`off, false, no`	No trace (default).
`local, on, true, yes`	Trace on this T-Server side only.
`remote`	Trace on the redundant T-Server side only.
`full, both`	Full trace (on both sides).

Changes Take Effect: Immediately

Specifies whether addp messages are traced in a log file, to what level the trace is performed, and in which direction. This option applies only if the `protocol` option is set to `addp`.

protocol

protocol

Default Value: `default`
Valid Values:

`default`	The feature is not active.
`addp`	Activates the Advanced Disconnect Detection Protocol.

Changes Take Effect: When the next connection is established.

Specifies the name of the method used to detect connection failures. If you specify the `addp` value, you must also specify a value for the `addp-timeout`, `addp-remote-timeout`, and `addp-trace` options.

sync-reconnect-tout

sync-reconnect-tout

Default Value: 20 seconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately
Specifies the time interval after which the backup T-Server attempts to reconnect to the primary server (for a synchronized link).

call-cleanup Section

The call-cleanup section contains the configuration options that are used to control detection and cleanup of stuck calls in T-Server. For more information on stuck call handling, refer to the *Stuck Call Management* chapter in the Framework 8.1 Management Layer User's Guide. See the topic, call-cleanup Section Examples, for more information.

cleanup-idle-tout

cleanup-idle-tout

Default Value: `0` (zero)
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits for a call to be updated from its last update. After this time elapses, if no new events about the call are received, T-Server clears this call as a stuck call, either by querying the switch (if a CTI link provides such capabilities) or by deleting the call information from memory unconditionally. The default value of `0` (zero) disables the stuck calls cleanup.

Warning: If the call-cleanup functionality is enabled in T-Server for Avaya Communication Manager, the UCID (Universal Call ID) feature must be enabled on the switch as well. This allows the UCID to be generated and passed to T-Server.

notify-idle-tout

notify-idle-tout

Default Value: `0` (zero)
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits for a call to be updated from its last update. After this time elapses, if no new events about the call are received, T-Server reports this call as a stuck call. The default value of `0` (zero) disables the stuck calls notification.

periodic-check-tout

periodic-check-tout

Default Value: 10 minutes
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval for periodic checks for stuck calls. These checks affect both notification and cleanup functionality, and are made by checking the T-Server's own call information with call information available in the switch. For performance reasons, T-Server does not verify whether the `notify-idle-tout` or `cleanup-idle-tout` option has expired before performing this check.

Warning: Setting this option to a value of less than a few seconds can affect T-Server performance.

call-cleanup Section Examples

Examples

This section presents examples of option settings in the `call-cleanup` section.

Example 1

```
cleanup-idle-tout = 0

notify-idle-tout = 0

periodic-check-tout = 10
```

With these settings, T-Server does not perform any checks for stuck calls.

Example 2

```
cleanup-idle-tout = 0

notify-idle-tout = 5 min

periodic-check-tout = 10 min
```

With these settings, T-Server performs checks every 10 minutes and sends notifications about all calls that have been idle for at least 5 minutes.

Example 3

```
cleanup-idle-tout = 20 min

notify-idle-tout = 5 min

periodic-check-tout = 10 min
```

With these settings, T-Server performs checks every 10 minutes, sends notifications about all calls

that have been idle for at least 5 minutes, and attempts to clean up all calls that have been idle for more than 20 minutes.

extrouter Section

The `extrouter` section contains the configuration options that are used to support multi-site environments with the Inter Server Call Control (ISCC) feature. The configuration options in this section of the document are grouped with related options that support the same functionality, as follows:

- Event Propagation Options
- GVP Integration Option
- ISCC/COF Options
- ISCC Transaction Options
- Number Translation Option
- Transfer Connect Service Options

For a description of the ways in which T-Server supports multi-site configurations and for an explanation of the configuration possibilities for a multi-site operation, see the Multi-Site Support PDF.

Warning: In a multi-site environment, you must configure the timeout, cast-type, and default-dn options with the same value for both the primary and backup T-Servers. If you do not do this, the value specified for the backup T-Server overrides the value specified for the primary T-Server.

match-call-once

match-call-once

Default Value: `true`
Valid Values:

`true`	ISCC does not process (match) an inbound call that has already been processed (matched).
`false`	Inter Server Call Control (ISCC)

	processes (attempts to match) a call as many times as it arrives at an ISCC resource or multi-site-transfer target.

Changes Take Effect: Immediately

Specifies how many times ISCC processes an inbound call when it arrives at an ISCC resource. When set to `false`, ISCC processes (attempts to match) the call even if it has already been processed.

Warning: Genesys does not recommend changing the default value of the `match-call-once` option to `false` unless you have specific reasons. Setting this option to `false` may lead to excessive or inconsistent call data updates.

reconnect-tout

reconnect-tout

Default Value: 5 seconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: At the next reconnection attempt

Specifies the time interval after which a remote T-Server attempts to connect to this T-Server after an unsuccessful attempt or a lost connection. The number of attempts is unlimited. At startup, T-Server immediately attempts the first connection, without this timeout.

report-connid-changes

report-connid-changes

Default Value: `false`
Valid Values:

`true`	`EventPartyChanged` is generated.
`false`	`EventPartyChanged` is not generated.

Changes Take Effect: Immediately

Specifies whether the destination T-Server generates EventPartyChanged for the incoming call when the resulting ConnID attribute is different from the ConnID attribute of an instance of the same call at the origination location.

use-data-from

use-data-from

Default Value: current
Valid Values:

active	The values of UserData and ConnID attributes are taken from the consultation call.
original	The values of UserData and ConnID attributes are taken from the original call.
active-data-original-call	The value of the UserData attribute is taken from the consultation call and the value of ConnID attribute is taken from the original call.
current	If the value of current is specified, the following occurs: • Before the transfer or conference is completed, the UserData and ConnID attributes are taken from the consultation call. • After the transfer or conference is completed, EventPartyChanged is generated, and the UserData and ConnID are taken from the original call.

Changes Take Effect: Immediately

Specifies the call from which the values for the UserData and ConnID attributes are taken for a consultation call that is routed or transferred to a remote location.

Warning: For compatibility with the previous T-Server releases, you can use the values `consult`, `main`, and `consult-user-data` for this option. These values are aliases for `active`, `original`, and `current`, respectively.

Event Propagation Options

compound-dn-representation

compound-dn-representation

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

Specifies which format T-Server uses to represent a DN when reporting an `OtherDN` or `ThirdPartyDN` attribute in event propagation messages. When set to `true`, the `<switch>::DN` (compound) format is used. This option value supports backward compatibility for pre-8.x T-Server ISCC/EPP functionality and is provided for multi-site deployments where the same DNs are configured under several switches.

When set to `false`, the `DN` (non-compound) format is used. This option value ensures more transparent reporting of `OtherDN` or `ThirdPartyDN` attributes and is recommended for all single-site deployments, as well as for multi-site deployments that do not have the same DNs configured under several switches. This option applies only if the `event-propagation` option is set to `list`.

Warning: Local DNs are always represented in the non-compound `(DN)` form.

epp-tout

epp-tout

Default Value: `0` (zero)
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval during which T-Server attempts to resolve race conditions that may occur in deployments that use switch partitioning or intelligent trunks. This option applies only if the `event-propagation` option is set to `list`.

Warning: If the time interval is not long enough to account for possible network switching delays, T-Server may produce duplicated events, such as events that are propagated by the ISCC and generated locally.

event-propagation

event-propagation

Default Value: `list`
Valid Values:

`list`	Changes in user data and party events are propagated to remote locations through call distribution topology.
`off`	The feature is disabled. Changes in user data and party events are not propagated to remote locations.

Changes Take Effect: Immediately

Specifies whether the Event Propagation feature is enabled.

propagated-call-type

propagated-call-type

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Switch Partitioning

Determines what T-Server reports as the value of the `CallType` attribute in events related to calls that have been synchronized with another site via ISCC, as follows:

- When set to `false`, T-Server reports in events related to calls that have been synchronized with another site via ISCC the same value for the `CallType` attribute as it did in pre-8.0 releases and adds the new `PropagatedCallType` attribute with the value of the `CallType` attribute at the origination site. This provides backward compatibility with existing T-Server clients.
- When set to `true`, T-Server reports in events related to calls that have been synchronized with another site via ISCC the same value for the `CallType` attribute as at the origination site, and adds the new `LocalCallType` attribute with the same value as `CallType` in pre-8.0 releases.

GVP Integration Option

handle-vsp

Default Value: no
Valid Values:

requests	ISCC processes and adjusts requests related to this DN and containing a Location attribute before submitting them to the service provider.
events	ISCC processes and adjusts events received from the service provider and containing a Location attribute before distributing them to T-Server clients.
all	ISCC processes and adjusts both events and requests.
no	No ISCC processing of such requests and events takes place.

Changes Take Effect: Immediately

Specifies the way ISCC handles events from, and requests to, an external service provider registered for a DN using the AddressType attribute set to VSP.

ISCC/COF Options

cof-ci-defer-create

cof-ci-defer-create

Default Value: `0` (zero)
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits for call data from the switch before generating a negative response for a call data request from a remote T-Server. If T-Server detects the matching call before this timeout expires, it sends the requested data. This option applies only if the `cof-feature` option is set to `true`.

cof-ci-defer-delete

cof-ci-defer-delete

Default Value: `0` (zero)
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits before deleting call data that might be overflowed. If set to `0`, deletion deferring is disabled. This option applies only if the `cof-feature` option is set to `true`.

cof-ci-req-tout

cof-ci-req-tout

Default Value: `500` milliseconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: For the next COF operation

Specifies the time interval during which T-Server waits for the call data requested with respect to a call originated at another site. After T-Server sends the call data request to remote T-Servers, all events related to this call will be suspended until either the requested call data is received or the specified timeout expires. This option applies only if the `cof-feature` option is set to `true`.

cof-ci-wait-all

cof-ci-wait-all

Default Value: `false`
Valid Values:

`true`	T-Server waits for responses from all T-Servers that might have the requested call data before updating the call data with the latest information.
`false`	T-Server updates the call data with the information received from the first positive response.

Changes Take Effect: Immediately

Specifies whether T-Server, after sending a request for matching call data, waits for responses from other T-Servers before updating the call data (such as `CallHistory`, `ConnID`, and `UserData`) for a potentially overflowed call. The waiting period is specified by the cof-ci-req-tout and cof-rci-tout options. This option applies only if the cof-feature option is set to `true`.

cof-feature

cof-feature

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

Enables or disables the Inter Server Call Control/Call Overflow (ISCC/COF) feature.

cof-rci-tout

cof-rci-tout

Default Value: `10` seconds
Valid Values: See, Timeout Value Format.

Changes Take Effect: For the next COF operation.

Specifies the time interval that T-Server waits for call data from other T-Servers' transactions. Counting starts when `cof-ci-req-tout` expires. This option applies only if the `cof-feature` option is set to `true`.

default-network-call-id-matching

default-network-call-id-matching

Default Value: No default value
Valid Values: See the T-Server-Specific Configuration Options section for an option description for your T-Server.
Changes Take Effect: Immediately

When a value for this option is specified, T-Server uses the `NetworkCallID` attribute for the ISCC/COF call matching. To activate this feature, the `cof-feature` option must be set to `true`.

Warning: SIP Server and several T-Servers support the `NetworkCallID` attribute for the ISCC/COF call matching in a way that requires setting this option to a specific value. For information about the option value that is specific for your T-Server, see the T-Server-Specific Configuration Options section of your *T-Server Deployment Guide.*

local-node-id

local-node-id

Default Value: `0` (zero)
Valid Values: `0` or any positive integer
Changes Take Effect: Immediately

This option, if enabled, checks all networked calls against the specified `NetworkNodeID` (the identity of the switch to which the call initially arrived). If the `NetworkNodeID` is the same as the value of this option, the request for call information is *not* sent. The default value of `0` (zero) disables the functionality of this option. To establish an appropriate `NetworkNodeID`, specify a value other than the default. This option applies only if the `cof-feature` option is set to `true`.

Warning: This option applies only to T-Server for Nortel Communication Server 2000/2100.

ISCC Transaction Options

cast-type

cast-type

Default Values:

- direct-ani
- direct-callid
- direct-digits
- direct-network-callid
- direct-notoken
- direct-uui
- dnis-pool
- pullback
- reroute
- route
- route-uui

Valid Values:

- direct-ani
- direct-callid
- direct-digits
- direct-network-callid
- direct-notoken
- direct-uui
- dnis-pool
- pullback
- reroute
- route
- route-uui

Changes Take Effect: For the next request for the remote service

Specifies—using a space-, comma- or semicolon-separated list—the routing types that can be performed for this T-Server.

The valid values provide for a range of mechanisms that the ISCC feature can support with various T-Servers, in order to pass call data along with calls between locations.

Because switches of different type provide calls with different sets of information parameters, some values might not work with your T-Server. The Multi-Site Support section also provides detailed descriptions of all transaction types.

Warning: For compatibility with the previous T-Server releases, you can use the `direct` value for this option. This is an alias for `direct-callid`. Warning: An alias, `route-notoken`, has been added to the `route` value.

default-dn

default-dn

Default Value: No default value
Valid Values: Any DN
Changes Take Effect: For the next request for the remote service.

Specifies the DN to which a call is routed when a Destination DN (`AttributeOtherDN`) is not specified in the client's request for routing. If neither this option, nor the client's request, contains the destination DN, the client receives a `EventError` message.

Warning: This option is used only for requests with route types `route`, `route-uui`, `direct-callid`, `direct-network-callid`, `direct-uui`, `direct-notoken`, `direct-digits`, and `direct-ani`.

direct-digits-key

direct-digits-key

Default Value: `CDT_Track_Num`
Valid Values: Any valid key name of a key-value pair from the `UserData` attribute.
Changes Take Effect: For the next request for the remote service.

Specifies the name of a key from the `UserData` attribute that contains a string of digits that are used as matching criteria for remote service requests with the `direct-digits` routing type.

Warning: For compatibility with the previous T-Server releases, this configuration option has an alias value of `cdt-udata-key`.

dn-for-unexpected-calls

dn-for-unexpected-calls

Default Value: No default value
Valid Values: Any DN
Changes Take Effect: Immediately

Specifies a default DN for unexpected calls arriving on an External Routing Point.

network-request-timeout

network-request-timeout

Default Value: `20 sec`
Valid Values: See, Timeout Value Format.
Changes Take Effect: For the next network request.

For a premise T-Server, this option specifies the time interval that the premise T-Server waits for a response, after relaying a `TNetwork<...>` request to the Network T-Server. For a Network T-Server, this option specifies the time interval that the Network T-Server waits for a response from an SCP (Service Control Point), after initiating the processing of the request by the SCP.

When the allowed time expires, the T-Server cancels further processing of the request and generates a `EventError` message.

register-attempts

register-attempts

Default Value: 5
Valid Values: Any positive integer
Changes Take Effect: For the next registration

Specifies the number of attempts that T-Server makes to register a dedicated External Routing Point.

register-tout

register-tout

Default Value: 2 seconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: For the next registration.

Specifies the time interval after which T-Server attempts to register a dedicated External Routing

Point. Counting starts when the attempt to register a Routing Point fails.

request-tout

request-tout

Default Value: 20 seconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: For the next request for remote service.

Specifies the time interval that a T-Server at the origination location waits for a notification of routing service availability from the destination location. Counting starts when the T-Server sends a request for remote service to the destination site.

resource-allocation-mode

resource-allocation-mode

Default Value: circular
Valid Values:

home	T-Server takes an alphabetized (or numerically sequential) list of configured DNs and reserves the first available DN from the top of the list for each new request. For example, if the first DN is not available, the second DN is allocated for a new request. If the first DN is freed by the time the next request comes, the first DN is allocated for this next request.
circular	T-Server takes the same list of configured DNs, but reserves a subsequent DN for each subsequent request. For example, when the first request comes, T-Server allocates the

	first DN; when the second request comes, T-Server allocates the second DN; and so on. T-Server does not reuse the first DN until reaching the end of the DN list.

Changes Take Effect: Immediately

Specifies the manner in which T-Server allocates resources (that is, DNs of the `External Routing Point` type and Access Resources with the `Resource Type` set to `dnis`) for multi-site transaction requests.

resource-load-maximum

resource-load-maximum

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the maximum number of ISCC routing transactions that can be concurrently processed at a single DN of the `External Routing Point` route type. After a number of outstanding transactions at a particular DN of the `External Routing Point` type reaches the specified number, T-Server considers the DN not available. Any subsequent request for this DN is queued until the number of outstanding transactions decreases. A value of `0` (zero) means that no limitation is set to the number of concurrent transactions at a single External Routing Point. In addition, the `0` value enables T-Server to perform load balancing of all incoming requests among all available External Routing Points, in order to minimize the load on each DN.

route-dn

route-dn

Default Value: No default value
Valid Values: Any DN
Changes Take Effect: Immediately

Specifies the DN that serves as a Routing Point for the `route` transaction type in the multiple-to-one access mode.

timeout

timeout

Default Value: `60` seconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: For the next request for remote service.

Specifies the time interval that the destination T-Server waits for a call routed from the origination location. Counting starts when this T-Server notifies the requesting T-Server about routing service availability. The timeout must be long enough to account for possible network delays in call arrival.

use-implicit-access-numbers

use-implicit-access-numbers

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After T-Server is restarted

Determines whether an External Routing Point in which at least one access number is specified is eligible for use as a resource for calls coming from switches for which an access number is not specified in the External Routing Point. If this option is set to `false`, the External Routing Point is not eligible for use as a resource for calls coming from such switches. If this option is set to `true`, an implicit access number for the External Routing Point, composed of the switch access code and the DN number of the External Routing Point, is used.

Warning: If an External Routing Point does not have an access number specified, this option will not affect its use.

Number Translation Option

inbound-translator-<n>

Default Value: No default value
Valid Value: Any valid name
Changes Take Effect: Immediately

Specifies the name of another configuration section as the value for the `inbound-translator-1 = ani-translator` where `ani-translator` is the name of the configuration that describes the translation rule for inbound numbers.

Transfer Connect Service Options

tcs-queue

tcs-queue

Default Value: No default value
Valid Values: Any valid DN number
Changes Take Effect: For the next request for the remote service

Specifies the TCS DN number to which a call, processed by the TCS feature, is dialed after the originating external router obtains an access number. This option applies only if the `tcs-use` option is activated.

tcs-use

tcs-use

Default Value: `never`
Valid Values:

`never`	The TCS feature is not used.
`always`	The TCS feature is used for every call.
`app-defined`	In order to use the TCS feature for a multi-site call transfer request, a client application must add a key-value pair with a TC-type key and a nonempty string value to either the `UserData` or `Extensions` attribute of the request.

Changes Take Effect: Immediately

Specifies whether the Transfer Connect Service (TCS) feature is used.

Warning: For compatibility with the previous T-Server releases, you can use the value `up-app-depended` for this option. This is an alias for `app-defined`.

License Section

The License section contains the configuration options that are used to configure T-Server licenses. They set the upper limit of the seat-related DN licenses (`tserver_sdn`) that T-Server tries to check out from a license file. See License Checkout.

Warnings:

- T-Server also supports the `license-file` option described in the *Genesys Licensing Guide.*
- The `license` section is not applicable to Network T-Server for DTAG.
- If you use two or more T-Servers, and they share licenses, you must configure the following options in the `license` section of the T-Servers.

num-of-licenses

num-of-licenses

Default Value: `0` (zero) or `max` (all available licenses)
Valid Values: `0` (zero) or string `max`
Changes Take Effect: Immediately

Specifies how many DN licenses T-Server checks out. T-Server treats a value of `0` (zero) the same as it treats `max`; that is, it checks out all available licenses.

The sum of all `num-of-licenses` values for all concurrently deployed T-Servers must not exceed the number of seat-related DN licenses (`tserver_sdn`) in the corresponding license file. The primary and backup T-Servers share the same licenses, and therefore they need to be counted only once. T-Server checks out the number of licenses indicated by the value for this option, regardless of the number actually in use.

num-sdn-licenses

num-sdn-licenses

Default Value: `0` (zero) or `max` (All DN licenses are seat-related)
Valid Values: String `max` (equal to the value of `num-of-licenses`), or any integer from `0`—`9999`
Changes Take Effect: Immediately

Specifies how many seat-related licenses T-Server checks out. A value of `0` (zero) means that T-Server does not grant control of seat-related DNs to any client, and it does not look for seat-related DN licenses at all.

The sum of all `num-sdn-licenses` values for all concurrently deployed T-Servers must not exceed the number of seat-related DN licenses (`tserver_sdn`) in the corresponding license file. The primary and backup T-Servers share the same licenses, and therefore they need to be counted only once. T-Server checks out the number of licenses indicated by the value for this option, regardless of the number actually in use.

Warning:

- For Network T-Servers, Genesys recommends setting this option to `0` (zero).
- Be sure to configure in the Configuration Database all the DNs that agents use (Extensions and ACD Positions) and that T-Server should control.

License Checkout

The following table shows how to determine the number of seat-related DN licenses that T-Server attempts to check out:

License Checkout Rules

Options Settings 1 In this table, the following conventions are used: x and y are positive integers; `max` is the maximum number of licenses that T-Server can check out; `min (y, x)` is the lesser of the two values defined by y and x, respectively.			**License Checkout 2** The `License Checkout` column shows the number of licenses that T-Server attempts to check out. The actual number of licenses depends on license availability at the time of checkout.
num-of-licenses	num-sdn-licenses		Seat-related DN licenses
max (or 0)	max		9999
max (or 0)	x		x
max (or 0)	0		0
x	max		x
x	y		min (y, x)
x	0		0

Examples

This section presents examples of option settings in the `license` section.

Example 1

If...	**Then...**

Options Settings	License File Settings	License Checkout
num-of-licenses = max num-sdn-licenses = max	tserver_sdn = 500	500 seat-related DNs

Example 2

If...		**Then...**
Options Settings	License File Settings	License Checkout
num-of-licenses = 1000 num-sdn-licenses = max	tserver_sdn = 500	500 seat-related DNs

Example 3

If...		**Then...**
Options Settings	License File Settings	License Checkout
num-of-licenses = 1000 num-sdn-licenses = 400	tserver_sdn = 600	400 seat-related DNs

Example 4

If...		**Then...**
Options Settings	License File Settings	License Checkout
num-of-licenses = max num-sdn-licenses = 1000	tserver_sdn = 5000	1000 seat-related DNs

Translation Rules Section

The section name is specified by the `inbound-translator-<n>` option. It contains options that define the translation rules for inbound numbers.

You can choose any name for this section, provided that it matches the value of the section. Every option in this section corresponds to a rule and must conform to the format described below. You can configure as many rules as necessary to accommodate your business needs.

rule-<n>

Default Value: No default value
Valid Value: Any valid string in the following format:

- `in-pattern=<input pattern value>;out-pattern=<output pattern value>`

Changes Take Effect: Immediately

Defines a rule to be applied to an inbound number. The two parts of the option value describe the input and output patterns in the rule. When configuring the pattern values, follow the syntax defined in *Using ABNF for Rules*. See, *Configuring Number Translation* for examples of these rules as well as detailed instructions for creating rules for your installation. For example, a value for this configuration option might look like this:

- `rule-01 = in-pattern=0111#CABBB*ccD;out-pattern=ABD`

TServer Section

The TServer section contains the configuration options that are used to support the core features common to all T-Servers.

ani-distribution

ani-distribution

Default Value: inbound-calls-only
Valid Values:

- all-calls
- inbound-calls-only
- suppressed

Changes Take Effect: Immediately

Controls the distribution of the ANI information in TEvent messages.

- If the value of this option is set to all-calls, the ANI attribute is reported for all calls for which it is available.
- If the value of this option is set to inbound-calls-only, the ANI attribute is reported for inbound calls only.
- If the value of this option is set to suppressed, the ANI attribute is not reported for any calls.

background-processing

background-processing

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

If the value of this option is set to true, T-Server processes all client requests in the background, giving higher priority to the rest of the messages, which ensures that it processes these messages without any significant delay. If the value of this option is set to false, T-Server processes multiple requests from one T-Server client before proceeding to the requests from another T-Server client, and so on.

If Background Processing functionality is enabled, T-Server does the following:

- Immediately processes all switch messages and waits until there are no switch messages before processing the message queue associated with the T-Server client requests.
- Reads all connection sockets immediately and places client requests in the input buffer, which prevents T-Server clients from disconnecting because of configured timeouts.

Note: When T-Server processes client requests from the message queue, requests are processed in the order in which T-Server received them.

background-timeout

background-timeout

Default Value: `60` microseconds
Valid Values: See, Timeout Value Format.
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits before processing client requests in background mode. You must set the value of the `background-processing` configuration option to `true` in order for this option to take effect.

check-tenant-profile

check-tenant-profile

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: For the next connected client

If the value of the option is set to `true`, T-Server only allows a client to register if the client provides the correct name and password of a T-Server Tenant. If the client provides the Tenant name concatenated with a slash (`/`) and the Tenant password for the Tenant to which T-Server belongs as the value of `AttributeApplicationPassword` attribute in the `TRegisterClient` request, T-Server allows that client to register DNs that are included in the switch configuration in the Configuration Database, but it does not allow the client to register DNs that are *not* included in the switch configuration.

consult-user-data

consult-user-data

Default Value: `separate`
Valid Values:

separate	Stores user data for original and consultation calls in separate structures. The data attached to the original call is available for review or changes only to the parties of that call. The data attached to the consultation call is available only to the parties of the consultation call.
inherited	Copies user data from an original call to a consultation call when the consultation call is created; thereafter, stores user data separately for the original and the consultation call. Changes to the original call's user data are not available to the parties of the consultation call, and vice versa.
joint	Stores user data for an original call and a consultation call in one structure. The user data structure is associated with the original call, but the parties of both the original and consultation calls can see and make changes to the common user data.

Changes Take Effect: For the next consultation call created

Specifies the method for handling user data in a consultation call.

Warning: A T-Server client can also specify the `consult-user-data` mode in the `ConsultUserData` key of the `Extensions` attribute for a conference or transfer request. If it is specified, the method of handling user data is based on the value of the `ConsultUserData` key-value pair of the request and takes precedence over the T-Server `consult-user-data` option. If it is not specified in the client request, the value specified in the `consult-user-data` option applies.

customer-id

customer-id

Default Value: No default value. (A value must be specified for a multi-tenant environment.)
Valid Values: Any character string
Changes Take Effect: Immediately

Identifies the T-Server customer. You must set the value of this option to the name of the Tenant that is using this T-Server. You must specify a value for this option, if you are working in a multi-tenant environment.

Warning: Do not configure the `customer-id` option for single-tenant environments.

dn-scope

dn-scope

Default Value: `undefined`
Valid Values:

- `undefined`
- switch
- office
- tenant

Changes Take Effect: Immediately
Related Feature: See, Switch Partitioning in the Multi-Site Support PDF.

Specifies whether DNs associated with the `Switch`, `Switching Office`, or `Tenant` objects are considered in the T-Server monitoring scope, enabling T-Server to report calls to or from those DNs as internal.

- If the value of the option is set to `tenant`, all DNs associated with the switches that are within the `Tenant` are in the T-Server monitoring scope.
- If the value of the option is set to `office`, all DNs associated with the switches that are within the `Switching Office` are in the T-Server monitoring scope.
- If the value of the option is set to `switch`, all DNs associated with the `Switch` are in the T-Server monitoring scope.
- If the value of the option is set to `undefined` (the default), pre-8.x T-Server behavior applies and the switch partitioning is not turned on.

Warning: Setting the option to a value of `office` or `tenant`, which requires T-Server to monitor a large set of configuration data, may negatively affect T-Server performance.

log-trace-flags

log-trace-flags

Default Values: `+iscc, +cfg$dn, -cfgserv, +passwd, +udata, -devlink, -sw, -req, -callops, -conn, -client`
Valid Values (in any combination):

`+/-iscc`	Turns on/off the writing of information about Inter Server Call Control (ISCC) transactions.
`+/-cfg$dn`	Turns on/off the writing of information about DN configuration.
`+/-cfgserv`	Turns on/off the writing of messages from Configuration Server.
`+/-passwd`	Turns on/off the writing of `AttributePassword` in TEvents.
`+/-udata`	Turns on/off the writing of attached data.
`+/-devlink`	Turns on/off the writing of information about the link used to send CTI messages to the switch (for multi-link environments).
`+/-sw`	Reserved by Genesys Engineering.
`+/-req`	Reserved by Genesys Engineering.

`+/-callops`	Reserved by Genesys Engineering.
`+/-conn`	Reserved by Genesys Engineering.
`+/-client`	Turns on/off the writing of additional information about the client's connection.

Changes Take Effect: Immediately

Specifies—by using a space-, comma- or semicolon-separated list—the types of information that are written to the log files.

management-port

management-port

Default Value: `0` (zero)
Valid Values: `0` or any valid TCP/IP port
Changes Take Effect: After T-Server is restarted

Specifies the TCP/IP port that management agents use to communicate with T-Server. If the value is set to `0` (zero), this port is not used.

merged-user-data

merged-user-data

Default Value: `main-only`
Valid Values:

`main-only`	T-Server attaches user data from the remaining call only.

merged-only	T-Server attaches user data from the merging call.
merged-over-main	T-Server attaches user data from the remaining and the merging call. In the event of equal keys, T-Server uses data from the merging call.
main-over-merged	T-Server attaches data from the remaining and the merging call. In the event of equal keys, T-Server uses data from the remaining call.

Changes Take Effect: Immediately

Specifies the data that is attached to the resulting call after a call transfer, conference, or merge completion.

Warning: This option setting does not affect the resulting data for merging calls if the `consult-user-data` option is set to `joint`. (See, the `consult-user-data` option in this section).

server-id

server-id

Default Value: An integer equal to the `ApplicationDBID` value as reported by Configuration Server.
Valid Values: Any integer from `0` (zero)—16383
Changes Take Effect: Immediately

Specifies the `Server ID` that T-Server uses to generate `Connection IDs` and other unique identifiers. In a multi-site environment, you must assign each T-Server a unique `Server ID`, in order to avoid confusion in reporting applications and T-Server behavior.

Note: Configuration of this option is necessary for Framework environments in which there are two or more instances of the Configuration Database.

Warning:

- If you do not specify a value for this option, T-Server populates it with the `ApplicationDBID` as reported by Configuration Server. Each data object in the Configuration Database is assigned a separate DBID

that maintains a unique Server ID for each T-Server configured in the database.

- Genesys does not recommend using multiple instances of the Configuration Database.

user-data-limit

user-data-limit

Default Value: 16000 bytes
Valid Values: 0 (zero)—65535
Changes Take Effect: Immediately

Specifies the maximum size (in bytes) of user data in a packed format.

Warning: When T-Server works in a mixed 8.x/7.x/6.x environment, the value of this option must not exceed the default value of 16000 bytes; otherwise, 6.x T-Server clients might fail.

T-Server Specific Configuration Options

This section describes the configuration options unique to the T-Server for CSTA Connector and includes these topics:

- Application-Level Options
- DN-Level Options
- Agent-Specific Override Options

Note: To establish a link connection, configure the link options that are applicable to the connection protocol used in your environment (TCP/IP).

Application-Level Options

The configuration options specific to the T-Server functionality are set in Configuration Manager, in the corresponding sections on the `Options` tab of the T-Server `Application` object.

For ease of reference, the options have been arranged in alphabetical order within their corresponding sections:

Call-Type-Rules Section

This section must be called `call-type-rules`.

rule-<n>

Default Value: none
Valid Values: Any valid string in the following format :
`pattern=<input pattern>; value=<internal|external|unknown>`
Changes Take Effect: Immediately
Related Feature: Call Type Prediction

Defines a rule to be applied to an inbound number, where `n=1-N`. Multiple rules can be created and number will be matched against all patterns for those rules. As soon as first match is found then result specified in the value part of the option is used for call type assignment.

Link-Control Section

This section must be called `link-control`.

call-rq-gap

call-rq-gap

Default Value: `250`
Valid Value: Any integer from `0-1000`
Changes Take Effect: Immediately

Specifies (in milliseconds) the length of delay applied to a request issued against a busy call (a call that has another request working on it already). This prevents race conditions on the different call legs.

Set the value of this option to a time longer than the usual response time for a request from the switch.

connect-tout

connect-tout

Default Value: 2
Valid Values: Any positive integer from 1–`1000`
Changes Take Effect: On CTI link restart
Related Feature: Multiple Configured Links

Specifies the length of timeout, in seconds, T-Server waits for the CTI link with the highest priority to become operational.

device-rq-gap

device-rq-gap

Default Value: `250`
Valid Value: Any integer from `0-1000`
Changes Take Effect: Immediately

Related Feature: Request Handling Enhancements

Specifies (in milliseconds) the length of delay applied to a request issued against a busy call (a call that has another request working on it already). This prevents race conditions on the different call legs.

Set the value of this option to a time longer than the usual response time for a request from the switch.

ha-sync-dly-lnk-conn

ha-sync-dly-lnk-conn

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: At T-Server start/restart
Related Feature: Hot-Standby HA Synchronization

Determines whether the backup T-Server delays sending an `EventLinkConnected` message until it has been notified that the T-Server synchronization is complete:

- If the option is set to `true`, the backup T-Server sends an `EventLinkConnected` message once it has completed switch synchronization (that is, after all calls are cleared in the primary T-Server).
- If the option is set to `false`, there is no delay in sending an `EventLinkConnected` message and synchronization takes place the same as for pre-7.1 T-Servers.

kpl-interval

kpl-interval

Default Value: `10`
Valid Value: Any integer from `0-600`
Changes Take Effect: Immediately
Related Feature: Keep-Alive Feature Handling

Specifies a *keep-alive* interval (in seconds). To check network connectivity, T-Server issues a dummy CTI request at the interval specified when there is no other activity on the link. A value of `0` (zero) disables this feature. See, the `kpl-tolerance` option.

The value of this option may need to be increased to avoid false restarts, if the switch is slow to respond—for example, during busy periods.

kpl-loss-rate

kpl-loss-rate

Default Value: `10, 100`
Valid Value: Any single integer or comma-separated pair of integers
Changes Take Effect: Immediately
Related Feature: Keep-Alive Feature Handling

Specifies how many KPL positive responses are needed to decrement either the failure or warning tolerance counter. A value of `0` (zero) disables this option. Two comma-separated values signifies that T-Server calculates both the failure counter and the warning counter (the failure rate is always the lower value).

A single value signifies that T-Server calculates only the failure counter.

Note: This option has no effect if the value of the `kpl-tolerance` option is set to `0` (zero). In this case, a single KPL failure triggers a link restart.

kpl-tolerance

kpl-tolerance

Default Value: `3`
Valid Value: Any integer from `0-10`
Changes Take Effect: Immediately
Related Feature: Keep-Alive Feature Handling

Specifies the threshold number of accumulated failed keep-alive requests that T-Server permits before considering the CTI link to be interrupted. When this threshold is reached, T-Server treats the CTI link as either:

- Lost—T-Server tries to reconnect to the CTI link.
- Unstable—T-Server issues a warning message.

See, the `kpl-interval` option.

link-alarm-high

link-alarm-high

Default Value: 0 (zero)
Valid Values: 0-100
Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the percentage of the use-link-bandwidth option when the MSG_TS_COMMON_LINK_ALARM_HIGH LMS message is triggered.

A value of 0 (zero) disables this feature.

link-alarm-low

link-alarm-low

Default Value: 0 (zero)
Valid Values: 0-100
Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the percentage of use-link-bandwidth option when the MSG_TS_COMMON_LINK_ALARM_LOW LMS message is triggered.

max-outstanding

max-outstanding

Default Value: 8
Valid Value: Any integer from 0-1000
Changes Take Effect: Immediately

Specifies the maximum number of sent requests that are not yet acknowledged by the switch at any given time. T-Server initially sets the option to the value provided by the switch in the capability exchange service response, but if the option value is changed while T-Server is running, the new configured value takes precedence.

The option can also be set at the DN level: in the TServer section of the Annex tab of the DN object.

quiet-cleanup

quiet-cleanup

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

Disables the events that T-Server would otherwise send to clients during clean-up to notify them about the deleted calls. If the value of this option is to `true`, T-Server clients are supposed to drop all the calls upon receiving a `EventLinkDisconnected` message without waiting for T-Server notification. See also, the `restart-cleanup-limit` option.

quiet-startup

quiet-startup

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

Disables the events that T-Server would otherwise send to clients during link startup to notify clients about the changes that occurred during the link outage. If the value of the configuration option is set to `true`, clients should query T-Server after the `EventLinkConnected` event.

reg-delay

reg-delay

Default Value: `1000` milliseconds
Valid Values: `0-5000`
Changes Take Effect: Immediately

Defines the time (in milliseconds) that T-Server waits for the `DN Created` notification from Configuration Server before it starts processing the registration request from the client as a request for a DN not configured in the Configuration Layer.

reg-interval

reg-interval

Default Value: `60` seconds

Valid Values: Any integer from `0-600`
Changes Take Effect: Immediately

Specifies the time interval (in seconds) for the `Start Monitor` request to be re-sent to the switch if the initial request fails. A value of `0` (zero) switches this feature off.

reg-silent

reg-silent

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

- If this option is set to a value of `true`, T-Server reports `EventRegistered` for *on-demand* registration with the PBX when the procedure is completed.
- If this option is set to a value of `false`, T-Server reports `EventRegistered` as early as possible during the PBX registration procedure.

restart-cleanup-dly

restart-cleanup-dly

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the delay, in seconds, for T-Server to keep *unreliable* calls after link startup. This delay allows T-Server to salvage calls that existed before the link failure (for which any events were received) if T-Server was unable to verify their existence using snapshot. A value of `0` (zero) means any non-verified calls are cleared up immediately after the completion of the link startup.

restart-cleanup-limit

restart-cleanup-limit

Default Value: `0` (zero)
Valid Values: Any positive integer
Changes Take Effect: Immediately

Defines the maximum number of reconnect attempts for calls (and possibly agent logins) in T-Server

during link outage. A value of `0` (zero) means all of the calls are deleted immediately after the link failure. See, the `restart-period` option.

restart-period

restart-period

Default Value: `20` seconds
Valid Values: `0-600`
Changes Take Effect: Immediately

Specifies the interval (in seconds) that T-Server waits between attempts to reconnect to the switch when the link fails. A value of `0` (zero) means that T-Server does not try to reconnect unless the link configuration is changed.

rq-conflict-check

rq-conflict-check

Default Value: `true`
Valid Value: `true`, `false`
Changes Take Effect: Immediately
Related Feature: Request Handling Enhancements

Specifies whether request conflict resolution is enabled. Request conflict resolution intelligently resolves any conflicting client requests.

rq-expire-tout

rq-expire-tout

Default Value: `10000` milliseconds
Valid Value: Any positive integer from `0-30000`
Changes Take Effect: Immediately

Specifies the interval (in milliseconds) that T-Server waits before deleting pending requests (these are requests for which it has received no notification from the switch) from clients.

This timeout should be set to a value higher than the system latency.

rq-gap

rq-gap

Default Value: `0` (zero)
Valid Value: Any integer from `0-1000`
Changes Take Effect: Immediately

Specifies the minimum time interval (in milliseconds) between succeeding CTI requests sent over the link. You can adjust the value to meet the CTI-link load and performance requirements.

use-link-bandwidth

use-link-bandwidth

Default Value: `auto`
Valid Values: `0-999, auto`
Changes Take Effect: Immediately
Related Feature: Link Bandwidth Monitoring

Specifies the maximum number of requests per second throughput to be used by T-Server to calculate the link alarm messages. A value of `0` (zero) disables this feature.

Link-tcp Section

For the following configuration options, you must specify if a connection to the CSTA Connector is configured using the `link-n-name` option. This section's name is specified by the `link-n-name` option. If redundant links are used, there must be a `link-n-name` section for each redundant link, a `link-1-name` for the first link section, and a `link-2-name` for the second link, and so on. At start-up, T-Server initiates a connection for each link.

To establish a link connection, simply configure the link options (TCP/IP) that are applicable to the connection protocol used in your environment.

Note:

1. If T-Server is not yet connected and one of the link sections is reconfigured, T-Server attempts to reconnect using new link properties at the next scheduled reconnect attempt.
2. If an active link is reconfigured, then T-Server drops the connection and starts the re-connection procedure using the new link properties. This behavior is due to the specific implementation of link reconfiguration in the T-Server Common Part.

hostname

hostname

Default Value: Mandatory field. No default value.
Valid Value: Any valid host name or numeric IP address
Changes Take Effect: Immediately

Specifies the host name or IP address of the CSTA Connector server to which T-Server connects. You *must* specify a value for this option.

port

port

Default Value: `1040`
Valid Value: Any valid TCP port address
Changes Take Effect: Immediately

Specifies the TCP/IP port address of the CSTA Connector server.

SwitchSpecificType Section

This section must be called `SwitchSpecificType` and contains the options for all type of devices that T-Server supports. The configuration options for a specific device type exists in the configuration section when:

- The device type is supported by T-Server.
- T-Server supports more then one Switch Specific Type (excluding the Switch Specific Types for the reserved DN)for this supported device type.

T-Server clients are able to override the default value for a switch-specific type by using the `SwitchSpecificType Extensions` attribute key provided in the `TRegisterAddress` request.

acd-position

acd-position

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `ACD Position` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `ACD Position` (`AddressTypePosition`) that are not configured in the Configuration Layer.

acd-queue

acd-queue

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `ACD Queue` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `ACD Queue` (`AddressTypeQueue`) that are not configured in the Configuration Layer.

data

data

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Data Channel` (`Modem` in the configuration environment) supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Modem` (`AddressTypeDataChannel`) that are not configured in the Configuration Layer.

extension

extension

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Extension` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Extension` (`AddressTypeDN`) that are not configured in the Configuration Layer.

music

music

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Music Port` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Music Port` (`AddressTypeAnnouncement`) that are not configured in the Configuration Layer.

routing-point

routing-point

Default Value: `0` (zero)

Valid Value: Switch-specific types for DN of type `Routing Point` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Routing Point` (`AddressTypeRouteDN`) that are not configured in the Configuration Layer.

routing-queue

routing-queue

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Routing Queue` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Routing Queue` (`AddressTypeRouteQueue`) that are not configured in the Configuration Layer.

trunk

trunk

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Routing Point` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Trunk` or `Tie Line` (`AddressTypeTrunk`) that are not configured in the Configuration Layer.

voicemail

voicemail

Default Value: `0` (zero)
Valid Value: Switch-specific types for DN of type `Voice Mail` supported by T-Server
Changes Take Effect: Immediately

Defines the switch-specific type that T-Server uses for registration of DNs of type `Voice Mail` (`AddressTypeVoiceChannel`) that are not configured in the Configuration Layer.

TServer Section (General)

General TServer Section Options

All of the options in this section must be called TServer.

accept-dn-type

accept-dn-type

Default Value: +acdqueue +announcement +data +extension +position +routedn +routequeue +trunk +voicemail
Valid Values:
+/-acdqueue—Accepts or rejects registration on DN of type ACD Queue (AddressTypeQueue)
+/-announcement—Accepts or rejects registration on DN of type Music Port (AddressTypeAnnouncement)
+/-data—Accepts or rejects registration on DN of type Modem (AddressTypeDataChannel)
+/-extension—Accepts or rejects registration on DN of type Extension (AddressTypeDN)
+/-position—Accepts or rejects registration on DN of type Position (AddressTypePosition)
+/-routedn—Accepts or rejects registration on DN of type Routing Point (AddressTypeRouteDN)
+/-routequeue—Accepts or rejects registration on DN of type Route Queue (AddressTypeRouteQueue)
+/-trunk—Accepts or rejects registration on DN of type trunk or tie line (AddressTypeTrunk)
+/-voicemail—Accepts or rejects registration on DN of type Voice Mail (AddressTypeVoiceChannel)
Changes Take Effect: Immediately

Defines the supported set of device types that are not configured in the Configuration Layer, but that T-Server can register.

Note: All possible values are listed here, however, this set is T-Server specific.

agent-only-private-calls

agent-only-private-calls

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

Specifies whether T-Server will classify a call as `private` when the initial business type of the call is `unknown` and there is no agent on the call in situations, but if an agent was on the call, the classification would be private.

- If the value of this option is set to `true`—the call remains as business type, `unknown`, when no agent is on the call, where the business type classification would be changed from `unknown` to `private`, if an agent was on the call.
- If the value of this option is set to `false`—calls with no agent(s) on the call are classified as `private` instead of being left as business type, `unknown`.

agent-group

agent-group

Default Value: `none`
Valid Value: Any agent group value
Changes Take Effect: At the next agent login session

Specifies a value for a virtual group to be used for T-Server reporting.

T-Server obtains the value for this option in the following order of precedence:

1. In the `TServer` section of the `Annex` tab of the `Agent Login` object
2. In the `TServer` section of the `Annex` tab of the`DN` object
3. In the main `TServer` section.

callback-dn

callback-dn

Default Value: `CallbackDN`
Valid Values: Any valid string representing a simulated DN
Changes Take Effect: Immediately

Sets the value of the third party DN used in reporting call back scenario as a simulated single-step transfer.

consult-supervised-rt

consult-supervised-rt

Default Value: `false`

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

Specifies whether T-Server allows supervised routing of consultation calls. If this option is set to a value of `false`, T-Server forces non-supervised routing for consultation calls, regardless of the configuration option or call-by-call settings.

Note: When set at the `Application`-level, this option defines the default value for all Routing Points. However, this option can also be specified on the `Annex` tab of `Routing Point` DNs, in which case it overrides the option set at the `Application`-level.

correct-connid

correct-connid

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

If the value of this option is set to `true`, T-Server corrects the wrong `ConnectionID` provided by the application in CTI requests. If the value of this option is set to `false,` this feature is disabled.

correct-rqid

correct-rqid

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

If the value of this option is set to `true,` T-Server corrects the wrong CTI client request. If the value of this option is set to `false`, this feature is disabled.

default-dn-type

default-dn-type

Default Value: `none`, `extension`, `position`
Valid Values:

- `acdqueue`—T-Server uses the `AddressTypeQueue` value
- `announcement`—T-Server uses the `AddressTypeAnnouncement` value

- data—T-Server uses the AddressTypeDataChannel value
- extension—T-Server uses the AddressTypeDN value
- none—T-Server assigns the DN type using the PBX-provided information
- position—T-Server uses the AddressTypePosition value
- trunk—T-Server uses the AddressTypeTrunk value
- voicemail—T-Server uses the AddressTypeVoiceChannel value

Changes Take Effect: Immediately

Defines the value that T-Server applies for the AttributeAddressType attribute when the client does not provide it or provides the value, AddressTypeUnknown, instead.

Note: All possible values are listed here, however, this set is T-Server specific.

dn-del-mode

dn-del-mode

Default Value:idle
Valid Values: never, idle, force, Timeout Value Format

- never—T-Server does not unregister the DN with the PBX and the device-related information is never deleted from the T-Server memory.
- idle—T-Server unregisters the DN with the PBX and the device-related information is deleted from the T-Server memory as soon as there are no more calls on this device.
- force—T-Server unregisters the DN with the PBX and the device-related information is deleted from the T-Server memory regardless of whether any calls exist on that DN.
- Timeout Value Format—T-Server applies a defined delay before unregistering the DN after the last call has left that DN. The valid value, idle is equivalent to setting the Timeout Value to 0 (zero).

Changes Take Effect: Immediately

Defines how T-Server handles device and device-related information when the DN is not configured in the Configuration Layer and there are no clients registered on that DN.

enable-rp-tout

enable-rp-tout

Default Value: 0 (zero)
Valid Values: See the Timeout Value Format section in the Framework 8.x T-Server for CSTA Connector

Deployment Guide
Changes Take Effect: Immediately

Specifies the time interval that T-Server waits before enabling message routing on a Routing Point that has message routing disabled outside of T-Server control. When the value of this configuration option is set to `0` (zero), T-Server does not attempt to re-enable routing on such a disabled Routing Point.

link-control

link-1-name

Default Value: None. This option is required if the `link-control` section is not specified. Valid Values: Any valid section name.
Changes Take Effect: At next system restart

Specifies the section name where the CTI link options are specified.

link-n-name

link-n-name

Default Value: `link-tcp` The `link-tcp` section is required, if the connection to the CSTA Connector is not configured using the `Application` object's `Connections` tab
Valid Values: Any valid section name.
Changes Take Effect: Immediately

Specifies the section name that contains the configuration options assigned to the link for the connection to the CSTA Connector, where *n* is a consecutive number for a CTI link. The `link-control` section options only define the link handling—for example, the number of restarts, gaps, and so on. You *must* specify a value for this option.

The `link-n-name` option name refers to the link number and the section name—for example, `link-1-name`.

Warning: Do not update the link configuration while T-Server is running. Doing so causes a temporary disconnection. If that happens, you must validate each configuration option contained in the link section to reestablish the connection.

max-pred-req-delay

max-pred-req-delay

Default Value: 3 seconds
Valid Value: Any integer from `0-10`
Changes Take Effect: Immediately

Defines the maximum time (in seconds) that T-Server waits for a free dialing resource to become available before rejecting a `TMakePredictiveCall` request.

nas-indication

nas-indication

Default Value: `none`
Valid Values:

- `none`—No `ReasonCode` attribute or `Extensions` attribute is provided in the `EventReleased` event.
- `ext`—The `NO_ANSWER_TIMEOUT` `Extensions` attribute is supplied in the `EventReleased` event.
- `rsn`—The `NO_ANSWER_TIMEOUT` `ReasonCode` attribute is supplied in the `EventReleased` event.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies the reporting action in the `EventReleased` event when No-Answer Supervision overflows a call. See, `no-answer-timeout`.

retain-call-tout

retain-call-tout

Default Value: 15 seconds
Valid Value: Any integer from `0-3600`
Changes Take Effect: Immediately

Specifies the time interval (in seconds) that T-Server waits before deleting information about calls that are completed, but for which it has received no notification from the switch.

show-supervisor-dns

show-supervisor-dns

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

Specifies whether T-Server distinguishes supervisor DNs from regular parties in the `Extensions` attribute when reporting transfer and/or conference calls. Enables the special reporting of Supervisor DNs in transfer and conference call scenarios.

- If the value of this option is set to `true`, T-Server differentiates between the supervising devices and reports them as the `OrigSV-n` and `ConsultSV-n` keys of the `Extensions` attribute (as opposed to regular party reporting that uses the `OrigDN-n` and `ConsultDN-n` keys of the `Extensions` attribute).
- If the value of this option is set to `false`, T-Server reports supervising parties as regular parties using the `Extensions` attribute keys, `OrigDN` and `ConsultDN` in transfer and/or conference calls.

Note: Since the supervisor presence no longer makes a two-party call into a conference call, if this option is enabled, the `OtherDN` attribute is reported the same as if the call was monitored.

supervised-route-timeout

supervised-route-timeout

Default Value: 5 seconds
Valid Value: Any integer from `0-600`
Changes Take Effect: Immediately

Specifies the interval (in seconds) that T-Server waits for a call to be answered that is routed from an Routing Point using supervised routing. If the call is not answered within the period specified, T-Server recalls the call to the Routing Point and initiates rerouting. A value of `0` (zero) deactivates this feature. See, agent-no-answer-timeout.

This timeout should be set to a value higher than the system latency.

Notes:

- You can use the `Extensions` attribute, `SUPERVISED_ROUTE`, to override the value of this configuration option on a call-by-call basis. See the Using the Extensions Attribute topic for more information.
- When set in the `TServer` section, this option defines the default value for all Routing Points. However, you can also set a value for this option on the `Annex` tab of DNs of type `Routing Point` in a section called `TServer`. When set there, this value overrides the default value for the specific Routing Point. You can also use the `Extensions` attribute, `SUPERVISED_ROUTE`, to override the value of this configuration option on a call-by-call basis.

- In order for the supervised routing feature to be able to recall the call to the Routing Point, no Bounced Calls should be configured on the Routing Point in the switch configuration.

unknown-xfer-merge-udata

unknown-xfer-merge-udata

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

If the value of this option is set to `true`, T-Server copies the user data from the current monitored call to the call transferred from an unmonitored destination. Because the primary call was hitherto unknown, normal user data inheritance mechanisms cannot be used. Use this option with the `merge-user-data` option.

TServer Section (Feature)

TServer Section Options Listed by Supported Features

Refer to the topics under the following supported features table to see the descriptions of their related options where appropriate. All of the options in this section must be called `TServer`.

Feature	Related Configuration Options
Account Codes	Account Codes Configuration Options
Agent Substitution for Monitored Agents	Agent Substitution for Monitored Agents Configuration Options
Business-Call Handling	Business-Call Handling Configuration Options
Call Recording	Call Recording Configuration Options
Call Release Tracking	Call Release Tracking Configuration Options
Call Type Prediction	Call Type Prediction Configuration Options
Emulated Agents	Emulated Agents Configuration Options
Failed-Route Notification	Failed-Route Notification Configuration Options
Hot-Standby HA	Hot-Standby HA Configuration Options
Keep-Alive Feature	Keep-Alive Feature Configuration Options
Link Bandwidth Monitoring	Link Bandwidth Monitoring Configuration Options
Multiple Configured Links	Multiple Configured Links Configuration Options
No-Answer Supervision	No-Answer Supervision Configuration Options
Request Handling Enhancements	Request Handling Enhancements Configuration Options
Smart OtherDN Handling	Smart OtherDN Handling Configuration Options

Feature	Related Configuration Options
Unregistered DNs	Unregistered DNs Configuration Options

DN-Level Options

TServer Section

You can only set the configuration options described in this section in the `TServer` section of the Annex tab of the relevant configuration object in the Configuration Layer. You cannot define them in the main `TServer` configuration section.

agent-emu-login-on-call

agent-emu-login-on-call

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server allows an emulated agent login or logout on a device where there is a call in progress.

This option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The `TServer` section of the `Annex` tab of the `Agent Login` object.
2. The `TServer` section of the `Annex` tab of a device.
3. The `TServer` section of the application.

The value can also be set by using the `AgentEmuLoginOnCall` `Extensions` attribute in the `TAgentLogin` or `TAgentLogout` requests. The value specified by the extension, where present, takes precedence over the settings configured in the Configuration Layer.

agent-logout-on-unreg

agent-logout-on-unreg

Default Value: `false`
Valid Values:

- `true`—T-Server logs out emulated and native agents on unregister.

- false—T-Server does not log out emulated or native agents on unregister.
- emu-only—T-Server logs out only emulated agents on unregister.

Changes Take Effect: At the next agent login session
Related Feature: Emulated Agents

Specifies whether T-Server performs an automatic logout of an agent whenever their client application unregisters the DN from T-Server. This happens whenever a client application disconnects from T-Server.

The option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The TServer section in the Annex tab of the device representing the agent's group (such as an ACD queue).
2. The TServer section of the Annex tab of the Agent Login object.
3. TheTServer section of the Annex tab of a device.
4. The TServer section of the application.

The Configuration Layer configuration setting may be overridden by adding the AgentLogoutOnUnregister Extensions attribute to the TAgentLogin request.

Any subsequent self-transition TAgentLogin request can override the current agent association by adding the AgentLogoutOnUnregister Extensions attribute with a value of true.

Similarly a TRegisterAddress request can override the current agent association by adding the AgentLogoutOnUnregister Extensions attribute with a value of true.

bsns-call-type

bsns-call-type

Default Value: none
Valid Values:

business—The call is classified as a business call.
private—The call is classified as a private call.
ignore—The distribution point has no effect on business call classification.

Changes Take Effect: Immediately
Related Feature: Business-Call Handling

Specifies the business call type for calls that pass through or arrive at the associated device.

Note: This option takes precedence over the following options that are set at the Application-level: inbound-bsns-calls, inherit-bsns-type, and outbound-bsns-calls. This option may be over-ridden by the BusinessCallType Extenstions attribute.

dn-for-undesired-calls

dn-for-undesired-calls

Default Value: No default value
Valid Values: Any valid switch DN
Changes Take Effect: Immediately
Related Feature: Smart OtherDN Handling

Specifies the DN that T-Server uses as the request destination if the client provides a reserved DN in the request.

Note: You can set a value for this option in the appropriate DN Annex tab in the TServer section. When set there, this value overrides the default value for the DN.

emulate-login

emulate-login

Default Value: on-RP
Valid Values:

- true—T-Server performs an emulated login.
- false—T-Server passes a login request to the PBX.
- on-RP—T-Server checks the Agent Group associated with the login request. If the Agent Group is a standard Routing Point, then the emulated login request succeeds. This value can only be set at the Application-level, and is available for backwards compatibility.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server performs an emulated agent login when the login device is configured in the Configuration Layer as a device of type extension.

This value can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next highest level, and so on.

1. In the TAgentLogin request, using the EmulateLogin key of the Extensions attribute.
2. In the TServer section of the Annex tab of the Agent Login object.
3. In the TServer section of the Annex tab of the login device object.
4. In the device representing an Agent Group object, on the Annex tab.

5. In the T-Server Application object, in the Tserver section.
6. Using an Agent Group corresponding to an object that is configured in the Configuration Layer as a device of type Routing Point.

emulated-login-state

emulated-login-state

Default Value: ready
Valid Values:

- not-ready—T-Server distributes EventAgentNotReady after EventAgentLogin.
- ready—T-Server distributes EventAgentReady after EventAgentLogin.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

When T-Server performs an emulated agent login and the client specifies an agent work mode other than ManualIn or AutoIn, T-Server uses this option to determine which event to distribute.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the Agent Login object on the Annex tab.
2. In the agent login device on the Annex tab.
3. In the login device representing an Agent Group object during login, on the Annex tab.
4. In the T-Server Application object in the Tserver section.

legal-guard-time

legal-guard-time

Default Value: 0 (zero)
Valid Value: Any integer from 0-30
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies a legal-guard time (in seconds) for emulated agents to postpone the transition to the Ready state after a business call. T-Server always considers a routed call a business call.

max-outstanding

max-outstanding

Default Value: `0` (zero)
Valid Values: `0-100`
Changes Take Effect: Immediately

Specifies the maximum number of outstanding sent requests awaiting the response from the link. T-Server must wait for a request response event for a request on this particular device before submitting any further requests.

nas-private

nas-private

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies whether No-Answer Supervision should be applied to private calls.

Note: When set in the `TServer` section, this option defines the default value for all private calls. However, you can also set a value for this option on the `Annex` tab of DNs of type `Extension` or `Agent Login` in the section called `TServer`. When this option is set there, this value overrides the default value for the specific DN.

no-answer-overflow

no-answer-overflow

Default Value: No default value
Valid Values:

- `none`—T-Server does not attempt to overflow a call on an agent desktop when `agent-no-answer-timeout` expires. T-Server treats this value as the end of a list. Subsequent values are not executed.
- `recall`—T-Server returns the call to the last distribution device (the device reported in the `ThisQueue` attribute of the call) when `agent-no-answer-timeout` expires.
- `release`—T-Server releases the call.

- default—T-Server stops execution of the current overflow sequence and continues with the T-Server default overflow sequence defined by the relevant overflow option in the mainTServer section.
- Any valid overflow destination—T-Server returns the call to the specified destination when agent-no-answer-timeout expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

The value of the option overrides any of the following T-Server configuration options set at the Application-level for the object where it has been set (depending on the type of configuration object):

- agent-no-answer-overflow, if defined for an Agent Login object.
- extn-no-answer-timeout, if defined for an Extension object.

T-Server attempts to apply the overflow in the order that is listed. If the first overflow destination fails, then T-Server attempts the next one in the list. If all overflow destinations in the list fail, then T-Server abandons overflow. If the list of overflow destinations contains the value recall and the call was not distributed, T-Server skips to the next destination in the list.

no-answer-timeout

no-answer-timeout

Default Value: Same as the value in the corresponding option set at the Application-level
Valid Value: Any integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time (in seconds) that T-Server waits for a call to be answered that is ringing on the device in question. When the timer expires, T-Server applies the appropriate overflow, and, in the case of agents, the appropriate logout or NotReady action.

A value of 0 (zero) deactivates the no-answer supervision for this device.

When set, this option overrides any of the following T-Server configuration options set at the Application-level for the object where it has been set (depending on type of configuration object):

- agent-no-answer-timeout, if defined for an Agent Login object.
- extn-no-answer-timeout, if defined for an Extension object.

override-switch-acw

override-switch-acw

Default Value: `false`
Valid Values:

- `true`—T-Server overrides the switch ACW.
- `false`—ACW overrides the emulated ACW.

Changes Take Effect: Immediately

Specifies whether T-Server emulated ACW overrides the switch ACW for calls distributed through a Routing Point.

This option can be set in Configuration Manager in the following places in order of precedence (highest to lowest):

1. In the `TServer` section in the `Annex` tab of DNs of type `Routing Point`.
2. In the `TServer` section of the `Options` tab of the T-Server `Application` object.

prd-dist-call-ans-time

prd-dist-call-ans-time

Default Value: `0` (zero)
Valid Value: Any positive integer from `0-10`
Changes Take Effect: Immediately

Specifies the time interval (in seconds) during which an agent can answer a predictive call before T-Server abandons it. If the value is set to `0` (zero), T-Server does not automatically abandon the call, which then rings on the agent desktop until it is answered.

When an emulated predictive dial is made from an emulated Routing Point, and the `nas-indication` and `supervised-route-timeout` configuration options are set, the value in the `prd-dist-call-ans-time` option takes precedence. For predictive dialing to work, you must set values greater than `0` (zero) for both options.

See, Related Configuration Options for a description of the options mentioned in this topic.

This option can be defined in two places:

1. In the T-Server `Application` object, which defines the default value to be applied for the predictive calls initiated from all distribution devices.
2. In the `TServer` section in the `Annex` tab of any ACD Queue or Routing Point that is to be used as the origination device for a predictive call. When this option is set there, this value overrides the value of the T-Server option set at the `Application`-level for all calls that originate from that ACD Queue or Routing Point.

Note: When using T-Server 8.0 with Outbound Contact Server (OCS) 7.6 or lower, this option must be set to 0 (zero).

recall-no-answer-timeout

recall-no-answer-timeout

Default Value: 15
Valid Values: Any positive integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time that T-Server waits for a call to re-appear on a device as a result of a recall—for example: a ringback waiting to be answered. When the timer expires, T-Server executes the actions defined by the relevant overflow option, as well as the action option for cases where an agent is logged in.

There is no No-Answer Supervision for such calls, if the value is set to 0 (zero).

This option can be defined either in the main Tserver section or in a section called TServer on the Annex tab of any of the following configuration object types in Configuration Manager:

- Extension
- ACD Position
- Voice Treatment Port
- Agent Login

rq-gap

rq-gap

Default Value: 0 (zero)
Valid Value: Any integer from 0-1000
Changes Take Effect: Immediately

Specifies the minimum interval (in milliseconds) between succeeding CTI requests sent over the link. You can adjust the value to meet CTI-link load and performance requirements.

You can set this option in the TServer section in the Annex tab of a device.

sync-emu-acw

sync-emu-acw

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server synchronizes emulated ACW for native agents.

This option can be set in Configuration Manager in the following places in order of precedence (highest to lowest):

1. In the `TServer` section in the `Annex` tab of an `Agent Login` object.
2. In the `TServer` section in the `Annex` tab of a device.
3. In the `TServer` section of the application.

The `SyncEmuACW` `Extensions` attribute of the `TAgentLogin` request overrides the value configured for this option.

wrap-up-time

wrap-up-time

Default Value: `0` (zero)
Valid Value: Any positive integer, `untimed`

`0` (zero)	ACW is disabled. Exception: If this option is set in the `Annex` tab of the `Agent Login` object, a value of `0` (zero) means that T-Server processes from Step 4 in the processing order of precedence below.
A value greater than `0` (zero), but less than the value set for the `untimed-wrap-up-value` option.	The number of seconds of timed ACW, after which T-Sever returns the agent automatically to the Ready state.

A value equal to the value set for the untimedwrap-up-value option.	ACW is untimed and the agent must manually return to the Ready state.
A value greater than the value set for the untimed-wrap-up-value option.	Disables ACW.
untimed	ACW is untimed and the agent must manually return to the Ready state. **Note:** This value cannot be set on the Annex tab of an Agent Login object.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the amount of wrap-up time (ACW) allocated to emulated agents at the end of a business call.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the WrapUpTime Extensions attribute key of the TAgentPendingACW request (applies to this agent only).
2. In the WrapUpTime Extensions attribute key of the TACWInIdle request (applies to this agent only).
3. In the call, in the WrapUpTime UserData attribute (limited to ISCC scenarios).
4. In a DN configuration object of type ACD Queue or Routing Point, on the Annex tab in the TServer section.
5. In the WrapUpTime Extensions attribute key of the TAgentLogin request, (applies to this agent only).
6. In the Agent Login configuration object, on the Annex tab in the TServer section (but not including the untimed value).
7. Using an Agent Group corresponding to an object configured in the Configuration Layer as a device of type ACD Queue.
8. In the T-Server Application object, on the Options tab in the TServer section.

Agent-Specific Override Options

TServer Section

You can only set the configuration options described in this section in the `TServer` section of the Annex tab of the relevant configuration object in the Configuration Layer for individual agents in the Framework Configuration Layer, therefore they need to be listed separately. You cannot define them in the main `TServer` configuration section.

agent-emu-login-on-call

agent-emu-login-on-call

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server allows an emulated agent login or logout on a device where there is a call in progress.

This option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The `TServer` section of the `Annex` tab of the `Agent Login` object.
2. The `TServer` section of the `Annex` tab of a device.
3. The `TServer` section of the application.

The value can also be set by using the `AgentEmuLoginOnCall` `Extensions` attribute in the `TAgentLogin` or `TAgentLogout` requests. The value specified by the extension, where present, takes precedence over the settings configured in the Configuration Layer.

agent-logout-on-unreg

agent-logout-on-unreg

Default Value: `false`
Valid Values:

- `true`—T-Server logs out emulated and native agents on unregister.

- false—T-Server does not log out emulated or native agents on unregister.
- emu-only—T-Server logs out only emulated agents on unregister.

Changes Take Effect: At the next agent login session
Related Feature: Emulated Agents

Specifies whether T-Server performs an automatic logout of an agent whenever their client application unregisters the DN from T-Server. This happens whenever a client application disconnects from T-Server.

The option can be set in the Configuration Layer in the following places in order of precedence (highest to lowest):

1. The TServer section in the Annex tab of the device representing the agent's group (such as an ACD queue).
2. The TServer section of the Annex tab of the Agent Login object.
3. TheTServer section of the Annex tab of a device.
4. The TServer section of the application.

The Configuration Layer configuration setting may be overridden by adding the AgentLogoutOnUnregister Extensions attribute to the TAgentLogin request.

Any subsequent self-transition TAgentLogin request can override the current agent association by adding the AgentLogoutOnUnregister Extensions attribute with a value of true.

Similarly a TRegisterAddress request can override the current agent association by adding the AgentLogoutOnUnregister Extensions attribute with a value of true.

emulate-login

emulate-login

Default Value: on-RP
Valid Values:

- true—T-Server performs an emulated login.
- false—T-Server passes a login request to the PBX.
- on-RP—T-Server checks the Agent Group associated with the login request. If the Agent Group is a standard Routing Point, then the emulated login request succeeds. This value can only be set at the Application-level, and is available for backwards compatibility.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server performs an emulated agent login when the login device is configured in

the Configuration Layer as a device of type extension.

This value can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next highest level, and so on.

1. In the TAgentLogin request, using the EmulateLogin key of the Extensions attribute.
2. In the TServer section of the Annex tab of the Agent Login object.
3. In the TServer section of the Annex tab of the login device object.
4. In the device representing an Agent Group object, on the Annex tab.
5. In the T-Server Application object, in the Tserver section.
6. Using an Agent Group corresponding to an object that is configured in the Configuration Layer as a device of type Routing Point.

emulated-login-state

emulated-login-state

Default Value: ready
Valid Values:

- not-ready—T-Server distributes EventAgentNotReady after EventAgentLogin.
- ready—T-Server distributes EventAgentReady after EventAgentLogin.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

When T-Server performs an emulated agent login and the client specifies an agent work mode other than ManualIn or AutoIn, T-Server uses this option to determine which event to distribute.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the Agent Login object on the Annex tab.
2. In the agent login device on the Annex tab.
3. In the login device representing an Agent Group object during login, on the Annex tab.
4. In the T-Server Application object in the Tserver section.

legal-guard-time

legal-guard-time

Default Value: `0` (zero)
Valid Value: Any integer from `0-30`
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies a legal-guard time (in seconds) for emulated agents to postpone the transition to the Ready state after a business call. T-Server always considers a routed call a business call.

monitor

monitor

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

Specifies whether the switch should monitor the agent. The value of the `monitor` configuration option overrides any value of the `monitor-agents` configuration option set at the `Application`-level.

nas-private

nas-private

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Specifies whether No-Answer Supervision should be applied to private calls.

Note: When set in the `TServer` section, this option defines the default value for all private calls. However, you can also set a value for this option on the `Annex` tab of DNs of type `Extension` or `Agent Login` in the section called `TServer`. When this option is set there, this value overrides the default value for the specific DN.

no-answer-action

no-answer-action

Default Value: none
Valid Values:

none—T-Server takes no action on agents when business calls are not answered.
notready—T-Server sets agents NotReady when business calls are not answered.
logout—T-Server automatically logs out agents when business calls are not answered.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

The value of the no-answer-action option overrides any value of the agent-no-answer-action configuration option set at the Application-level. See, Related Configuration Options for a description of the configuration options mentioned in this topic.

This option is defined in a section called TServer on the Annex tab of any Agent Login object in the Configuration Layer. If an emulated or real PBX agent receives a T-Server business call and the agent fails to answer the call within the time defined in agent-no-answer-timeout configuration option, the no-answer-action configuration option determines the action T-Server performs on this agent.

Note: If a call is abandoned before either agent-no-answer-timeout, no-answer-timeout, or supervised-route-timeout expires (depending on which timer is applicable), T-Server performs no action on this agent.

no-answer-overflow

no-answer-overflow

Default Value: No default value
Valid Values:

- none—T-Server does not attempt to overflow a call on an agent desktop when agent-no-answer-timeout expires. T-Server treats this value as the end of a list. Subsequent values are not executed.
- recall—T-Server returns the call to the last distribution device (the device reported in the ThisQueue attribute of the call) when agent-no-answer-timeout expires.
- release—T-Server releases the call.
- default—T-Server stops execution of the current overflow sequence and continues with the T-Server default overflow sequence defined by the relevant overflow option in the mainTServer section.
- Any valid overflow destination—T-Server returns the call to the specified destination when agent-no-answer-timeout expires.

Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

The value of the option overrides any of the following T-Server configuration options set at the Application-level for the object where it has been set (depending on the type of configuration object):

- agent-no-answer-overflow, if defined for an Agent Login object.
- extn-no-answer-timeout, if defined for an Extension object.

T-Server attempts to apply the overflow in the order that is listed. If the first overflow destination fails, then T-Server attempts the next one in the list. If all overflow destinations in the list fail, then T-Server abandons overflow. If the list of overflow destinations contains the value recall and the call was not distributed, T-Server skips to the next destination in the list.

no-answer-timeout

no-answer-timeout

Default Value: Same as the value in the corresponding option set at the Application-level
Valid Value: Any integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time (in seconds) that T-Server waits for a call to be answered that is ringing on the device in question. When the timer expires, T-Server applies the appropriate overflow, and, in the case of agents, the appropriate logout or NotReady action.

A value of 0 (zero) deactivates the no-answer supervision for this device.

When set, this option overrides any of the following T-Server configuration options set at the Application-level for the object where it has been set (depending on type of configuration object):

- agent-no-answer-timeout, if defined for an Agent Login object.
- extn-no-answer-timeout, if defined for an Extension object.

recall-no-answer-timeout

recall-no-answer-timeout

Default Value: 15
Valid Values: Any positive integer from 0-600
Changes Take Effect: Immediately
Related Feature: No-Answer Supervision

Defines the time that T-Server waits for a call to re-appear on a device as a result of a recall—for example: a ringback waiting to be answered. When the timer expires, T-Server executes the actions defined by the relevant overflow option, as well as the action option for cases where an agent is logged in.

There is no No-Answer Supervision for such calls, if the value is set to 0 (zero).

This option can be defined either in the main Tserver section or in a section called TServer on the Annex tab of any of the following configuration object types in Configuration Manager:

- Extension
- ACD Position
- Voice Treatment Port
- Agent Login

sync-emu-acw

sync-emu-acw

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies whether T-Server synchronizes emulated ACW for native agents.

This option can be set in Configuration Manager in the following places in order of precedence (highest to lowest):

1. In the TServer section in the Annex tab of an Agent Login object.
2. In the TServer section in the Annex tab of a device.
3. In the TServer section of the application.

The SyncEmuACW Extensions attribute of the TAgentLogin request overrides the value configured for this option.

wrap-up-time

wrap-up-time

Default Value: 0 (zero)
Valid Value: Any positive integer, untimed

0 (zero)	ACW is disabled. Exception: If this

	option is set in the Annex tab of the Agent Login object, a value of 0 (zero) means that T-Server processes from Step 4 in the processing order of precedence below.
A value greater than 0 (zero), but less than the value set for the untimed-wrap-up-value option.	The number of seconds of timed ACW, after which T-Sever returns the agent automatically to the Ready state.
A value equal to the value set for the untimedwrap-up-value option.	ACW is untimed and the agent must manually return to the Ready state.
A value greater than the value set for the untimed-wrap-up-value option.	Disables ACW.
untimed	ACW is untimed and the agent must manually return to the Ready state. **Note:** This value cannot be set on the Annex tab of an Agent Login object.

Changes Take Effect: Immediately
Related Feature: Emulated Agents

Specifies the amount of wrap-up time (ACW) allocated to emulated agents at the end of a business call.

This option can be set in a number of places, and T-Server processes it in the order of precedence shown below, highest first. If the value is not present at the higher level, T-Server checks the next level, and so on.

1. In the WrapUpTime Extensions attribute key of the TAgentPendingACW request (applies to this agent only).
2. In the WrapUpTime Extensions attribute key of the TACWInIdle request (applies to this agent only).
3. In the call, in the WrapUpTime UserData attribute (limited to ISCC scenarios).
4. In a DN configuration object of type ACD Queue or Routing Point, on the Annex tab in the TServer section.
5. In the WrapUpTime Extensions attribute key of the TAgentLogin request, (applies to this agent only).

6. In the `Agent Login` configuration object, on the `Annex` tab in the `TServer` section (but not including the `untimed` value).
7. Using an Agent Group corresponding to an object configured in the Configuration Layer as a device of type `ACD Queue`.
8. In the T-Server `Application` object, on the `Options` tab in the `TServer` section.

Deploying T-Server for CSTA Connector

The following topics provide information for the deployment and operation of T-Server for CSTA Connector:

T-Server Deployment Fundamentals

This PDF contains general information about T-Server features and functionality and about its configuration and installation.

T-Server Deployment Fundamentals

T-Server and CSTA Connector Deployment

This PDF contains general information for the deployment and configuration of your T-Server.

T-Server and CSTA Connector Deployment

High-Availability Deployment

This PDF describes the general steps for setting up a high-availability (HA) environment for your T-Server.

High-Availability Deployment

Multi-Site Support

This PDF contains general information about multi-site environments, as well as information on deploying a multi-site environment for your T-Server.

Multi-Site Support

Starting and Stopping T-Server and CSTA Connector

This PDF describes methods for stopping and starting T-Server and CSTA Connector.

Starting and Stopping T-Server and CSTA

Connector