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

Microsoft Skype for Business Deployment Guide

Multimedia Connector for Skype for Business 8.5.0

12/29/2021

Table of Contents

Multimedia Connector for Skype for Business Deployment Guide

Welcome to the Multimedia Connector for Skype for Business Deployment Guide. This Deployment Guide provides deployment procedures and detailed reference information about the Multimedia Connector for Skype for Business as a product, and its components: T-Server, UCMA Connector, and Workspace Plugin. See the summary of the highlighted topics below.

This document describes functionality tested and supported by Multimedia Connector for Skype for Business. Features and functionalities related to Skype for Business that are not described are not tested and, therefore, are not supported.

> **Important**
> The Multimedia Connector for Skype for Business also supports Lync 2013. In many cases the behavior or procedures apply to both Skype for Business and Lync 2013. Lync 2013 is explicitly mentioned only where it differs from Skype for Business. For example, the connector does not support video calls when integrating with Lync 2013.

About

Find out about integration with Skype for Business:

- Architecture
- Prerequisites

Deployment

Find procedures to deploy:

- Deployment summary
- T-Server
- UCMA Connector
- Workspace Plugin

Features

Find out about supported features:

T-Server Details

Find out about T-Server specifics:

Alternate Routing

Call Monitoring

Call Supervision

and more...

T-Library support

Attribute Extensions

Sizing and Capacity Recommendations

Error messages

Architecture

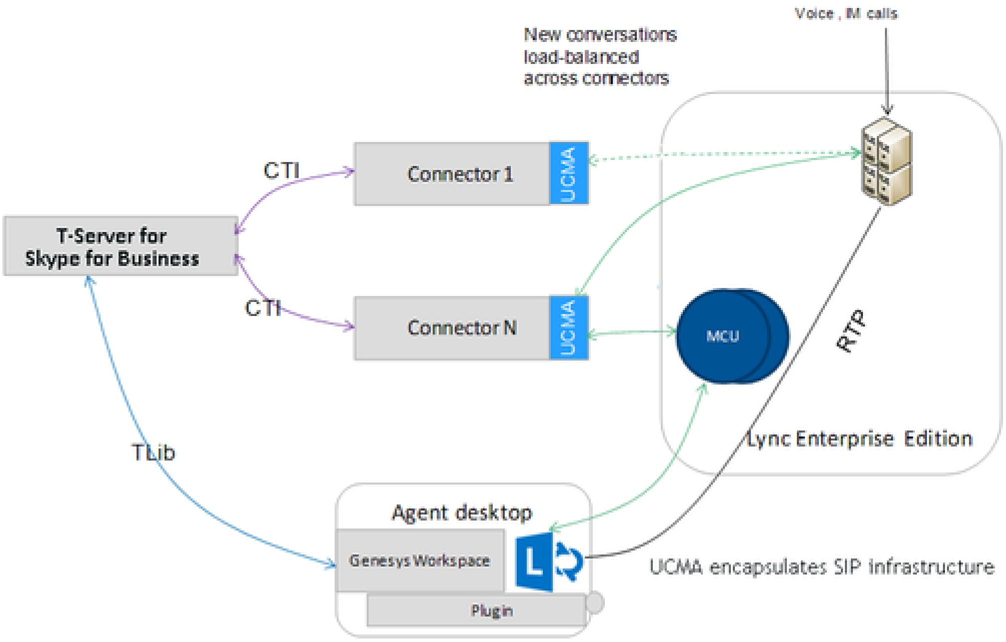
T-Server for Skype for Business has the same position in the Genesys Media Layer as all Genesys T-Servers. T-Server provides an interface between the Microsoft telephony implementation and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from, and are sent to, the Microsoft Skype for Business Server and its phone applications. T-Server is a TCP/IP-based server that can also act as a messaging interface between T-Server clients.

In addition to voice communications, T-Server for Skype for Business manages other media provided by the Microsoft platform, namely: presence, IM sessions, and video calls. It is therefore more expansive than other T-Servers and provides some specialized functions that are unique to the Skype for Business integration service.

T-Server consists of two components:

- T-Server—Provides the standard interface to other Genesys applications and third-party T-Server clients. It has access to the Genesys Management Framework and the Genesys configuration database. T-Server utilizes full capabilities of the Framework for logging, alarming, and secure communications.
- Connector—Provides the communication with Microsoft facilities. It does not have connection to the Genesys Framework.

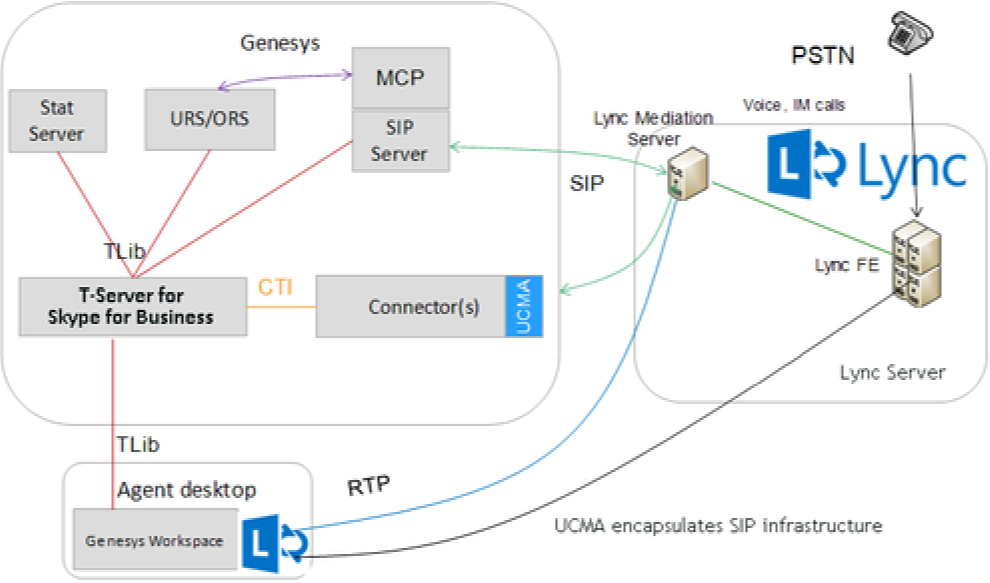
The Genesys Workspace Desktop Edition Plugin for Skype for Business should be installed on the desktop of agents who interact with the system, to fully exploit the T-Server features and to provide a good agent experience..



T-Server in Front

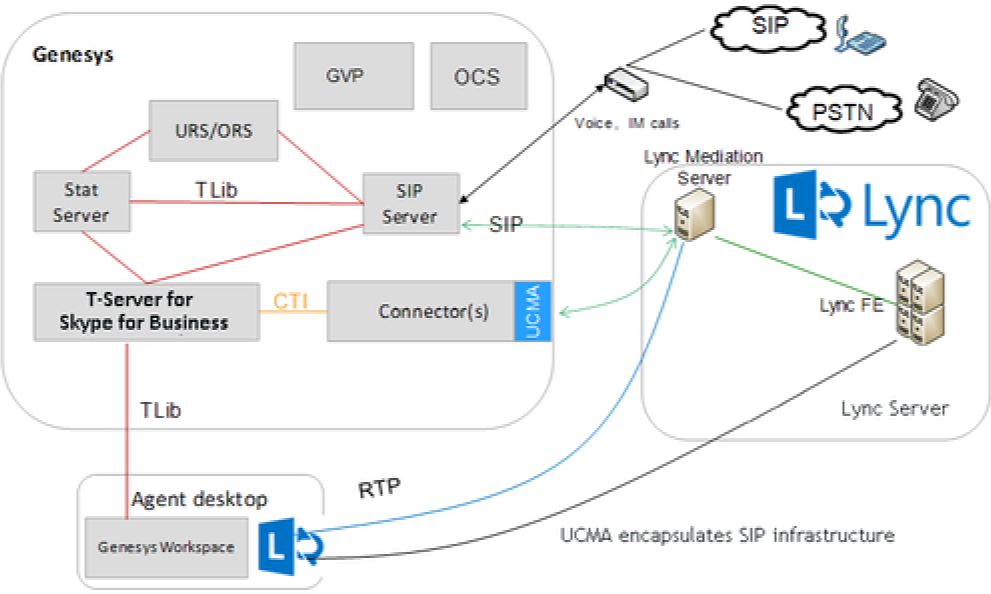
In the T-Server in Front architecture, calls first get to Skype for Business as shown in the following figure, and are then routed to T-Server.

T-Server supports treatments through SIP Server using GVP's Resource Manager and Media Control Platform. All treatment types are inherited from SIP Server, so most of the SIP Server strategies can be re-used. Note that the No-Answer Supervision feature is implemented differently comparing to SIP Server, because of call-model differences. For more information, see the No-Answer Supervision feature.



SIP Server In Front

In the configuration shown in the figure below (the standard deployment), T-Server is deployed behind a SIP Server. Calls land on SIP Server and all inbound calls (from customers to agents) are routed by SIP Server to a Microsoft Skype for Business Routing Point. Customer endpoints communicate directly with SIP Server. This architecture allows using outbound elements.



Multi-Site Support

T-Server is built with the T-Server Common Part that contains the ISCC component responsible for call data transfer between multiple sites. Currently, T-Server supports the following ISCC transaction types:

- `route` as origination and destination
- `pullback` as origination and destination

T-Server for Skype for Business supports ISCC connections with SIP Server and other T-Servers, but does not support ISCC connections with other instances of T-Server for Skype for Business.

For information about supported ISCC transaction types and ISCC features, see Multi-Site Support.

SBA/SBS Support

Starting with version 8.5.001.49, T-Server for Skype for Business supports user endpoints registered on a Survivable Branch Appliance (SBA) or a Survivable Branch Server (SBS) front-end server. When the SBA or SBS is disconnected from the main Skype for Business server, T-Server cannot control calls on such users until connection is restored.

Paired Front End Pools

Architecture with a single application and paired user Front End pools

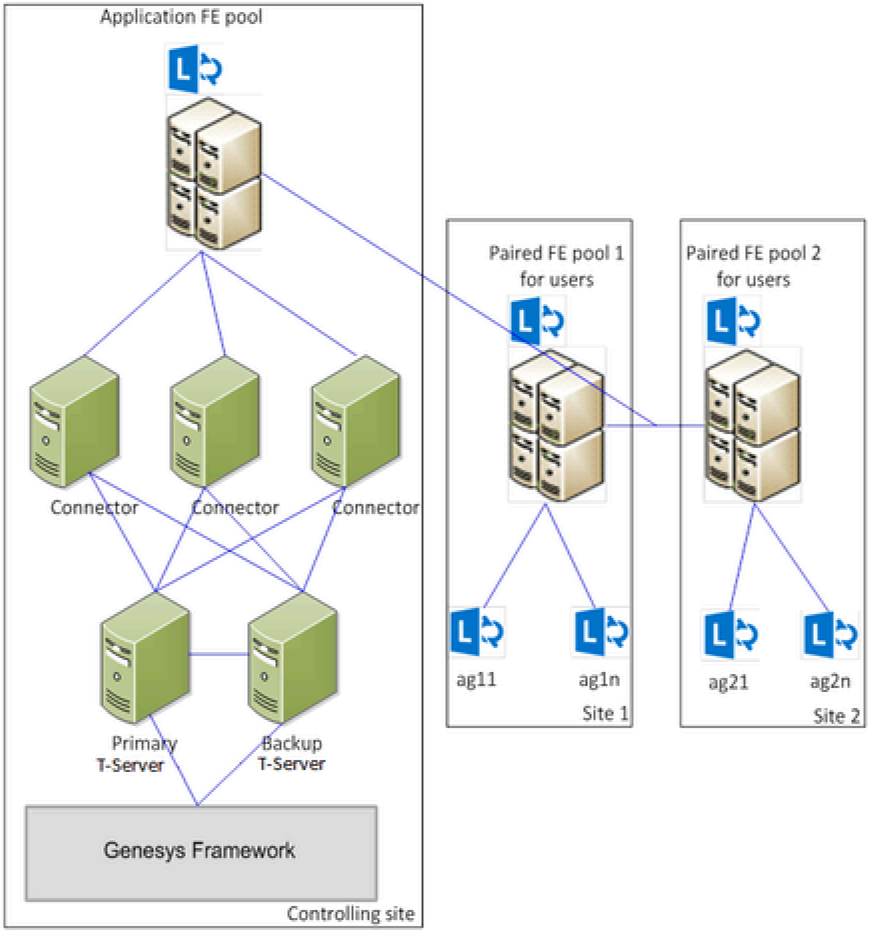
This deployment contains the following components:

- Single Enterprise Edition pool of Front End (FE) Servers for handling applications
- Paired pools of FE Servers for handling users and agents that reside at different geographic locations
- Computers in Trusted Application pool for Genesys Multimedia Connectors
- Servers required to host components such as Genesys Skype for Business T-Servers and Genesys Management Framework

The controlling site can be divided into two separate data centers:

1. The site with the Front End servers of the application.
2. The site with Connectors and Genesys software.

There are no restrictions or configuration limitations to perform this, except that the data interlink between sites must contain satisfactory conditions. The following figure illustrates the described architecture:



User pool failover scenarios

The call center behavior is the same as that in a deployment using a single pool for applications and users. The exception is that the complete failure of one of the user pools does not cause call center failure. However, it reduces the availability of agents from the affected pool.

User pool failover

According to Microsoft documentation (see https://technet.microsoft.com/en-us/library/jj205184.aspx), the user experiences the following scenarios during a failover.

- When a user is in a pool that fails, the user is logged out and the presence of this user is unknown until the failover has completed.
- The peer-to-peer sessions that include the participation and initiation of conference by the user will be terminated.
- The user cannot log back in until either the registrar resiliency timer expires or the administrator initiates failover procedures, whichever comes first.
- After the failover, when the user logs back in, the user will log in to the backup pool. If the user logs in before the failover has completed, the user will be in Resiliency mode until the failover is complete.

- The user can establish new, or restore previous, peer-to-peer sessions only after the failover is completed.
- Because the users in the affected pool are not fully available during the failover, Skype for Business servers might notify the Genesys call sessions that the user is removed or has disconnected. If there is only one participant, the session will be terminated by Genesys Connector.
- As the users in the affected pool are not completely available until the failover is completed, initiation of Genesys call sessions or adding such users to existing Genesys sessions might fail.

The recovery time depends on the administrator identifying the pool failure and initiating failover execution. This might take up to 60 minutes.

User pool is available

There are no restrictions in operations when the failover is completed and the environment is stabilized. The performance of the system might be slightly affected.

User pool failback (restoration of failed pool)

The behavior of paired pools during initial configuration or during failback (when the failed pool is restored) is similar to the behavior during failover.

- Participation of users is restricted based on the user's performance while in Resiliency mode. This corresponds to users that are transferred back to the restored pool, users in conferences, and users hosted by the application FE pool (that is Genesys controlled).
- Typically, completing failback from one pool to another (Recovery Time Objective (RTO)) can take anywhere from 15 to 20 minutes or more, up to 60 minutes.
- Recovery Point Objective (RPO), the time measure of data that might be lost due to failback, based on replication latency of backup service, is expected to be no more than 5 minutes. This time specifies the expected interval when the data might not have replicated during failback and would be lost. This loss will not be experienced by Genesys calls and sessions as they are hosted on an unaffected application FE pool.
- Genesys call control will not be affected because conferences will be hosted by an application FE pool.

Advantages of the architecture

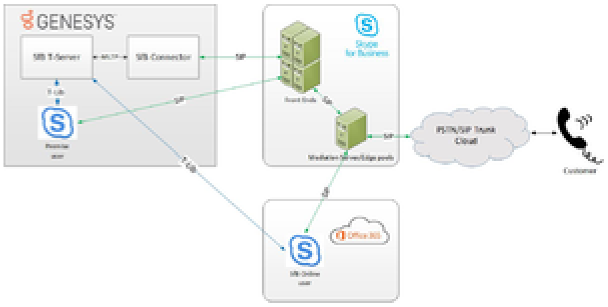
- The current Genesys T-Server and Connector for Skype for Business can be used out of the box without any concerns about where users are located.
- A failover from one user pool to another does not require applications or scripts other than those provided by Microsoft.
- Although performing a failover from one user pool to another would impact the availability of affected users, it will not impact Connectors.

Limitations

Microsoft does not provide support for failover of the Application FE pool.

Federation Platform with Microsoft Office 365 Cloud

Starting with release 8.5.001.44, T-Server provides support for Skype for Business federated users where Genesys T-Server and the UCMA Connectors for Skype for Business are hosted in the premise environment, but agents are partially or fully hosted in the Office 365 cloud.



T-Server supports the registration of devices that are hosted in the Office 365 cloud, and third-party call control (3pcc) is provided via a T-Library client (Workspace Desktop). T-Server provides partial agent functionality for such devices; specifically, the agent status is based only on presence availability, because of limitations on the Skype for Busines side.

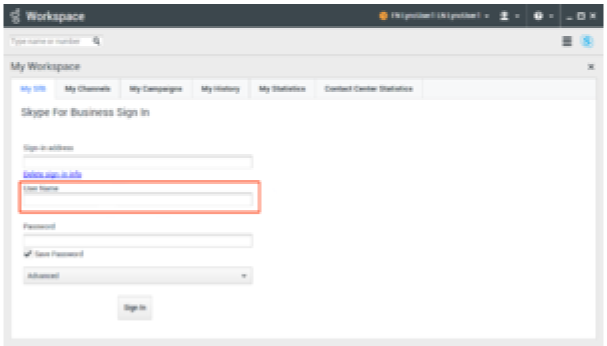
T-Server provides support for call control on devices that are hosted in the Office 365 cloud at the same level as for devices that are hosted in the premise environment, unless otherwise noted.

User Endpoint devices hosted in the Office 365 cloud are configured as devices of type Extension with the **Switch Specific Type** parameter set to 2.

A new extension key, **PresenceType**, is introduced in DN-status events to indicate the type of presence that the Connector currently monitors for the DN device. The following values are supported:

- `local`—indicates that the Connector monitors a local presence of a device and allows to change it
- `remote`—indicates that the Connector monitors a remote presence of a device and rejects attempts to change it

Workspace Plugin



Starting with version 8.5.000.83, the Workspace Plugin user interface is modified to support federated agents. It now shows the User Name field when an agent logs in the Skype for Business Front End Server. This field can be left blank if the user name is the same as the sign-in address. For federated users, the User Name differs from the Sign-in address.

Limitations

- Publishing of presence via T-Server for Skype for Business on Office 365 users is not supported.
- Presence subscription for Office 365 users is supported but is limited to 5 states: Available, Busy, Away, Do Not Disturb, and Offline. It is not possible to see any additional presence information, such as notes or custom availability (indication that agent is on a call or in a conference), because of restrictions in the handling of presence of federated users.
- Calls presented directly to Office 365 users cannot be handled by T-Server—only routed calls and calls made via T-Server for Skype for Business are supported.
- Handling of 1pcc single-step transfer scenarios performed on an Office 365 user is not supported.
- It is not possible to present dialing party names to a federated user, because only a SIP user URI is available for an Office 365 user in an incoming toast.
- Supervisor services cannot be supported in scenarios where an Office 365 user is selected as a supervisor due to a limitation of Skype for Business.
- Escalation of calls to another media by an Office 365 user is not supported due to a limitation of Skype for Business.
- If a video conversation is placed on hold, only the audio channel can be retrieved from hold.

Managing T-Server and UCMA Connectors

Deployment Summary

For this deployment, you must complete a number of configuration steps: some on Microsoft Skype for Business Server and some in the Genesys environment.

Genesys recommends the following deployment sequence:

1. Review Prerequisites that include system requirements and licensing.
2. Provision for UCMA Connectors. (Microsoft)
3. Configure and install UCMA Connector(s). (Genesys)
4. Configure required telephony objects, including Switch objects and corresponding DN objects. (Genesys)
5. Configure Skype for Business application endpoints for Routing Points, External Routing Points, and conference services. (Microsoft)
6. Create a pool of ready conference resources that UCMS Connector will create at startup time. These resources guarantee that there are conference resources available for call handling. (Genesys)
7. Configure Skype for Business user endpoints. (Microsoft)
8. Configure and install T-Server for Skype for Business. (Genesys)
9. Configure and install SIP Server. Set up the multi-site (ISCC) connection to T-Server for Skype for Business. See the Framework 8.1 SIP Server Deployment Guide for details. (Genesys)
    - On the Connections tab of the SIP Server Application object, add an ISCC connection to T-Server.
10. Create a new PSTN Gateway using the Microsoft Skype for Business Topology Builder. Configure a trunk to provide connectivity with SIP Server. See details in Microsoft documentation: https://technet.microsoft.com/en-us/library/Gg425945.aspx.
11. Define External Access policies, voice routes, and PSTN usage to be used for remote treatments. See details in Microsoft documentation: https://technet.microsoft.com/en-us/library/gg398272(v=ocs.16).aspx.
12. Configure and install Genesys Media Server. (Genesys)
    - When integrated with SIP Server, the Genesys Media Server provides Real-Time Protocol (RTP) streaming for a variety of media services—treatments, conferences, call recording, and so on—using the Media Server Markup Language (MSML). See the Genesys Media Server Deployment Guide for details.
13. Deploy Workspace Desktop Edition for each agent. (Genesys)
14. Deploy Workspace Plugin for Skype for Business for each agent. (Genesys)
15. Implement performance enhancements.

Important

For additional information about configuring Skype for Business, consult the Multimedia Connector for Skype for Business Configuration of Microsoft Skype for Business platform White Paper.

Prerequisites

T-Server has a number of prerequisites for deployment. Read through this section before deploying T-Server for Skype for Business.

> ### Important
> A key prerequisite before deploying the Genesys software is that the Skype for Business environment is deployed and functioning as expected. All features that are provided by Skype for Business must be active. Presence, IM, voice, and video are available for direct communication between Skype for Business clients, along with PSTN connectivity to Skype for Business clients if required by the deployment.

Microsoft recommends an Enterprise Edition Skype for Business pool for use with contact centers.

> ### Important
> On the Skype For Business Front End Pool that is used by Connector, the Meeting Configuration option **PstnCallersBypassLobby** must be enabled. This feature is enabled by default when creating a new Application Pool in Skype For Business so no specific action is required, but this feature should never be disabled on the Front End Pool used by Connector.

The Standard Edition server is designed for small organizations, and for pilot projects of large organizations. It enables many of the features of Lync Server, and the necessary databases, to run on a single server. This enables you to have Lync Server functionality for a lower cost, but does not provide a true high-availability solution.

Standard Edition server enables you to use instant messaging (IM), presence, conferencing, and Enterprise Voice, all running on one server. For a high-availability solution, use Lync Server Enterprise Edition. Thus, contact centers and other mission-critical workloads will work on Standard Edition boxes but are NOT recommended.

Enterprise Edition is recommended for the following reasons:

- High-Availability and Disaster Recovery features are only available on Enterprise Edition. Contact center agents and the Application itself can be deployed redundantly in the form of a paired pool on Enterprise Edition for Disaster Recovery. Additionally, if a Front End server is taken out of service, other Front End servers will balance the load.
- Performance/Expansion—Enterprise Edition pools can be scaled up and down by adding or removing Front End servers.

Genesys cannot guarantee any performance level on a Standard Edition platform.

Software Requirements

1. T-Server supports both UCMA 4.0 with Microsoft Lync 2013, and UCMA 5.0 with Skype for Business.
   - If you are using **Microsoft Lync 2013:**
     - Ensure you have installed UCMA 4.0 Runtime and applied the latest Microsoft Lync 2013 Server Cumulative updates. See the following pages for more information:
       - https://www.microsoft.com/en-us/download/details.aspx?id=36820
       - https://www.microsoft.com/en-gb/download/details.aspx?id=34992
     - The required version of Microsoft Lync 2013 Client must be 15.0.4763.1001 or later.
   - If you are using **Microsoft Skype for Business:**
     - Ensure you have installed UCMA 5.0 Runtime. For UCMA 5.0 support, you must ensure that you have installed the Skype for Business Server and applied the latest Microsoft Cumulative server updates as well as the latest UCMA 5.0 Runtime updates. See the following pages for more information:
       - https://www.microsoft.com/en-us/download/details.aspx?id=47344
       - https://www.microsoft.com/en-us/download/details.aspx?id=47690
2. The Workspace Plugin for SfB uses 32-bit dlls. So, you must install the 32-bit Microsoft Office Skype for Business client. The 64-bit Microsoft Office Skype for Business Client is not supported.
3. Review Microsoft Patching Policy.
4. Review DNS Requirements.
5. UCMA Connector supports two modes: manual and auto-provisioning. If you use the auto-provisioning mode, complete the *Activating an auto-provisioned application* procedure on the host where the Connector will be running. See Microsoft documentation for details:
   - Skype for Business: https://msdn.microsoft.com/en-us/library/dn466123(v=office.16).aspx
   - Lync Server 2013: https://msdn.microsoft.com/en-us/library/dn466123(v=office.15).aspx

Genesys Components

You can only configure T-Server after you have deployed the Configuration Layer of Genesys Framework. This layer contains Configuration Server, the Configuration Database, and Genesys Administrator (or Configuration Manager). If you intend to monitor or control T-Server through the Management Layer, you must also install and configure components of this Framework layer, such as Local Control Agent (LCA), Database Access Point (DAP), Message Server, Log Database, and Solution Control Server (SCS) before deploying T-Server.

Refer to the *Management Framework Deployment Guide* for information about, and deployment instructions for these Framework components.

Recommended minimum versions of Genesys components:

- SIP Server 8.1.102.62+
- URS 8.1.3+

- ORS 8.1.3+
- Stat Server 8.1.2+
- GVP 8.5.1+

Microsoft Patching Policy

Lync and Skype for Business Server Updates

Microsoft delivers patches and updates for these components in Cumulative Update packages that must be manually downloaded and applied.

- Genesys installs and tests all Cumulative Update packages to ensure they are fully compatible with a Genesys deployment. Each Cumulative Update will be explicitly documented.
- Genesys recommends that customers do not apply Cumulative Updates for Lync and Skype for Business before Genesys has completed their tests and has approved these Cumulative Updates.

Skype for Business Server 2015 Cumulative Update Status

Genesys has tested and approved the following Skype for Business Server Cumulative Update (CU) versions:

CU Version	Release Date	Status
6.0.9319.537	January 2019	Approved with T-Server 8.5.001.67+
6.0.9319.534	July 2018	Approved with T-Server 8.5.001.65+
6.0.9319.516	April 2018	Approved with T-Server 8.5.001.49+
6.0.9319.510	December 2017	Approved with T-Server 8.5.001.49+
6.0.9319.281	May 2017	Approved with T-Server 8.5.001.02+
6.0.9319.277	February 2017	Approved with T-Server 8.5.001.02+
6.0.9319.272	November 2016	Approved with T-Server 8.5.001.02+
6.0.9319.259	June 2016	Approved with T-Server 8.5.001.02+
6.0.9319.102	November 2015	Approved

See this link for details and installation instructions: https://support.microsoft.com/en-gb/kb/3061064.

Lync Server 2013 Cumulative Update Status

Genesys has tested and approved the following Lync Server 2013 Cumulative Update versions:

CU Version	Release Date	Status
5.0.8308.1001	July 2018	Approved
5.0.8308.992	July 2017	Approved
5.0.8308.987	March 2017	Approved
5.0.8308.984	January 2017	Approved
5.0.8308.977	December 2016	Approved
5.0.8308.974	November 2016	Approved
5.0.8308.965	August 2016	Approved
5.0.8308.956	April 2016	Approved
5.0.8308.920	July 2015	Approved

See this link for details and installation instructions: https://support.microsoft.com/en-gb/kb/2809243.

Skype for Business Client Versions

For the Skype for Business client versions, Genesys recommends that customers follow their normal IT patching policies. The Skype for Business clients used in the Genesys testing environments are updated using the Microsoft Office Current Channel.

> **Important**
>
> Genesys does not recommend installing Skype for Business client version 16.0.7329.1083, because of its stability issues. Those issues were fixed and successfully tested by Genesys in Skype for Business client version 16.0.7766.7080.

Microsoft Windows Updates and Security Patches

For regular Windows updates and security patches, Genesys recommends that customers follow their normal IT patching policies. These patches are applied on a weekly basis in the Genesys testing environments as they are delivered from Microsoft. If any patch is found to interfere with the normal operation of a Genesys deployment, then these issues will be documented.

Skype for Business DNS Requirements

Genesys Multimedia Connector for Skype for Business only has the following DNS requirement for proper operation:

- All hosts where Genesys Multimedia Connector for Skype for Business is deployed must be able to reach the Skype for Business Front End Pool and all Front End servers belonging to that pool.
- All Skype for Business Front End servers must be able to reach the FQDN of every host defined in the Skype for Business Trusted Application Pool used for the deployment of Skype for Business Multimedia Connector.

In order for Skype for Business to provide all services required by Skype for Business Multimedia

Connector, all DNS prerequisites defined by Microsoft must be fulfilled. The following links provide useful information:

- https://technet.microsoft.com/en-us/library/dn951397.aspx
- https://technet.microsoft.com/en-us/library/mt346420.aspx
- https://blogs.technet.microsoft.com/praj/2016/10/14/skype-for-business-client-sign-in-call-flow-detailed/

Hardware Requirements

Both Skype for Business Server 2015 and Lync Server 2013 Enterprise Edition server roles and computers running the respective administrative tools require 64-bit hardware.

The specific hardware varies depending on the size and usage requirements.

For best performance, it is recommended to run Skype for Business Server 2015 or Lync Server 2013 Enterprise Edition on servers with hardware that meets the requirements described in Microsoft documentation below. Use of less powerful hardware may cause functionality issues or poor performance.

Minimum Hardware Requirements

T-Server for Skype for Business:

- 1 core CPU
- 4 GB memory

UCMA Connector:

- 6 core CPU
- 8 GB memory

SQL database size:

- Ensure that free disk space on Front End servers is at least twice the size of the local SQL database. This size can be estimated by looking at the size of the folder “<DeploymentDrive>:\CsData” on the Front End server.

Consult the following Microsoft guide for server hardware sizing:

- https://technet.microsoft.com/en-us/library/dn951388.aspx

The standard Skype for Business Capacity Calculator (https://www.microsoft.com/en-us/download/details.aspx?id=51196) is not suitable for calculating the sizing of a Front End pool that will host a Genesys Contact Center. Therefore, refer to the *Skype for Business Solution Blueprint* document for Genesys sizing guidelines.

Licensing Requirements

All Genesys software is licensed. Genesys products are protected through legal license conditions as part of your purchase contract. However, the level of technical license-control enforcement varies across different solutions and components.

T-Server for Skype for Business as all Genesys T-Servers uses License Manager for licensing. Connector does not need any additional licensing.

Before you begin to install T-Server, remember that, although you may not have had to use technical licenses for your software when you deployed the Configuration and Management Layers in their basic configurations, this is not the case with the Media Layer. T-Server requires seat-related DN technical licenses to operate even in its most basic configuration. Without appropriate licenses, you cannot install and start T-Server. If you have not already done so, Genesys recommends that you install License Manager and configure a license file at this point. For complete information on which products require what types of licenses, and on the installation procedure for License Manager, refer to the Genesys Licensing Guide.

Licensing HA Implementations

T-Servers operating with the hot standby redundancy type require a special CTI HA technical license, which allows for high-availability implementations, in addition to regular T-Server licenses. Neither T-Server in a redundant pair configured for hot standby starts if this license is unavailable. Moreover, the primary and backup T-Servers must use the same licenses to control the same pool of DNs. If your T-Servers are configured with the hot standby redundancy type, order licenses for CTI HA support.

Licensing Multi-Site Implementations

T-Servers/SIP Servers performing multi-site operations require licenses that allow for such operations, in addition to regular T-Server licenses. While T-Server for Skype for Business only performs multi-site operations with SIP Server, a Multi-Site license is still required in the deployment.

Provisioning for UCMA Connectors

There are two different UCMA Connectors: UCMA Connector for Microsoft Lync using UCMA 4 and UCMA Connector for Skype for Business using UCMA 5. The provisioning process is the same for both connectors. You can provision for UCMA Connectors by either using shell scripts or by using the Skype for Business Topology Builder.

This section contains instructions for provisioning an UCMA Connector application on a trusted application pool with multiple computers, using the Skype for Business (or Lync) Server Management Shell.

See details in Microsoft Developer Network documentation:

- Skype for Business
- Lync Server 2013

To provision for UCMA Connectors using shell scripts:

1. Create a **trusted application pool** with the computer(s) where UCMA Connector(s) will be running.
   A. Create a pool with one computer. For example:

   ```
   New-CsTrustedApplicationPool -Identity “trustedpool.lyncdco.lab” -Registrar
    Registrar:”pool01.lyncdco.lab” -Site “DalyCity” -ComputerFqdn
    “computer1.lyncdco.lab”
   ```

   B. Add a second computer to the pool. For example:

   ```
   New-CsTrustedApplicationComputer -Identity “computer2.lyncdco.lab” -Pool
    “trustedpool.lyncdco.lab”
   ```

   C. Repeat the above step to add another computer as required.
2. Create and enable a new **trusted application** with the service port of the UCMA Connectors and assign this trusted application to the UCMA Connector trusted application pool. For example:

   ```
   New-CsTrustedApplication -ApplicationId “Connector_app” -TrustedApplicationPoolFqdn
    “trustedpool.lyncdco.lab” -Port “6001”
   ```

3. Run the Enable-CsTopology cmdlet to create the appropriate trusted service entries:

   ```
   Enable-CsTopology
   ```

4. To balance the load among UCMA Connectors, configure **DNS-based load balancing** for the application pool. For example, there are two computers in the application pool `trustedpool.lyncdco.lab`, so the following entries must be present in the DNS:

```
computer1 Host(A) 123.1.1.1
computer2 Host(A) 123.1.1.2
trustedpool Host(A) 123.1.1.1
trustedpool Host(A) 123.1.1.2
```

DNS Time to live (TTL) for these entries must be set to `0`.

> ### Important
>
> - Relevant DNS AAAA records are also required for application pools and computers that are used in IPv6 network.
> - Because balancing the load between Connectors is based on DNS load balancing, it is not 100% fault-resistant. All Trusted Applications (Connectors) must be running on all computers in the Trusted Application Pool. If some Trusted Applications (Connectors) are not running, call reporting might be delayed. That delay will depend on System Network failure detection, for which any misconfiguration must be corrected as soon as possible.

5. Create **certificates** for the UCMA Connector computers in a trusted application pool. For example:

```
Request-CsCertificate -New -Type default -FriendlyName "trustedpool.lyncdco.lab
 Pool" -CA dc.lyncdco.lab\DC-CA -ComputerFQDN trustedpool.lyncdco.lab -DomainName
 "computer1.lyncdco.lab,computer2.lyncdco.lab"
```

Each host in the pool must import a copy of this certificate.

> ### Important
>
> For additional information about provisioning for UCMA connectors, consult the Multimedia Connector for Skype for Business Configuration of Microsoft Skype for Business platform White Paper.

Back to Deployment Summary

Using Telephony Objects

Deploying T-Server manually requires that you configure a number of different objects in the Configuration Layer prior to setting up your T-Server objects and then installing T-Server. Use Configuration Manager or Genesys Administrator for creating telephony objects as described below.

1. Create a Switching Office object.
2. Create two Switch objects: one for T-Server and one for SIP Server.
3. Create devices for T-Server.
4. Create devices for SIP Server.
5. Create Agent Logins.

Switching Office

Configure a Switching Office object of type **SIP Switch** that accommodates your Switch object under Environment. Until you have done this, you cannot register a Switch object under Resources (single-tenant environment) or a Tenant (multi-tenant environment).

Switches

1. Configure two Switch objects for this deployment. Assign one **Switch** object to T-Server for Skype for Business, and assign another **Switch** object to SIP Server.
2. On the Annex tab of the Switch for T-Server, create the following sections:
   - **[conference-services]**
   - **[connector]**
   - **[log]**

   You will add configuration options as required for your deployment or functionality.
3. In the **[conference-services]** section, add two configuration options:
   - count
   - uri-pattern

   > Important
   >
   > - Trusted Application Endpoints to be used for conference services must be created

> using the **count** and **uri-pattern** options.
>
> - Genesys recommends that any changes to options related to conference services are made during a scheduled maintenance window. After any change to these options, restart all Connectors to ensure that they are all operating with the same configuration.

4. If implementing the multi-site configuration, specify access codes for all switches on the network so that the call-processing applications can route and transfer calls between switches.
   Two types of access codes exist in a Genesys configuration:
   - Default access codes that specify how to reach this switch from any other switch in the Genesys environment.
   - Switch-to-switch access codes that specify how to reach a particular switch from any other switch. Use this type when either a nondefault dial number or routing type is required between any two locations. When a switch-to-switch access code is configured, its value has a higher priority than that of a default access code. See Multi-Site Support for step-by-step instructions.

Devices for T-Server

> ### Important
>
> T-Server internally converts all DN names to lower case because only lower case URIs are supported by Skype for Business. If two or more DNs are configured with names that only differ in the case of some characters (like `sip:dn1` and `sip:DN1`), T-Server creates the LMS message MSG_TS_COMMON_DN_MISCONFIGURED and only one of these DNs will be in service. If such DNs are created, in order to avoid unpredictable behavior, you must delete all of them and then create a single DN with the correct name.

T-Server supports the following DN types that you configure in the Genesys configuration environment under the **Switch** object assigned to T-Server for Skype for Business:

- **Extension**—Create a DN of type Extension for each Skype for Business user with the number corresponding to the SIP URI of the Skype for Business user that was created and enabled for Skype for Business.
  For example:

  ```
  sip:alice@lyncdco.lab
  ```

  ```
  sip:andrew.smith@lyncdco.lab
  ```

- **Routing Point**—Create a DN of type Routing Point with the number corresponding to the SIP URI of the Trusted Application Endpoint.
  For example, `sip:RP1@lyncdco.lab`

- **External Routing Point**—Create a DN of type External Routing Point with the number corresponding to the SIP URI of the Trusted Application Endpoint.
  For example, `sip:ERP1@lyncdco.lab`
  - Configure the **Association** field with the dialable phone number assigned to a referenced line. This value will be used by SIP Server as the user part of the URI in SIP INVITE to reach the Skype for Business External Routing Point. This number corresponds to the `LineURI` parameter value in the corresponding Trusted Application Endpoint.
- **Virtual Queue**—Used for routing and reporting. Support of this DN has no specifics related to Skype for Business.
- **Voice Over IP Service**—Used for different services and configuration tasks. For example, for presence mapping configuration. Every DN of this type must have option **service-type** set to support a particular service, such as Music on Hold, Media Server, and so on.
- **Trunk Group**—Must be named **gcti::park**. It is used for parking of chat during media escalation.

You must configure all DNs that agents and their supervisors use in day-to-day contact center operation—so-called seat-related DNs—such as Extensions. All Extensions, Routing Points, External Routing Points, and Trunk Groups must be configured under the Microsoft Skype for Business or Microsoft Lync Switch object with a name corresponding to its SIP URI.

Devices for SIP Server

1. Under the **Switch** object assigned to SIP Server, create a DN of type **Trunk** for Microsoft Skype for Business or Microsoft Lync.
2. In the **[TServer]** section of the Trunk DN, configure the following options:
   - **contact**—For correct communication with a Mediation Server or Mediation Server Pool, you must configure a SIP SRV record to be used in the contact properties. The SRV record protocol should be configured as `tcp` (typically port 5068), or in case of secure connections use `tls` (typically port 5067) to match the Mediation Server configuration.
     For example:

     contact=`genesys.com;transport=tcp`

     contact=`genesys.com;transport=tls`

     Refer to the “DNS Name Resolution” and “Transport Layer Security for SIP Traffic” chapters in the Framework 8.1 SIP Server Deployment Guide for more information.
   - **prefix**—Set this option to the initial digits of the number matching this SIP Server outbound trunk. For example, `001`.
   - **sip-proxy-headers-enabled**—Set this option to `false`.
3. Under the Switch object assigned to SIP Server, create a **Switch Access Code** to be used by SIP Server to reach Skype for Business. The Access Code must match the appropriate SIP Server outbound trunk. For example, `001`.

Agent Logins

It is recommended, but not mandatory, to create an Agent Login object for each agent. An administrator can, however, enforce strict policy for Agent Login and forbid using non-configured agent names. The Application option **agent-strict-id** in the **[TServer]** section controls this policy.

.

Back to Deployment Summary

Managing UCMA Connectors

This section describes how to configure, install, and start/stop UCMA Connector for Skype for Business or Lync.

Prerequisites

- Ensure that you have met the prerequisites listed on Software Requirements.
- Ensure that provisioning for UCMA Connectors is completed.

Configuring Connector

Using Genesys Administrator (or Configuration Manager), create an Application object of type **Third Party Server** for the Connector Application object.

See mandatory and optional options that are configured in the configuration file. Additional configuration options can be specified in the Annex tab of the Switch object and are described in the Skype for Business Options Reference.

Installing Connector

Prerequisites: Connector Application object is created in the Genesys configuration environment.

1. Copy the correct Connector installation package to the computer where Connector will be installed, depending on your environment, as follows:
    - UCMA Connector for MS Lync supports UCMA 4.0
    - UCMA Connector for Skype for Business supports UCMA 5.0
2. In the directory to which the Connector installation package was copied, locate and double-click **Setup.exe** to start the installation of the Connector.
3. When prompted, specify the connection parameters to the Configuration Server associated with this Connector.
4. When prompted, select the Connector Application object you configured in Configuring Connector from the list of applications.
5. When prompted, specify the destination directory into which the Connector is to be installed.
6. When prompted, select the provisioning mode—Manual or Auto—to be used for this Connector.

7. When prompted, depending on your selected provisioning mode, specify parameters for that mode. To consult on the parameter descriptions, see the About the Configuration File section.
8. Click **Install** to begin the installation.
9. Click **Finish** to complete the installation.

When installation is complete, the **connector.config** configuration file that you configured is placed in the installation directory.

> **Important**
>
> When installing multiple Connectors, each Connector must be installed on a different host. Each host where Connector is to be installed must belong to the same Skype for Business/Lync application pool.

Starting Connector

You can start the Connector using the Management Layer, or a manual procedure. When starting manually, specify the following command line:

```
mslync_connector.exe –configFile <config file name>
```

where `<config file name>` is the name of the configuration file created during the installation procedure. By default, it is called **connector.config**. The command line is automatically added to the **Start Info** tab of the Connector Application object.

For example:

```
mslync_connector.exe –configFile connector.config
```

> **Warning**
>
> If no connector configuration file is provided in the command line option **-configFile**, the connector will look for the file named **mslync_connector.exe.config**.

For starting server applications using the Management Layer, see Starting and Stopping Framework Components in the *Management Framework Deployment Guide*.

Stopping Connector

To stop a server application on Windows, do one of the following:

- Type `Ctrl+C` in the application's console window.
- Click **End Task** in the Windows Task Manager.

For stopping server applications using the Management Layer, see Starting and Stopping Framework Components in the *Management Framework Deployment Guide*.

About the Configuration File

UCMA Connector must be configured using the configuration file. By default, the installation procedure creates the configuration file named **connector.config**. This file has two mandatory sections and some optional sections as described below.

- Section **configSections**—Mandatory section. Describes the configuration sections in the XML file. It must contain all the names of the sections used in the configuration file:

Option Name	Type	Description
Name	Mandatory	Specifies the name of the configuration section.
Type	Mandatory	The value must be **System.Configuration.AppSettingsSection**.

- Section **startupOptions**—Mandatory section. Describes the configuration options that are required to start the application and connect to Skype for Business Server.

Option Name	Type	Description
connectorPort	Mandatory	The TCP port for a CTI link. Example: `9001`
provisionMode	Mandatory	The provisioning mode the Connector will use for communication with Skype for Business Server: • auto—for auto-provisioning mode of work • manual—for manual-provisioning mode of work For more information about auto-provisioning mode, see Microsoft documentation:

Option Name	Type	Description
		- Skype for Business - Lync Server 2013
applicationUrn	Mandatory for auto mode	The unique identifier of the application in the deployment. It is assigned when the application is provisioned. Example: `urn:application:Connector_app`
applicationUserAgent	Optional	The part of the user agent string that identifies the application. Can be empty or non-present.
applicationPort	Mandatory for manual mode	The configured port of Trusted Application to listen to incoming connections. Example: `6001`
computerGruu	Mandatory for manual mode	Computer GRUU of Trusted Application. The value is unique for each Connector. Example: `sip:computer1.lyncdco.lab@lyncdco.lab;gruu;opaque=s` `oZ_uG-ia3xAAA`
certificateThumbprint	Mandatory for manual mode	The thumbprint of the certificate to use for Trusted Application.
serverAddress	Mandatory for manual mode	The FQDN of FrontEnd of Skype for Business Server for the UCMA application connection. Example: `pool01.lyncdco.lab`
serverPort	Mandatory for manual mode	The port of FrontEnd of Skype for Business Server for the UCMA application connection. Example: `5061`
connectorCertificate	Optional	Thumbprint of the certificate to use for the TLS connection with T-Server.

- Section **log**—Optional section. Describes the standard Genesys logging options. Default options for logging:
  - **verbose** = `all`
  - **all** = `lyncConnector`

    - **expire** = `3`
    - **segment** = `50 MB`
    - **keep-startup-file** = `1 MB`

- Section **miscParams**—Optional section. Describes the miscellaneous options used by Connector:
    - **caching-enabled**—Enables conference caching by default. Conference caching allows to reuse previously scheduled conferences. It reduces the load of Skype for Business Server and the time for establishing new calls. To disable conference caching, configure this option with a value of `0`, as follows:

      ```
      <miscParams>

      <add key="caching-enabled" value="0" />

      </miscParams>
      ```

    - **musicOnHoldFilePath**—Optional. Specifies the path (full path, relative path or network path are supported) to the file with music that will be used as Music On Hold. The Connector supports audio file .wma type.

Back to Deployment Summary

Managing T-Server

This section describes how to configure, install, and start/stop T-Server for Skype for Business.

Configuring T-Server

1. Using Genesys Administrator (or Configuration Manager), create an Application object of type `T-Server` in accordance with the procedure for server-type applications as described in the Management Framework Deployment Guide.
2. On the Connections tab, add a SIP Server application to which this T-Server must connect. You can leave the default values for other fields.
3. On the Options tab, configure common T-Server options that manage licensing and logging. (Sections **[license]** and **[log]**.) See Configuration Options.
4. Configure T-Server options in the **[TServer]** section:

   link-*n*-name—Mandatory option. This option defines the name of the section where you configure connection parameters for T-Server and Connector, where *n* is a consecutive number for a Connector—for example, **link-1-name**=`connector1`.

   - Create a section with the name specified by the **link-*n*-name** option—for example, **[connector1]**.
   - In the section dedicated to the Connector—for example, **[connector1]**—specify the following options:
     - **hostname**—Set to the host name where this Connector runs.
     - **port**—Set to the port number of this Connector.
     - **protocol**—Set to `tcp`, the transport protocol to be used between T-Server and this Connector.

   Configuration example for a single Connector:

   ```
   [TServer]
        link-1-name=connector1

        [connector1]

        hostname=computer1.lyncdco.lab

        port=9001

        protocol=tcp
   ```

   Configuration example for three Connectors:

   ```
        [TServer]

        link-1-name=connector1

        link-2-name=connector2
   ```

```
link-3-name=connector3
[connector1]
hostname=computer1.lyncdco.com
port=9001
protocol=tcp
[connector2]
hostname= computer2.lyncdco.com
port=9001
protocol=tcp
[connector3]
hostname= computer3.lyncdco.com
port=9001
protocol=tcp
```

5. Configure the following configuration options in the **[extrouter]** section:
   - **cast-type** = `route pullback`
   - **use-data-from** = `current`
   - **event-propagation** = `list`

Other configuration options enable or disable supported T-Server functionality. See Configuration Options for option descriptions. See Multi-Site Support for information about multi-site functionality. See High Availability for information about the High Availability configuration.

Installing T-Server

Prerequisites: T-Server Application object is created in the Genesys configuration environment.

1. In the directory to which the T-Server installation package was copied, locate and double-click **Setup.exe** to start the installation.
2. When prompted, specify the connection parameters to the Configuration Server associated with this T-Server.
3. When prompted, select the T-Server Application object you configured in Configuring T-Server from the list of applications.
4. Specify the license information that T-Server is to use: either the full path to, and the name of, the license file, or the license server parameters.
5. Specify the destination directory into which T-Server is to be installed.
6. Click **Install** to begin the installation.
7. Click **Finish** to complete the installation.

By default, T-Server is installed as a Genesys service (Windows Services) with Automatic startup type.

Starting T-Server

Before starting T-Server, be sure that the following components are running:

- Configuration Server
- License Manager

You can start and stop Framework components using the Management Layer, a startup file, a manual procedure, or the Windows Services Manager. With all these methods, command-line parameters are usually required for a server application in addition to an executable file name.

Starting T-Server on Windows manually

Start T-Server from either the Start menu or the MS-DOS window. If you use the MS-DOS window, go to the directory where T-Server is installed, and type the following command-line parameters:

```
mslync_server.exe -host <Configuration Server host> -port <Configuration Server port>
-app <T-Server Application> -l <license address> -nco [X]/[Y]
```

For starting server applications using the Management Layer or the Windows Services Manager, see Starting and Stopping Framework Components in the *Management Framework Deployment Guide*.

Stopping T-Server

To stop a server application on Windows, do one of the following:

- Type `Ctrl+C` in the application's console window.
- Click **End Task** in the Windows Task Manager.

For stopping server applications using the Management Layer or the Windows Services Manager, see Starting and Stopping Framework Components in the *Management Framework Deployment Guide*.

Configuration Options

- Common Configuration Options
- T-Server Common Configuration Options
- T-Server-specific options

Back to Deployment Summary

Upgrading Multimedia Connector for Skype For Business

Upgrade of Connectors must be performed in the maintenance window. The Skype for Business Contact Center must not be operating during this upgrade.

T-Server and Connectors Upgrade Procedure

1. Shut down both primary and backup T-Servers to move all Connectors into passive mode and prevent receiving incoming calls.
2. Shut down all Connectors.
3. Back up the Connector configuration files to prevent them from being overwritten during the upgrade.
4. Upgrade all T-Servers for Skype for Business to a new version.
5. Upgrade all Connectors to a new version.
6. Restore the Connector configuration files, if required.
7. Start all Connectors.
8. Start primary and backup T-Servers.

Procedure to apply Skype for Business Cumulative Updates

To update Microsoft UCMA components, you must perform the following steps:

1. Shut down both primary and backup T-Servers to move all Connectors into passive mode and prevent receiving incoming calls.
2. Shut down all Connectors.
3. Follow the Microsoft recommended procedure to install Cumulative Updates.
4. Start all Connectors.
5. Start primary and backup T-Servers.

> **Important**
>
> If Front End Servers are stopped during normal operation, it can impact ongoing contact center activities. See Skype For Business Front End Server Maintenance for details.

Configuring Skype for Business Application Endpoints

You can configure Skype for Business application endpoints using the Management Shell.

Using the procedures described in Microsoft documentation, complete the following steps:

1. Create **Trusted Application Endpoints** for Routing Points.
   For example:
   ```
   New-CsTrustedApplicationEndpoint -ApplicationId “Connector_app”
   -TrustedApplicationPoolFqdn “trustedpool.lyncdco.lab” -SipAddress
   “sip:RP1@lyncdco.lab” –LineURI TEL:16505551212
   ```
   - where the value of the parameter `SipAddress` must correspond to the name of the Routing Point DN object in the Genesys configuration environment.
2. Create **Trusted Application Endpoints** for External Routing Points.
   For example:
   ```
   New-CsTrustedApplicationEndpoint -ApplicationId “Connector_app”
   -TrustedApplicationPoolFqdn “trustedpool.lyncdco.lab” -SipAddress
   “sip:ERP1@lyncdco.lab” –LineURI "TEL:14155551212"
   ```
   - where the value of the parameter `SipAddress` must correspond to the name of the External Routing Point DN object (in the Genesys configuration environment) and the `<number>` in the parameter `LineURI` must correspond to the `Association` field of that External Routing Point object.
3. Create **Trusted Application Endpoints** for conference services.
   The endpoint names must be created based on the pattern in the **uri-pattern** option and their quantity must match the **count** option set on the Switch object.

   For example: If `uri-pattern=sip:conf{DD}@lyncdco.lab` and `count=99`, then you must create 99 endpoints with names from `sip:conf01@lyncdco.lab` to `sip:conf99@lyncdco.lab`, where numbers from 1-99 are endpoint numbers.

   See also how to work with conference resource pools

Trusted Application Endpoints for conference services

See Conference Resource Pools for details.

Configuring Skype for Business User Endpoints

To configure Skype for Business User endpoints:

1. Create users in Active domain if required. A Skype for Business user must have a corresponding domain account. See details in Microsoft documentation.
2. Add and enable users using the Skype for Business Server procedure described at the following links of Microsoft TechNet Library:
   - Using the Server Control Panel:
     Skype for Business

     Lync Server 2013

     Or
   - Using Microsoft PowerShell
3. Create an Extension DN (in the Genesys configuration environment) for each Lync user with the number corresponding to the SIP URI of the Lync user.

Important

T-Server does not support TEL URI for Skype for Business users. Therefore, only the SIP URI must be configured for Skype for Business users and only this SIP URI must be used for routing and calls.

Warning

Do not delete Skype for Business users during their active calls. Doing so might have an unpredictable effect on the call.

High-Availability Deployment

This section describes the general steps for setting up a high-availability (HA) environment for T-Server and UCMA Connector for Skype for Business or for Lync 2013.

Skype for Business High Availability

The main high-availability scheme for most server roles in Skype for Business or Lync 2013 is based on server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors. Skype for Business also enhances Back End Server high availability, by supporting synchronous SQL mirroring for your Back End databases.

For information about high availability, see Microsoft documentation:

- Microsoft Skype for Business Server 2015
- Microsoft Lync Server 2013

Note: Skype for Business or Lync 2013 high-availability features are available for the Enterprise edition only.

Deployment

For information about deploying high availability, see Microsoft documentation:

- Microsoft Skype for Business Server 2015
- Microsoft Lync Server 2013

T-Server High Availability

The high-availability architecture of T-Server for Skype for Business implies the existence of redundant applications, a primary and a backup. These are monitored by a management application so that, if one application fails, the other can take over its operations without any significant loss of contact center data. The Framework Management Layer currently supports two types of redundant configurations: warm standby and hot standby. Microsoft Lync Server 2013 supports both warm and hot standby. Microsoft Skype for Business Server 2015, however, supports only hot standby.

Licensing HA Implementations

T-Servers operating with the hot standby redundancy type require a special CTI HA technical license, which allows for high-availability implementations, in addition to regular T-Server licenses. Neither T-Server in a redundant pair configured for hot standby starts if this license is unavailable. Moreover, the primary and backup T-Servers must use the same licenses to control the same pool of DNs. If your T-Servers are configured with the hot standby redundancy type, order licenses for CTI HA support.

Synchronization Between Redundant T-Servers

When T-Servers operate in a high-availability environment, the backup T-Server must be ready to take on the primary role when required. For this purpose, both T-Servers must be running and must have the same information. When you configure redundant T-Servers to operate with the hot standby type, the primary T-Server uses the connection to the backup to deliver synchronization updates. Genesys recommends that you enable the Advanced Disconnect Detection Protocol (ADDP), for this connection. Do so using the configuration options in the “Backup-Synchronization Section” section. Refer to the T-Server Common Configuration Options chapter for option descriptions.

Configuration Warnings

When configuring T-Servers to support hot standby redundancy type, remember:

- When at least one of the two T-Servers that operate in a redundant mode is running, do not change a redundancy type, host, or port in either T-Server configuration.
- When both the primary and backup T-Servers are running, do not remove the backup T-Server Application object from the configuration.
- You are responsible for the option synchronization in the configuration of the primary and backup T-Servers; Configuration Server does not synchronize either options or their values in different T-Server Application objects. That is, you must configure both T-Servers to have the same options with the same values. If you change a value in one T-Server configuration, you must change it in the other T-Server configuration manually. The log options in the primary T-Server can differ from those in the backup T-Server configuration. The link configuration options in the primary T-Server can also differ from those in the backup T-Server configuration.

> Important
>
> Genesys strongly recommends that you install the backup and primary T-Servers on different host computers.

Hot Standby Redundancy

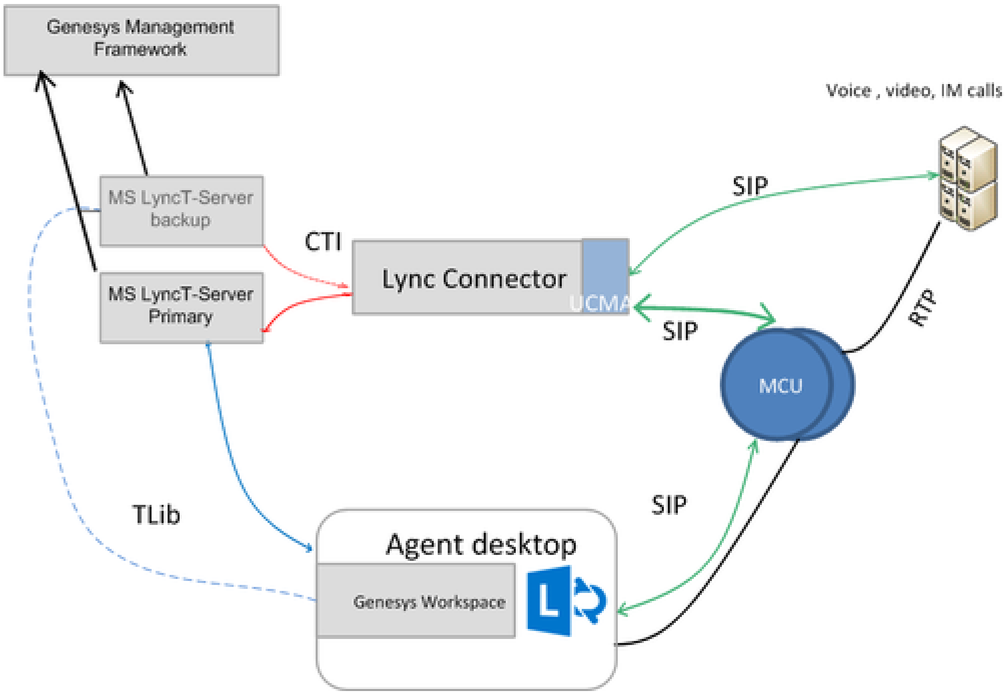
Genesys uses the expression *hot standby* to describe the redundancy type in which a backup server application remains initialized, clients connect to both the primary and backup servers at startup, and the backup server data is synchronized from the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component.

T-Servers start simultaneously and connect to the switch via Connector component. At T-Server startup, the Management Layer assigns the role of the primary server to T-Server 1, and the role of backup to T-Server 2. T-Server clients register with both T-Servers, but only the primary T-Server handles client requests other than the registration requests. The internal T-Server information is synchronized between the primary and backup T-Servers, such as:

- Calls (all necessary information including UCMA data)

- Device info
- Monitoring subscriptions
- Agent states
- Remote Treatment sessions

Therefore, the backup T-Server has the same information as the primary T-Server. If T-Server 1 fails, the Management Layer makes T-Server 2 the new primary server, and it starts processing client requests. The Management Layer attempts to restart T-Server 1, and if it is successful, it makes T-Server 1 the new backup server.



Benefits of Hot Standby Redundancy

The hot standby redundancy type provides the following benefits:

- Ensures the processing of interactions in progress if a failure occurs. After the primary T-Server (T-Server 1) fails, T-Server 2 handles all new interactions and takes over the processing of interactions that are currently in progress.
- T-Servers perform one-way (from primary to backup) synchronization of call-associated data, including, but not limited to:
  - Connection IDs.
  - Attached user data.
  - Inter Server Call Control (ISCC; formerly called External Routing) call references to another site in a multi-site environment (to support the ISCC/COF feature).
  - Allocation of ISCC-controlled resources.

Deployment

The general guidelines for T-Server hot standby configuration are:

1. Configure two T-Server Application objects as described in Configuring T-Server.
2. Make sure the Switch object is configured for the switch these T-Servers should serve, as described in Switches.
3. Modify the configuration of the primary and backup T-Servers as instructed below.

Modifying the primary T-Server configuration for hot standby

1. Stop both primary and backup T-Servers if they are already running.
2. Using Genesys Administrator or Configuration Manager, open the Properties dialog box of the Application object for the T-Server that you want to configure as a primary server.
3. On the **Switches** tab, ensure that it specifies the Switch that this T-Server Application should serve. If necessary, select the correct Switch using the Browse button.
4. In the **Server Info** tab:
   - In the Ports section, select the port to which the backup server will connect for HA data synchronization and click **Edit Port**. In the Port Properties dialog box, on the **Port Info** tab, select the **HA sync** check box.
   - Specify the T-Server Application you want to use as the backup server. Use the Browse button next to the Backup Server field to locate the backup T-Server Application object.
   - Select **Hot Standby** as the Redundancy Type.
5. On the **Start Info** tab, select **Auto-Restart**.
6. To enable ADDP between the primary and backup T-Servers, click the **Options** tab. Open or create the **[backup-sync]** section and configure corresponding options.

Modifying the backup T-Server configuration for hot standby

1. Ensure the two T-Servers are not running.
2. Using Genesys Administrator or Configuration Manager, open the Properties dialog box of the Application object for the T-Server that you want to configure as a backup server.
3. On the **Switches** tab, using the Browse button, select the same Switch object you associated with the primary T-Server Application.
4. On the **Server Info** tab:
   - In the Ports section, select the port to which the primary server will connect for HA data synchronization and click **Edit Port**. In the Port Properties dialog box, on the **Port Info** tab, select the **HA sync** check box.
5. On the **Start Info** tab, select **Auto-Restart**.
6. On the **Options** tab, modify the values for all necessary configuration options. Genesys recommends that you set all configuration options for the backup T-Server to the same values as for the primary T-Server; the only exceptions are the log options and the **server-id** option.

Known T-Server HA Limitations

The following limitations apply to T-Server HA:

- Client requests sent during the failure and switchover might be lost.
- Treatment sessions are not synchronized between the primary and backup T-Servers and are interrupted if the primary T-Server goes down or is switched over.
- Routing requests sent by the switch during the failure and switchover might be lost.
- T-Server does not synchronize interactions that begin before it starts.
- Some T-Library events might be duplicated or lost.
- Reference IDs from client requests can be lost in events.
- Only *hot standby* redundancy type is supported.
- During a T-Server switchover, an unfinished single-step transfer of an instant messaging or audio/video call can lead to lost information about a transfer controller in T-Library messaging. Queries performed for this call might return all parties participating in the single-step transfer as being in a conference call.

UCMA Connector High-Availability

The high-availability architecture for UCMA Connector for Skype for Business implies:

- UCMA HA data storage
- Synchronization of HA data between UCMA Connector and T-Server
- Existence of a pool of UCMA Connectors (Skype for Business 2015 or Lync Server 2013 Enterprise edition only)

UCMA HA Data Storage

To prevent loss of calls if the server disconnects, the Connector stores all necessary HA call data, such as:

- Conferences
- Conversations
- Calls and parties
- B2B calls

This information allows UCMA Connector to recover calls after the restoration of communication with Skype for Business.

Synchronization of HA data between UCMA Connector and T-Server

To provide high-availability of existing calls, UCMA Connector synchronizes all necessary HA call data with T-Server. Data synchronization comprises information about:

- Conferences info
- Conversations info
- Calls and parties info
- B2B calls info

This information allows T-Server and UCMA Connector for Skype for Business to recover calls after Connectors restart.

Pools of UCMA Connectors

A pool of UCMA Connectors allows the T-Server and UCMA Connector environment to proceed working normally, even if some Connectors are down. In this case, T-Servers redistribute DNs from non-working Connectors to remaining Connectors. Skype for Business distributes all incoming calls to remaining Connectors. After recovery, each Connector will try to restore calls according to HA information received from T-Server.

Note: Pooling of UCMA Connectors is available only with Skype for Business Server 2015 or Lync Server 2013 Enterprise edition.

Deployment

Storage of UCMA HA data and synchronization of HA data between UCMA Connector and T-Server work automatically and do not require additional configuration.

A pool of UCMA Connectors can be configured as described in Provisioning for UCMA Connectors.

Known Connector HA Limitations

- Instant Message calls cannot be recovered after the Connector restarts.
- Calls can only be recovered on the Connector where they were originally created, after the Connector restarts.
- Graceful shutdown and in-service upgrade of Connector is currently not supported

Performance

To enhance connector performance and reduce server workload at peak times, Genesys recommends that you enable conference pooling and AudioVideo call reuse. Environments that serve over 500 agents must enable conference pooling.

To use these features, you must ensure that conference caching is enabled (it is by default) and configure at least one service endpoint (also part of a default installation).

> **Important**
>
> Genesys recommends that when deploying in contact centers with hundreds of agents, and depending on the volume of additional enterprise Skype for Business traffic, all agents should be in the same Skype for Business FE Servers pool, with no other Skype for Business users in that pool. That is, there should be one pool reserved to Genesys and the contact center agents.

See performance tests results in the Hardware Sizing Guidelines and Capacity Planning topic.

Conference pooling

When enabled, conference pooling pre-creates a number of conferences, reducing conference startup time and on-demand workload.

The option conference-pool-size sets the number of conferences the pool maintains at one time. Set the value to 20% higher than the maximum number of simultaneous calls handled by the connector.

The connector creates conferences one at a time until it reaches the configured pool size, then creates new ones whenever a conference is used or expires.

AV call reuse

AudioVideo call reuse can reduce initial call handling time. To eliminate a memory leak that can occur with excessive call reuse, however, set the option reuse-avcall to a relatively low value, no greater than 50.

Managing Workspace Plugin for Skype for Business

Overview

Genesys provides a plugin that adds functionality to Workspace Desktop Edition to tightly integrate it with the Skype for Business client on the agent desktop. Through the plugin, agents can handle voice, video, and instant messaging interactions handled by Skype for Business, in addition to accessing their Skype for Business contacts and seeing their presence status.

Important

- Video is available only in a Skype for Business environment, and not with Lync 2013.
- If Skype for Business 2016 is installed on the Workspace Desktop, then apply registry changes as described in Microsoft documentation. Administrator rights are required to make these registry changes.
- The Workspace Desktop Edition SIP Endpoint Role must only be activated when operating Workspace Plugin for Skype for Business in Hybrid mode with SIP Server.

Prerequisite

Workspace Plugin for Skype for Business requires the full version of the Skype for Business client that is delivered as part of either Microsoft Office 2013 or 2016 to be installed on the agent desktop. Correct operation is not guaranteed if using the Skype for Business Basic (free) client version.

Deployment

1. Configure Workspace Desktop Edition. Note the following:
    - To use role-based access control, you must use Genesys Administrator to configure Workspace Desktop Edition and the Plugin. Be sure that your configuration procedure includes importing the template and metadata (see the Genesys Administrator 8.1 Help for information on importing metadata). This makes roles and other required items available.
    - Genesys recommends to assign the "Instant Messaging: Can release" privilege to all agents, since some Skype for Business clients might not support disconnection functionality for IM calls. See details in the Workspace Desktop Edition documentation.

2. Install Workspace Desktop Edition.
3. Install Workspace Plugin for Skype for Business for each Workspace Desktop Edition that your agent uses. Be sure that your configuration procedure includes importing the template and metadata for the Plugin.
4. Assign privileges, if you are using role-based access control. The following privileges are available:
   - **IM - Can Delete From Conference:** Enables the initiator of a conference to delete a party from a conference.
   - **IM - Can One Step Conference:** Enables instant conference of an IM call.
   - **IM - Can One Step Transfer:** Enables instant transfer of an IM call.
   - **IM - Can Set Interaction Disposition:** Allows an agent to set a Disposition code during or after an IM call.
   - **Skype for Business - Can Use Plug-in for Microsoft UC:** The agent is permitted to use functions of Workspace Plugin for Skype for Business. The other privileges of Microsoft Skype for Business cannot be configured if the value is Not Assigned.
   - **Skype for Business - Can change presence:** The agent is permitted to change presence of the associated Skype for Business user.
   - **Video - Can Join Lync Video Channel:** The agent is permitted to join an existing Skype for Business video channel.
   - **Video - Can Use Lync Video Channel:** The agent is permitted to use the Skype for Business video channel.
5. Disable the "Voice - Can Suspend or Reinstate A Conference Party" role, because the Plugin does not support it.
6. Provide values for the configuration options that you added to your Workspace Desktop Edition application.

Silent installation/upgrade

You can silently install or upgrade the Skype for Business Workspace Plug-in by using the following command-line entry:

```
.\setup.exe /s /z"-s C:\Downloads\WPluginMSUC\8.5.000.83\genesys_silent.ini -sl c:\logs\
plugin.log
```

Skype for Business Client

> **Important**
>
> Ensure that you follow recommended instructions and Microsoft Patching Policy.

Operating modes

When used with the Workspace Plugin, the Skype for Business client can run in parallel mode with parallel Workspace and Skype for Business windows on the agent screen or in GUI-suppressed mode, where Agents see only the WDE interaction window on the screen.

You can run the commands within the **GUISuppressionCommands/ EnableUISuppressionMode.reg** and **GUISuppressionCommands/ DisableUISuppressionMode.reg** files found in your deployment package.

To run the GUI-suppressed mode command:

- Stop the Skype for Business client.
- Double-click the **GUISuppressionCommands/EnableUISuppressionMode.reg** file and accept the informational dialog boxes that follow.

The next time it starts, Genesys Workspace Desktop Edition starts the Skype for Business client in GUI-suppressed mode.

To run the parallel mode command:

- Stop the Skype for Business client.
- Double-click the **GUISuppressionCommands/DisableUISuppressionMode.reg** file and accept the informational dialog boxes that follow.

The next time it starts, Genesys Workspace Desktop Edition starts the Skype for Business client in parallel mode.

The parallel or suppressed mode of the Skype for Business client used by the Workspace Plugin affects the preferred setting for direct call handling.

Starting Skype for Business Client

Starting with version 8.5.00.81, Workspace Plugin provides the ability to dynamically control the registry settings that define the suppressed mode of the Skype For Business Client, by using the **lync.parallel-gui** option in the **[interaction-workspace]** section.

Prior to version 8.5.000.81, to install the plugin in Workspace, you had to make registry changes directly on the Agent desktop to control the GUI-suppressed mode that was used. Therefore, if the same agent worked on another desktop, the same registry changes had to be made manually in the other desktop as well.

To control the registry settings, use the **lync.parallel-gui** option, which can be defined at the Application and Person object levels.

lync.parallel-gui
Setting: **[interaction-workspace]** section, at Application, Person levels
Default value: `registry`
Valid values: `true`, `false`, `registry`, `auto`
Changes take effect: After restart

For all settings, Workspace Plugin cleans up any processes which had been previously started:

- `true`: Sets the registry keys for parallel mode and starts.
- `false`: Sets the registry keys for suppressed mode and starts.

- `registry`: Provides support for backward compatibility and refers to the registry to determine the GUI mode.
- `auto`: Searches for a running Skype for Business Client. If found, Workspace Plugin starts in parallel UI mode. If not found, Workspace Plugin starts in suppressed mode.

Limitations

- Workspace Plugin does not affect the Skype for Business Client started by the agent.
- If the Skype for Business Client is terminated, Workspace Plugin cannot determine if a process that is incomplete or stops responding is a working process or not. The agent must check and clean up any unrequired non-working processes
- The agent must have rights to make changes to the local space registry.
- The agent must have rights to the deleted processes that were started.

Configuration Options

Application Options

In the Workspace Desktop Edition application, update the following existing options in the **[interaction-workspace]** section:

- **teamcommunicator.list-filter-showing** = `Agent,AgentGroup,Skill,RoutingPoint,Queue, InteractionQueue,Contact, LyncContact`
- **expression.team-communicator-phone-number** = `.*`
- **expression.phone-number** = `0123456789#*ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz-_@:.+`
- **expression.phone-number.supported-characters** = `0123456789#*ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz-_@:.+`

> **Important**
>
> If you want the video popup for a video call to appear on top of the Workspace window, you must set the Workspace options **interaction.window.popup-topmost-z-order** and **interaction-bar.enable-quick-access** to `false`.

DN Object Options

In the Skype for Business Switch configuration object, add the DNs for the Skype for Business agents. The value must be the URL of the Skype for Business—for example, `sip:skypeuser1@skypedco13.lab`.

Because this DN is used for multiple operations (voice, and IM), set the following options on the **Annex** tab in the **[TServer]** section:

- **multimedia** = `true`
- **voice** = `true`

Warning

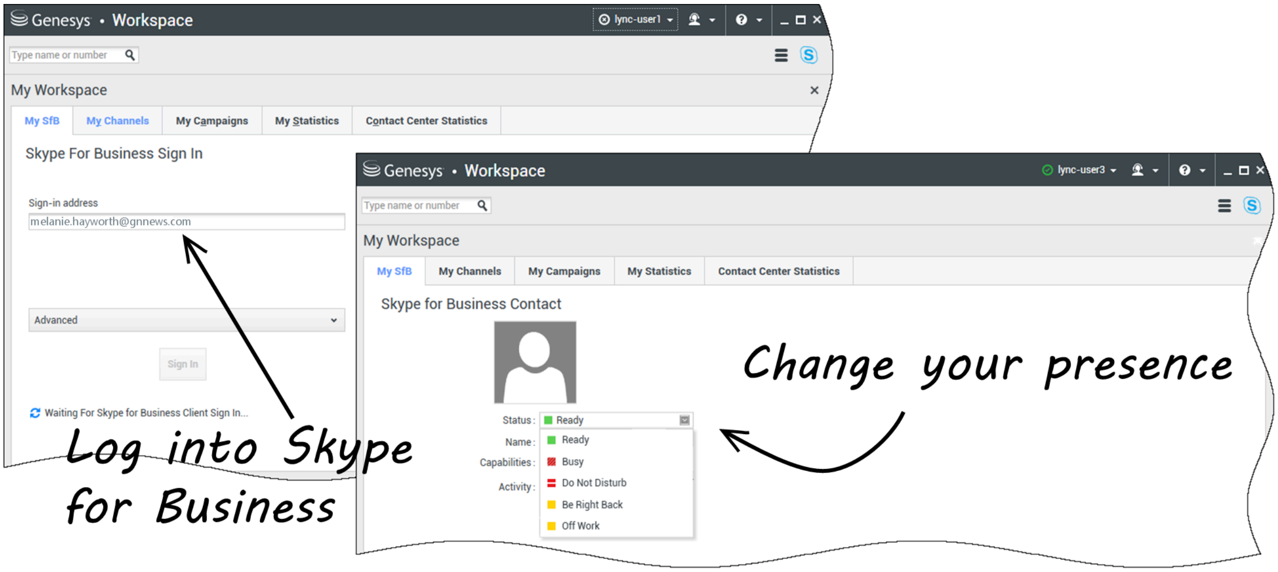
Direct calls between Skype for Business users are supported by the Plugin only when they are initiated through T-Server for Skype for Business. Direct calls initiated from the Skype for Business client are not supported.

Using Workspace Plugin for Skype for Business

For information about the general functionality for Workspace Desktop Edition, see the *Workspace User's Guide*.

> **Important**
>
> For this version of the Workspace Plugin for Skype for Business, Genesys supports Microsoft Lync 2013 and Skype for Business Server.

Logging into Workspace Desktop Edition to Access Skype for Business



Sign-in address: melanie.hayworth@gnnews.com

Status : Ready

Log into Skype for Business

Change your presence

When you log into Workspace Desktop Edition, you'll see the **My SfB** tab in your **My Workspace** screen, and you sign in to Skype for Business with your Skype for Business username and password.

> **Tip**

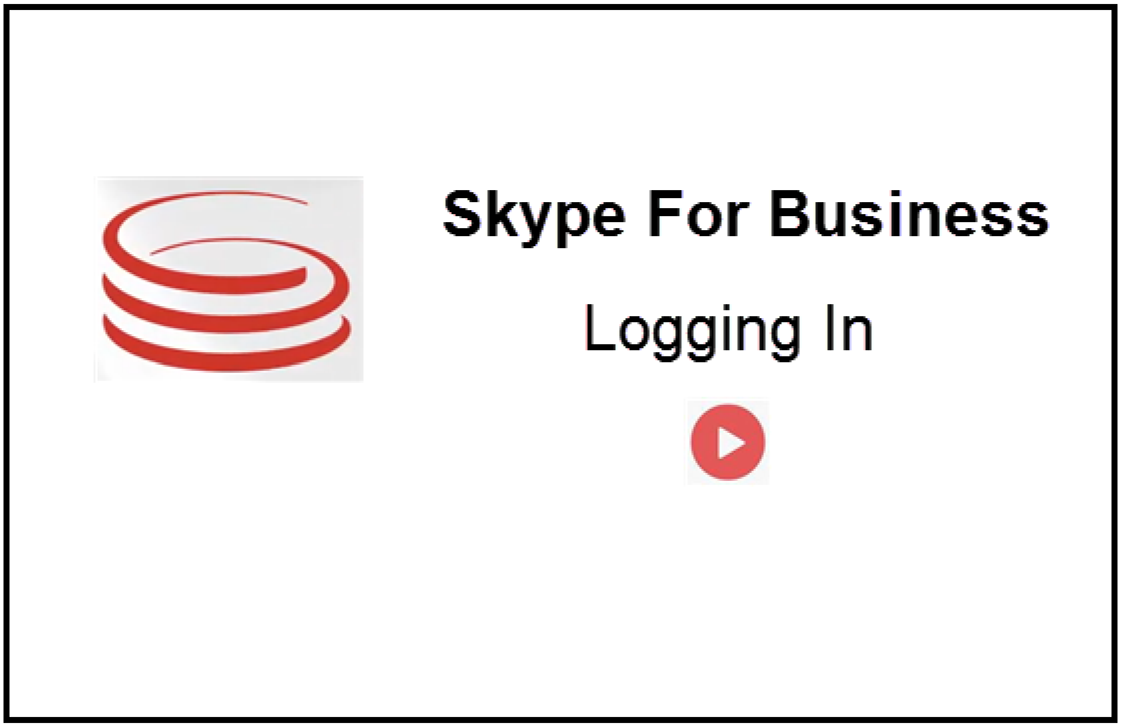
If you want to automatically log into Skype for Business the next time you log into your desktop, select **Remember Password**.

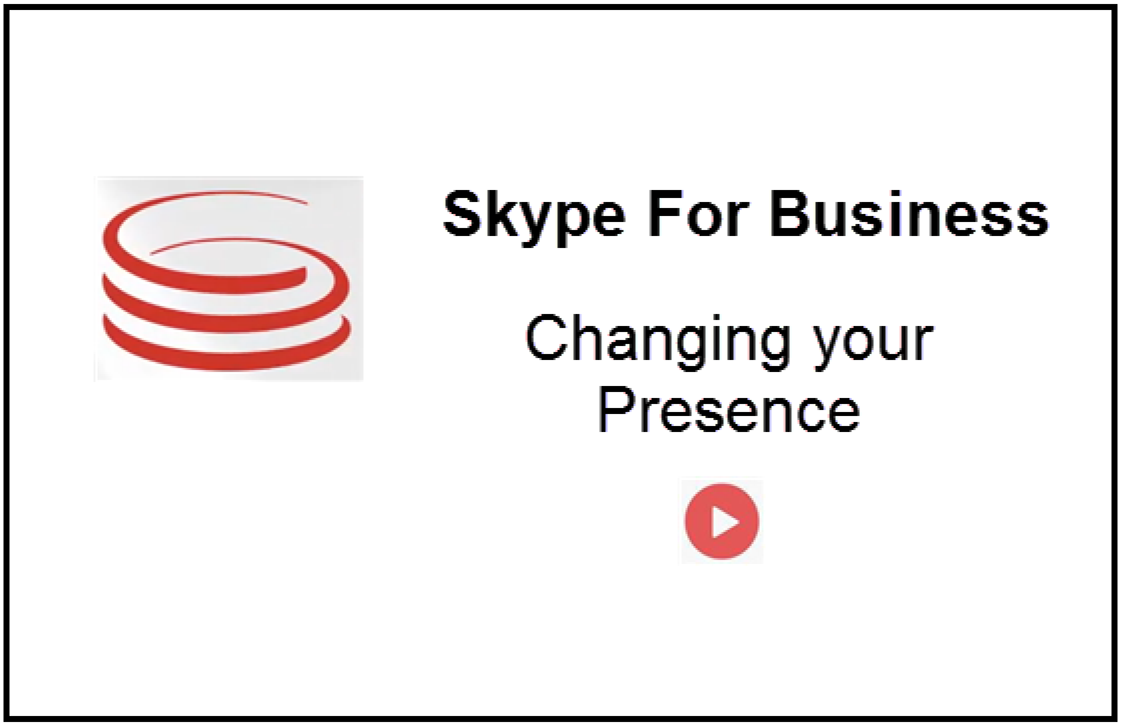
You can now control your Skype for Business presence on this tab.

Warning

While you can change the presence status that is shown to your Skype for Business coworkers, this is advisory only. The Genesys software will continue to route interactions to you, unless you change your status from the main Workspace Desktop toolbar.

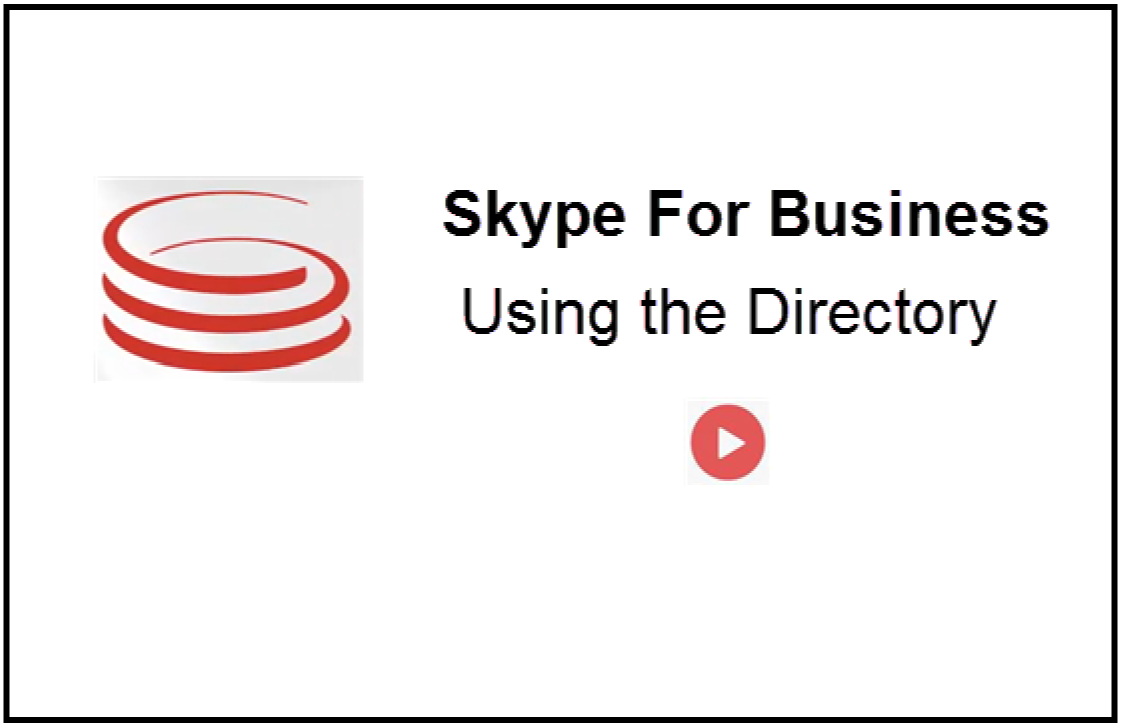
Watch these videos:





Skype For Business

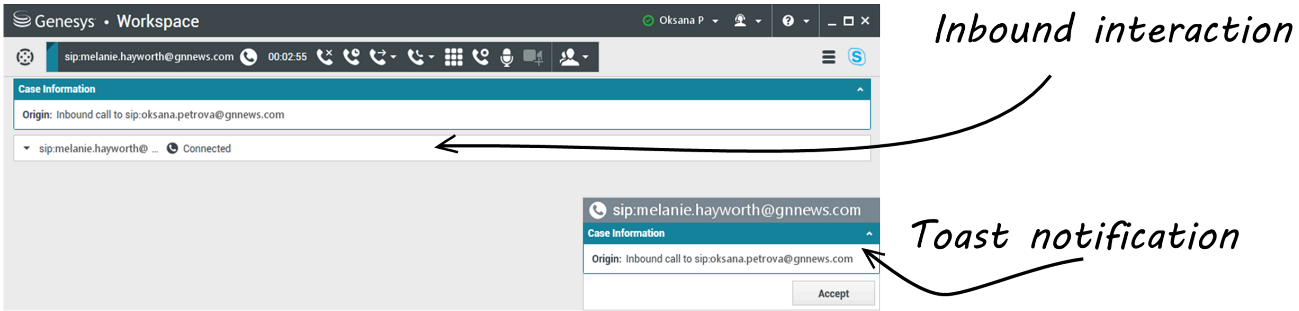
Changing your Presence



Skype For Business

Using the Directory

Accepting or Rejecting Interactions



sip:melanie.hayworth@gnnews.com 00:02:55

Case Information

Origin: Inbound call to sip:oksana.petrova@gnnews.com

sip:melanie.hayworth@ ... Connected

sip:melanie.hayworth@gnnews.com

Case Information

Origin: Inbound call to sip:oksana.petrova@gnnews.com

When a new inbound Skype for Business interaction is sent to your workstation, a toast notification is displayed at the bottom right-hand corner of your desktop.

You can:

- **Accept** — Open the interaction in the Workspace Desktop window.
- **Reject** — Decline the interaction. (Only visible if the interaction is sent through a Route Point)

If you do not accept the toast notification, it times out, and the interaction is not established.

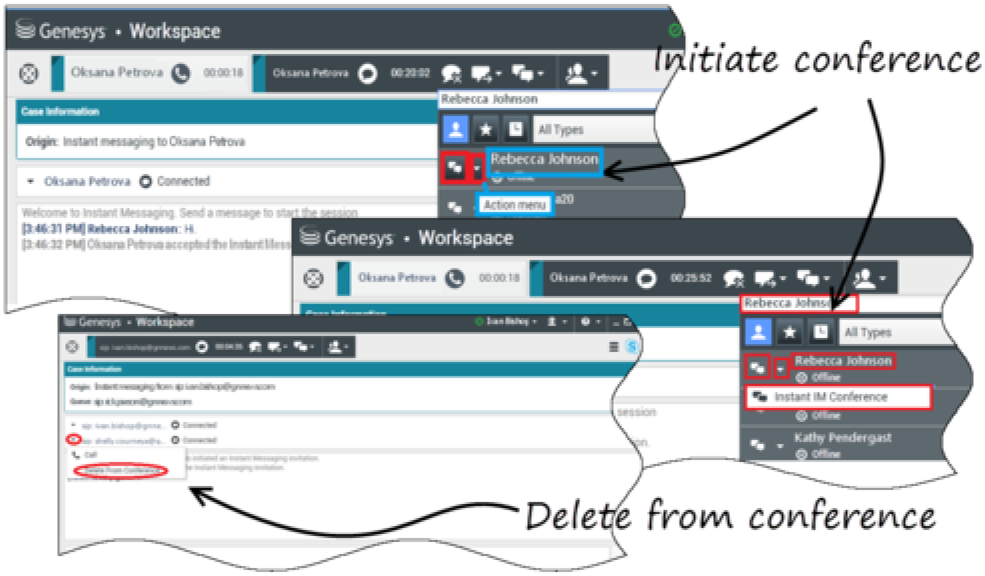
If you accept the toast notification, the inbound interaction view is displayed.

IM Interactions

When you are in an Instant Messaging (IM) interaction and require additional information, you have the following options:

- IM Conferencing: You can add another agent to an existing IM interaction.
- IM Transferring: You can transfer an IM interaction to another agent.
- IM Consultation: You can consult with another agent.
- Escalating to Voice: You can escalate an IM interaction to a voice interaction. Once you have escalated an IM interaction to a voice interaction, you can escalate it again to video, if the customer has already activated video. You cannot escalate to video directly from an IM interaction.
- Handling IM Transcripts: You save and restore an IM transcript.

IM Conferencing



Welcome to Instant Messaging. Send a message to start the session

[3:46:31 PM] Rebecca Johnson: Hi.

[3:46:32 PM] Oksana Petrova accepted the Instant Mess

Initiate conference

Delete from conference

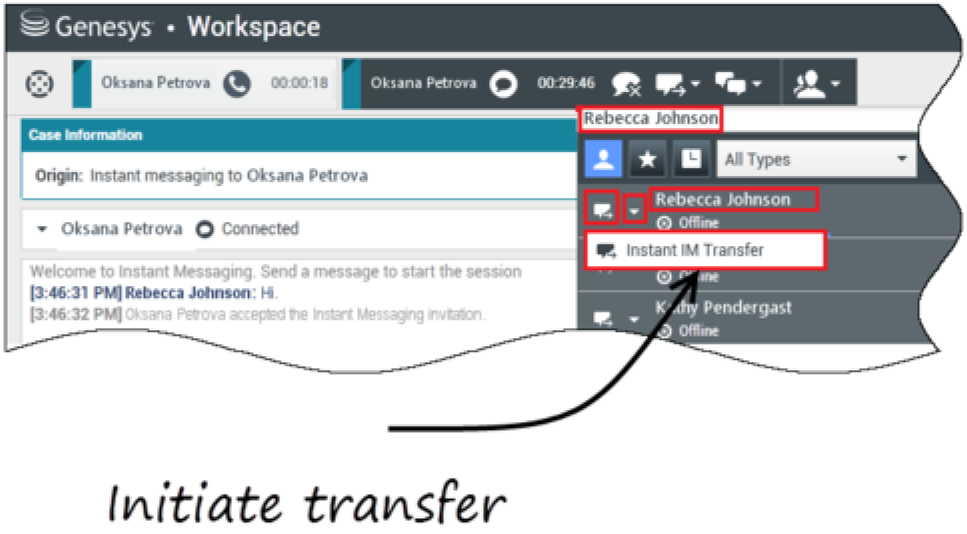
You can add another agent to an existing IM interaction. Select **Instant IM Conference**, and type the agent's name or contact URI into the text box. When you find the agent's name from the list, select **Instant IM Conference**, or the icon next to the agent's name.

The other agent receives a toast notification. The other agent can either accept or reject the interaction.

Now you can exchange IM messages with all parties in the conference.

When you are finished with the IM conference, you can remove either yourself or the other agent from the IM.

IM Transferring



Case Information

Origin: Instant messaging to Oksana Petrova

Welcome to Instant Messaging. Send a message to start the session

[3:46:31 PM] Rebecca Johnson: Hi.

[3:46:32 PM] Oksana Petrova accepted the Instant Messaging invitation.

Initiate transfer

You can transfer an existing IM interaction to another destination (agent, queue, route point, etc). Select **Instant IM Transfer**, and type the agent's name or contact URI into the text box. You can also find the agent's name from the list of all agents. Select the Action menu or the icon next to the agent's name.

The other agent receives a toast notification and can either accept or reject the interaction.

IM Consultation

Link to video

You can consult with another agent on an existing IM interaction. Select **Start a Consultation**, type the agent's name or contact URI into the text box, and select **Start Instant Message Consultation** from the Action menu.

A consultation IM window opens below the existing IM window. Type your IM message in the text field and press **Send**. A toast notification is displayed on the selected user site. The consultation IM is established when the agent accepts the toast notification for consultation IM.

You can now exchange messages with the other agent before returning to the conversation with your customer.

[+] See a screenshot.

500px

Escalating to Voice

Link to video

Your customer might need to escalate the conversation from IM to voice or vice versa. The customer uses their Skype for Business client to initiate a voice call or an IM interaction to you. By default, the voice escalation call is auto-answered. However, an agent can answer the call manually if the **interaction-workspace\lync.voice-escalation-auto-answer** option is set to `false`.

Or, you might need to escalate the conversation from IM to voice or vice versa. Use your Workspace Desktop to initiate a voice call or an IM interaction to your customer.

[+] See some screenshots.

file:Skype_plugin_consult.png file:Skype_plugin_agent.png

Voice Interactions

When you are in a voice interaction and require additional information, you have the following options

- Voice Conferencing: You can add another agent to an existing voice interaction.
- Voice Transferring: You can transfer a voice interaction to another agent.
- Voice Consultation: You can pause a voice interaction while you consult with another agent.
- Escalating to Video: You can escalate a voice interaction to a video interaction, if the customer has already activated video. You, as the agent receiving the call, cannot choose unilaterally to escalate to video. Only the originator of the call can escalate to video.

Voice Conferencing

You can add another agent to an existing voice interaction. Select **Instant Voice Conference**, and type the agent's name or contact URI into the text box. When you find the agent's name from the list, select **Instant Voice Conference**, or the icon next to the agent's name. The other agent receives a toast notification. The other agent can either accept or reject the interaction. You, the customer, and the other agent are placed into a three-way conference. When you are finished with the voice conference, you can remove either yourself or the other agent from the voice conference.

Voice Transferring

You can transfer an existing voice interaction to another destination (agent, queue, route point, etc). Select **Instant Voice Transfer**, and type the agent's name or contact URI into the text box. You can also find the agent's name from the list of all agents. Select the Action menu or the icon next to the agent's name. The other agent receives a toast notification and can either accept or reject the interaction.

Voice Consultation

You can consult with another agent on an existing voice interaction. Select **Start a Consultation**, type the agent's name or contact URI into the text box, and select **Initialize a Voice Consultation** from the Action menu. The voice consultation is established when the agent accepts the toast notification for the voice consultation. Your main conversation will be on hold. If you were on a video call when you request a voice consultation, your video will be stopped and the start/stop video button will be unavailable during the consultation.

During a voice consultation, the mute button is not displayed in the voice consultation window. However, you can use the Mute button from the main interaction to mute the conversation.

You can speak with the other agent before going back to the conversation with your customer.

Escalating to Video

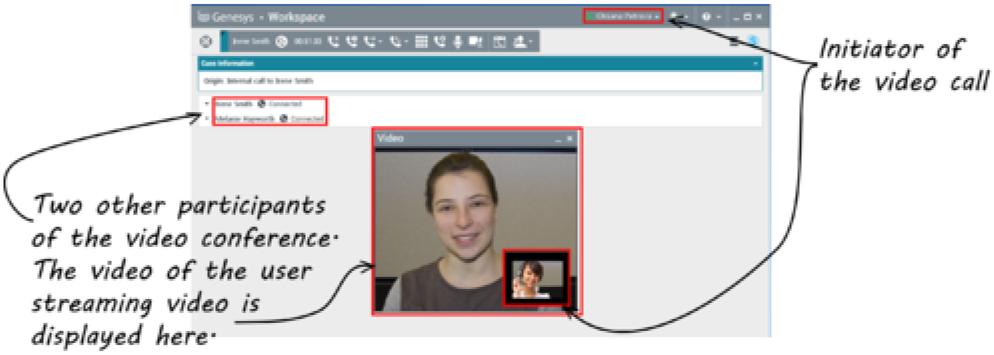
Your customer might need to escalate the conversation from voice to video or to de-escalate the conversation from video to voice. The customer uses their Skype client to initiate a voice call to you. You accept the call. Once you have accepted the call, the customer can escalate the voice call to video. You can add your own video to an existing video call if the customer has made a video call to the agent or has already added video to an existing call.

Video Interactions

When you are in a video call and require additional information, you have the following options

- Video Conferencing: You can add another agent to an existing video call.
- Video Transferring: You can transfer a video call to another agent.
- Video Consultation: You can pause a video call while you consult with another agent and, if necessary, later on do Transfer or Conference from this voice consultation.

Video Conferencing



Initiator of the video call

Two other participants of the video conference. The video of the user streaming video is displayed here.

You can add another agent to an existing video call. Select **Instant Call Conference**, and type the agent's name or contact URI into the text box. When you find the agent's name in the list, select **Instant Call Conference**, or click the icon next to the agent's name. The other agent receives a toast notification and can either accept or reject the invitation to a call. Now you can speak with all parties in the conference with video, if the invitation was accepted. All participants in the conference can see the video of the customer. Only one agent can display video to the customer. Other agents will not be able to display their video unless the first agent stops his video. When you are finished with the video conference, you can remove either yourself or the other agent from the video conference.

Video Transferring

You can transfer an existing video interaction to another destination (agent, queue, route point, etc). Select **Instant Call Transfer**, and type the agent's name or contact URI into the text box. You can also find the agent's name from the list of all agents. Select the Action menu or the icon next to the agent's name. The other agent receives a toast notification and can either accept or reject the invitation.

Video Consultation

While you are on a video call, you can request a consultation with another agent.

Select **Start a Consultation**, type the agent's name or contact URI into the text box, and select **Start Voice Consultation** from the **Action** menu. A toast notification is displayed on the selected user site. Note that the consultation is voice only; video consultation is not available.

You can speak with the other agent before going back to the video call.

Note that while you are consulting with the other agent, the video is temporarily unavailable, even if the video call is `On Hold` or `Connected`. You can resume streaming after you end the consultation by pressing the **Start video** button.

Handling IM Transcripts

Starting with release 8.5.000.68, Workspace Plugin supports the storage of incoming and outgoing Instant Messaging (IM) content through the Workspace Desktop Edition (WDE) in the Universal Contact Server (UCS) database when WDE is connected to UCS.

The plug-in will create only one entry in the contact history per call (for voice calls, WDE itself creates a separate entry for each agent). Transferred and conference IM calls create a single UCS interaction record.

The IM content is saved in chunks whenever an agent party ends. So, the whole context will be available in the contact history after all agent's parties have released. However, some chunks of the transcript may be available during the call.

For more information about UCS, see UCS Administration. For more information about WDE connection to UCS, see Configuring the Workspace Application Object.

Disposition Code

The Disposition Code feature enables agents to specify outcomes for interactions that they are handling. Disposition Codes are handled as Business Attributes in Genesys Framework. The interaction disposition is part of the attached data for the interaction.

Agents select an item from the tree or click a radio button to specify the disposition of an interaction. This disposition becomes part of the attached data of the interaction.

For more information, see Enabling the Disposition Code feature.

Limitations

Consultation IM calls are not supported.

Supported Features

T-Server for Skype for Business supports the following features:

- Alternate Routing
- Call Monitoring
- Call Supervision
- Emulated Agents
- Emulated Ringing
- Handling Direct Calls
- Hiding Sensitive Data in Logs
- No-Answer Supervision
- Presence
- Remote Recording
- Remote Treatments
- Transport Layer Security
- UTF-8 Encoding

See also Supported Media Types and Supported Media Escalations.

Alternate Routing

The main call delivery mechanism in T-Server for Skype for Business is routing from a Routing Point to an endpoint. T-Server supports internal mechanisms to handle call delivery failures, such as:

- Alternate Routing when no registered Routing Application present
- Alternate Routing for unresponsive Universal Routing Server (URS)
- Routing Delivery Supervision (No call delivery after a routing instruction is applied on the UCMA level)

Under those error conditions, the Connector will apply rules as defined in the feature configuration. When there are no Routing applications registered on the Routing Point, or when URS does not supply a Routing or Treatment instruction within the specified timeout, T-Server will send the call to the destination specified in the default-dn option. T-Server will stop redirections after the limit specified by the default-redirection-limit option is reached to avoid a redirection loop.

If a routing destination does not accept the call within the timeout specified by the option **no-answer-timeout**, EventError is reported. The call is released at the destination of routing to be routed again.

T-Server supports delivering calls to an alternative location in situations in which the Universal Routing Server (URS) becomes non-operational or unresponsive. T-Server sends the call to a specified alternate DN if no instructions from URS arrived within the time specified by the router-timeout option.

Note that the enabled Emulation Ringing feature does not affect Delivery Supervision. Only accept call on destination is considered as successful routing.

The configuration options **default-dn**, **default-redirection-limit**, **no-answer-timeout**, and **router-timeout** are configured in the **[TServer]** section of the Application object.

The configuration options **default-dn** and **router-timeout** can be configured on a particular Routing Point in the **[TServer]** section. The value configured on the Routing Point overrides the value configured on the Application object. An alternative routing parameter **no-answer-timeout** could be also extracted from AttibuteExtensions of TRouteCall. The attribute should have a string value, which defines the timeout interval in seconds. This value has the highest priority in the configuration hierarchy.

Call Monitoring

A direct (or 1pcc) call is a call which is initiated from Skype for Business, Workspace Desktop Edition, or from outside of enterprise directly to the agent. Without special effort such calls are not visible to T-Server. For a proper distribution of calls to the call center agent, it is important to understand what communications are in progress on the agent device.

To support this monitoring, T-Server and Workspace Desktop Edition implement the following:

- T-Server uses `Conversation-ID` to distinguish a Genesys monitored conversation from a non-monitored conversation. This is done by adding special symbols into `Conversation-ID` generated by T-Server. Currently, it is the word "Genesys" in `Conversation-ID`.

- For every Extension DN configured in the Switch object, T-Server subscribes to notifications on a corresponding Lync user endpoint. For monitoring of direct calls, T-Server enables handling of voice calls on this endpoint. When two instances of the endpoint exist in the Lync Server 2013 environment, it uses forking and delivers a call to both endpoints—the real agent phone and the endpoint defined in T-Server.

- When T-Server receives a call with "Non-Genesys" `Conversation-ID`, it answers the call on the secondary created user endpoint. Then it originates a new conversation toward a user with an indication in `Conversation-ID` that this is a "Genesys monitored" conversation.

- When a desktop application receives a new conversation, it checks whether this is a Genesys-monitored conversation. If this is not-monitored conversation, the desktop ignores it. Otherwise, it should be handled according to the application logic (see Emulated Ringing).

Call Supervision

Call supervision functionality is designed to enable contact center managers to monitor agent DNs, and it also enables agents to invite their supervisors to the call when dealing with a customer. T-Server supports the Standard Call Supervision architecture where supervisors and agents are located on the same site.

There are two types of call supervision that T-Server supports:

- *Subscription* monitoring enables supervisors to subscribe and monitor one agent DN. If the subscription is active, T-Server automatically invites the supervisor to all calls where the agent DN participates. T-Server stops working in this mode when the subscription is cancelled.
- *Assistance* monitoring is activated by an agent by issuing an assistance request sent to the supervisor. The agent can issue this while he or she is on a call with a customer.

Supervision Modes

Call supervision is performed in three different modes:

- *Silent monitoring* hides the supervisor’s presence from all call participants, including the monitored DN for the agent who is the target of the supervisor’s attention.
- *Whisper coaching* hides the supervisor’s presence from all call participants but the monitored agent. Only the agent can hear the supervisor.
- *Open supervisor presence* invites the supervisor to the call through subscription or assistance call supervision scenarios, but all call participants are aware of the supervisor’s presence and can hear the conversation.

The supervisor can choose any of these three modes for the call supervision subscription, but the agent can only use the last two modes for an assistance request.

Supervision Scopes

The call supervision scope specifies the time frame when the supervisor must participate in the call. There are two supervision scopes available:

- *Agent scope* allows the supervisor to monitor the agent. The supervisor joins the call when the call is established on the agent’s monitored DN. The supervisor leaves the call immediately after the agent leaves the call.
- *Call scope* allows the supervisor to control the customer’s experience. The supervisor joins the call when the call is established on the agent’s monitored DN, or when the supervisor receives the assistance request from the agent. T-Server keeps the supervisor as part of the call as long as either a customer or monitored agent remains in the call.

The supervisor can choose either of these scopes for the monitoring subscription.

An assistance request issued by the agent does not specify the supervision scope, so the scope always contains the call value. Therefore, if a supervisor is invited to a call through an assistance request, she will stay on the call until the call is finished.

Supervision Types

The call supervision type specifies the number of calls to be monitored—either one call or all calls.

- If *one call* is chosen for the subscription, the subscription is cancelled automatically when the supervisor finishes monitoring the first call on the monitored DN.
- If *all calls* is chosen for the subscription, the supervisor must cancel the subscription manually when he or she wants to stop monitoring the agent's calls.

The call supervision type cannot be specified for an assistance request. The *one call* type is always used when call supervision is initiated through an assistance request. The type cannot be changed through the configuration settings.

Monitoring Session

A monitoring session is the process in which a supervisor listens to an agent customer conversation. There are two types of monitoring sessions that are defined by the session creation scenario:

- A *subscription session* is created by T-Server automatically when a call is delivered to an agent's DN using the existing call supervision subscription.
- An *assistance session* is created as a result of the assistance request sent by an agent to a supervisor.

A monitoring session of any type must be initialized with the following three parameters when it is created:

- Supervision type
- Supervision mode
- Supervision scope

These parameters in the subscription session are initialized with the values of the corresponding parameters in the subscription from which this session was derived. An assistance session uses information passed in the assistance request and includes some configuration parameters for the initialization purpose.

A monitoring session begins when a supervisor joins a call, and ends when the supervisor disconnects from the call.

A call received by an agent can have monitoring sessions of both types, which are active at the same time. Each monitoring session is uniquely identified by the supervisor involved. As a result, the supervisor can participate in only one monitoring session at a time, but one agent can be part of multiple monitoring sessions where one of the sessions is subscription-based and other sessions are assistance request-based.

The following example demonstrates how multiple monitoring sessions are created in one call:

- Agent1 answers an incoming call and Supervisor1 is invited to the call based on the existing subscription.

- Agent1 sends an assistance request to Supervisor2 who also joins the call.

This call has two monitoring sessions active at the same time: the first session has a subscription type, and the second session is an assistance session.

Intrusion

Intrusion occurs when a supervisor activates a new call supervision subscription to monitor an agent who is currently on a call. T-Server creates the requested subscription and immediately invites the supervisor to join the existing call.

Note the specific T-Server behavior in the following scenario:

1. A supervisor selects Agent1 for monitoring.
2. An inbound call is routed to Agent2.
3. Agent2 transfers (two-step operation) the call to Agent1.
4. Agent1 answers and handles the call.
5. The supervisor is not notified about this call.

Monitoring Consultation Calls

T-Server supports the monitoring of consultation calls made to or from a DN under call supervision. This feature is disabled by default. To enable this feature, use the option monitor-consult-calls.

Switching Between Supervision Modes

A supervisor can switch between any supervision modes as follows:

- To switch from any mode to connect (or open supervision), the supervisor uses a TSetMuteOff request.
- To switch from any mode to mute, the supervisor uses a TSetMuteOn request.
- To switch from mute to coach, the supervisor uses a TSetMuteOff request with the MonitorMode=coach extension key.
- To switch from connect to coach, the supervisor uses a TSetMuteOn request with the MonitorMode= coach extension key.

When a supervisor changes the supervision mode using the TSetMuteOff or TSetMuteOn request, T-Server generates an EventMuteOn/EventMuteOff message with the MonitorMode key in AttributeExtensions to the supervisor and agent DNs, and all of subscribed T-Library clients.

Switching between supervision modes can be performed only during an established supervision call (with a supervisor present on the call), and from the same supervisor DN from which the TMonitorNextCall request was sent.

Support Notes:

- This feature is supported for Assistance Supervision, and for both monitoring scopes `agent` and `call`.
- This feature depends on support by specific versions of Workspace Desktop or a T-Library client. Consult

corresponding documentation for the availability of this new feature in those components.

To enable switching between supervision modes, set the *No results* option to `true`.

Call Supervision Configuration

Subscription

Call supervision subscription is controlled by two T-Library requests:

- TMonitorNextCall
- TCancelMonitoring

The supervisor’s desktop must be able to process these two requests to perform call supervision. The first request creates a new subscription, and the second request cancels the existing subscription. These requests use AttributeThisDN to identify the supervisor and AttributeOtherDN to identify the monitored agent DN.

Subscription Creation

T-Server creates a new subscription based on the TMonitorNextCall request from the supervisor. The request is either accepted or rejected.

T-Server rejects the request in the following scenarios:

- The supervisor or the monitored agent DN already has an active subscription.

However, if the TMonitorNextCall request tries to activate a monitoring subscription that is already active (for example, the supervisor who submitted this request is already set up to monitor the agent), T-Server responds with standard EventMonitoringNextCall messages sent to the agent and supervisor DNs. This request is not rejected, because it does not create multiple subscriptions on one DN.

- The supervisor or the agent DN is not configured in the Configuration Layer.

If the request is accepted, T-Server creates a new subscription and initializes it with the type, mode, and scope information that was defined in the request.

This information is part of the request as the following attributes:

- AttributeMonitorNextCallType, which defines the type of call supervision. Its possible values are MonitorOneCall and MonitorAllCalls.
- AttributeExtensions/MonitorMode, which defines the mode of call supervision. Its possible values are normal, mute, coach, and connect.
- AttributeExtensions/MonitorScope, which defines the scope of call supervision. Its possible values are call and agent.

If one or both of the monitoring extensions are missing or incorrect, the following values are used:

- default-monitor-scope for MonitorScope
- default-monitor-mode for MonitorMode

T-Server confirms the new subscription for both the supervisor and the agent by sending an EventMonitoringNextCall message to both destinations. This event always contains AttributeExtensions that include both monitoring extensions. These extensions represent the monitoring configuration for a new subscription.

Notes:

- T-Server identifies the agent to whom call supervision will be applied by the agent DN specified in the OtherDN attribute of the TMonitorNextCall request. The agent's login ID is not used for this purpose. In particular, this means that T-Server does not try to identify the agent who is logged in on the monitored DN, or to analyze the agent's state to decide if supervision should be activated for a call. T-Server monitors calls made to or from the specified DN, regardless of the person using this DN, until supervision scope expires.

Subscription Cancellation

T-Server can cancel active subscriptions using the following methods:

- Manual, where a supervisor submits a TCancelMonitoring request.
- Automatic, where T-Server cancels the subscription when a MonitorOneCall-type monitoring session is terminated.

A supervisor can submit a TCancelMonitoring request at any time. T-Server identifies a subscription by the pair of supervisor and agent DNs. If this subscription exists, then it will be cancelled. Otherwise, T-Server returns an EventError message.

T-Server generates EventMonitoringCancelled events for both the supervisor and the agent to inform them that the subscription was cancelled.

Assistance Request

An assistance request is a TSingleStepConference request containing the AssistMode parameter in the extensions. T-Server creates a new monitoring session based on the assistance request, but a monitoring subscription is not created. The AssistMode extension is identical to the MonitorMode extension used in the TMonitorNextCall request. The difference is that AssistMode can contain only the connect and coach values. There are no parameters to define the scope and type of monitoring in an assistance request, so the following monitoring parameters are used:

- MonitorScope set to call
- MonitorType set to MonitorOneCall

These two settings are hard-coded and cannot be changed.

Supervisor Auto-release

Depending on the type of monitoring scope and mode, T-Server determines whether to release a supervisor from the call. If the monitoring scope is agent, T-Server releases the supervisor from the call at the same time that the monitored agent leaves the call. If the monitoring scope is call and the other party of the call is aware of the supervisor’s presence on the call and can hear this supervisor, T-Server does not release the supervisor from the call.

Hiding Supervisor Presence

A supervisor who is performing silent monitoring or whisper coaching must be hidden from other call participants. If the scenario involves whisper coaching, only the monitored agent (who can hear the supervisor) must be aware of his or her presence on the call.

Call participants receive information about other participants joining or leaving the call from the corresponding T-Library events distributed by T-Server. Supervisor presence is not shown to any new participant joining the call. The T-Library desktop applications used by call center employees must be able to process T-Library events and indicate recent changes in a call status. For example, they can show that new participant has just joined or left the call.

Hiding a supervisor’s presence means filtering out any events that inform other participants about the supervisor's activity. T-Server inserts specific information into the T-Library events that allow T-Library clients to decide if a particular event must be shown to the customer or it must be suppressed. T-Server makes modifications to the events if at least one monitoring session is active on a call. The following attributes support this functionality:

- AttributeCallState
- AttributeOtherDNRole
- AttributeThirdPartyDN
- AttributeThirdPartyDNRole

The details on how those attributes are modified are found in the Genesys Events and Models Reference

Configuration Options

The following T-Server Application-level options support call supervision functionality:

- cancel-monitor-on-disconnect
- default-monitor-mode
- default-monitor-scope
- intrusion-enabled
- monitor-internal-calls
- monitor-consult-calls

Feature Limitations

The following known limitations currently apply to call supervision:

- A supervisor participating in a monitoring session should not initiate a 1pcc or 3pcc call transfer or conference call because this can change either the supervisor's status in the conference call or the status of a new party added to the call because of the conference or transfer.
- If a supervisor is already engaged in a call when an agent DN that it is targeting joins a new call (which requires monitoring), T-Server does not invite the supervisor to monitor the new agent conversation. Even if the supervisor disconnects from its current call, the monitoring session for the new agent conversation will not start. T-Server will activate monitoring for the next call on the targeted DN. This limitation is applied to supervision initiated through subscription monitoring (MonitorMode) and does not apply to the assistance monitoring (AssistMode).
- Supervision is not supported for Instant Messaging (IM) calls.

Calling using Back-to-Back User Agent

Starting with release 8.5.001.63, T-Server for Skype for Business can dial a new destination using the Back-to-Back User Agent (B2BUA) method, where call switching and control is performed by Genesys components. This feature allows the provisioning of a configured Caller ID and the correct reporting of the origination party of ISCC calls. It also permits calls to be made to TEL URI destinations, Response Groups, and destinations with forwarded calls, none of which can be dialed directly by T-Server.

The use of B2BUA may adversely affect performance. Therefore, Genesys recommends that its configuration be limited to destinations matching a given dial plan or even to the level of individual calls.

Configuring Calling using B2BUA

To enable the B2BUA calling method, configure a DN of type Voice over IP Service with the **service-type** option set to `dialplan`, and assign this DN in the **calling-method-dialplan** option of the T-Server application. In the dialplan DN, configure dial-plan rules if required. If the destination matches the dial plan and **calling-method** = `b2b`, the destination will be called using the B2BUA method. To customize Caller ID information that is displayed on a destination party phone, use the **cpn** configuration option on the Application and/or DN levels.

The destination of a call dialed using B2BUA will be reported as the requested URI until the call is answered. At this point, the destination URI will be replaced with the actual URI of the answering party. This means, for example, that if the destination URI is a TEL URI of a Skype for Business user, then the TEL URI party will be replaced with a SIP URI party when the Skype for Business user answers. Further examples can be found in the call flow tables below.

Configuration Options

Application-level options:

- calling-method-dialplan
- cpn

DN-level options:

- dial-plan-rule-<n>
- calling-method
- cpn

Dial Plan Rule Examples

The dial-plan rules use the following metacharacters:

- { } (braces)—the start and end of the variable area of the pattern
- D—any single digit
- S—any single case-insensitive character
- # (pound)—any number of digits
- * (asterisk)—any number of any characters

Dial plan pattern	Description	Examples
+{DDDDDDDD}	Matches 8 digits with a '+' prefix	+12345678

+{69DDDDDD}
+69{DDDDDD}
	Matches 8 digits with a '+69' prefix	+69123456

+{DD812DDD}	Matches 8 digits with a '+' prefix and 812 in positions 4-6	+078129876; +008121234
{DD812#}	Matches a number with 812 in positions 3-5	
sip:{SSSS}@domain.com	Matches any SIP URI that belongs to domain.com with a user part containing exactly 4 characters	sip:andy@domain.com
sip:{SSSS}@{*}	Matches any SIP URI that contains exactly 4 characters in the user part	sip:andy@domain.com; sip:mike@domain01.uk.com
sip:{*}@domain02.uk.com	Matches the SIP URI of any user that belongs to domain02.uk.com	sip:123@domain02.uk.com; sip:alice321@domain02.uk.com;sip:987bob@domain02.uk sip:michael@domain02.uk.com
sip:{#}@domain02.uk.com	Matches any SIP URI that belongs to domain02.uk.com and contains only digits in the user part	sip:1234567@domain02.uk.com; sip:987@domain02.uk.com
tel:{#}	Matches any TEl URI that contains digits only	tel:012345; tel:987
tel:+{#}	Matches any TEl URI that with a '+' prefix followed by digits only	tel:+012345; tel:+987

sip:SSS{SSSS}@domain.com	Matches any SIP URI that belongs to domain.com and has a user part containing 'SSS' and 4 additional characters	sip:SSSabcd@domain.com;
		sip:sssdcba@domain.com;

sip:SSS{DDDD}@domain.com	Matches any SIP URI that belongs to domain.com and has a user part containing 'SSS' followed by 4 digits	sip:SSS1234@domain.com;
		sip:sss4321@domain.com;

AttributeExtensions

Key: **calling-method**
Values: `b2b, dialout`
Description: To provide B2BUA ability for the following requests:

- TMakeCall
- TRouteCall
- TSingleStepConference

- TSingleStepTransfer
- TInitiateConference
- TInitiateTransfer

Providing an Extension key with value b2b in one of the above T-Library requests ensures that the call is made using B2BUA regardless of any dial plan. In addition, EventRinging generated by T-Server for a destination that is called by the B2BUA method will contain the same key-value pair in AttributeExtensions.

Providing the Extension key with value `dialout` in one of the above T-Library requests ensures that the call is dialed out directly regardless of any dial plan.

Key: **CPNDigits**
Value: A valid SIP URI
Description: To provide caller ID information to the destination of the B2BUA call in the following requests:

- TMakeCall
- TRouteCall
- TSingleStepConference
- TSingleStepTransfer
- TInitiateConference
- TInitiateTransfer

Providing this Extension key in any of the above T-Library requests in a B2BUA call overrides any value configured in the T-Server option cpn.

Event Flow Diagrams for Typical Destinations

Event flow in scenario "User A makes a call to User B’s Tel URI"

A	B SIP URI
Make Call to B’s Tel URI	
EventDialing	
EventNetworkReached	
	Answer Call
	EventRinging
Established	Established

PARTY A	PARTY B
Make Call to B's Tel URI (TMakeCall)	
EventDialing	

PARTY A	PARTY B
ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B Tel URI** OtherDNRole **Destination** CallState **Ok**	
EventNetworkReached ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B Tel URI** OtherDNRole **Destination** CallState **Ok**	
	Answer Call
	EventRinging ConnID **1** ThisDN **B SIP URI** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Forwarded**
EventEstablished ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B SIP URI** OtherDNRole **Destination** CallState **Ok**	**EventEstablished** ConnID **1** ThisDN **B SIP URI** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Ok**

Event flow in scenario "User B has forwarded calls to User C, User A makes a call to User B"

A	B	C
Make Call to B		
EventDialing		
	EventRinging	
		Answer Call
	EventReleased	EventRinging
EventEstablished		EventEstablished

PARTY A	PARTY B	PARTY C
Make Call to B's Tel URI (TMakeCall)		
EventDialing ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B**		

PARTY A	PARTY B	PARTY C
OtherDNRole **Destination** CallState **Ok**		
	EventRinging ConnID **1** ThisDN **B** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Ok**	
		Answer Call
	EventReleased ConnID **1** ThisDN **B** ThisDNRole **Destination** ThirdPartyDN **C** ThirdPartyDNRole **DeletedBy** CallState **Forwarded**	**EventRinging** ConnID **1** ThisDN **C** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Forwarded**
EventEstablished ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **C** OtherDNRole **Destination** CallState **Ok**		**EventEstablished** ConnID **1** ThisDN **C** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Ok**

Event flow in scenario "User A makes a call to Response Group B, the call delivered to Response Group Member C"

A	B	C
Make Call to B		
EventDialing		
	EventRinging	
EventEstablished	EventEstablished	
		SfB Client Accept Call
		EventRinging
EventPartyAdded	EventPartyAdded	
		EventEstablished
	EventReleased	
EventPartyDeleted		EventPartyDeleted

PARTY A	PARTY B	PARTY C
Make Call to B (TMakeCall)		
EventDialing		

PARTY A	PARTY B	PARTY C
ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B** OtherDNRole **Destination** CallState **Ok**		
	EventRinging ConnID **1** ThisDN **B** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Ok**	
EventEstablished ConnID **1** ThisDN **A** ThisDNRole **Origination** OtherDN **B** OtherDNRole **Destination** CallState **Ok**	**EventEstablished** ConnID **1** ThisDN **B** ThisDNRole **Destination** OtherDN **A** OtherDNRole **Origination** CallState **Ok**	
		SfB Client Accept Call
		EventRinging ConnID **1** ThisDN **B** ThisDNRole **ConfMember** CallState **Ok**
EventPartyAdded ConnID **1** ThisDN **A** ThisDNRole **ConfMember** OtherDN **C** OtherDNRole **NewParty** ThirdPartyDN **B** ThirdPartyDNRole **AddedBy** CallState **Conferenced**	**EventPartyAdded** ConnID **1** ThisDN **B** ThisDNRole **ConfMember** OtherDN **C** OtherDNRole **NewParty** ThirdPartyDN **B** ThirdPartyDNRole **AddedBy** CallState **Conferenced**	
		EventEstablished ConnID **1** ThisDN **C** ThisDNRole **ConfMember** CallState **Conferenced**
	EventReleased ConnID **1** ThisDN **B** ThisDNRole **ConfMember** CallState **Ok**	
EventPartyDeleted ConnID **1** ThisDN **A**		**EventPartyDeleted** ConnID **1** ThisDN **C**

PARTY A	PARTY B	PARTY C
ThisDNRole **ConfMember** OtherDN **B** OtherDNRole **Deleted** ThirdPartyDN **B** ThirdPartyDNRole **DeletedBy** CallState **Ok**		ThisDNRole **ConfMember** OtherDN **B** OtherDNRole **Deleted** ThirdPartyDN **B** ThirdPartyDNRole **DeletedBy** CallState **Ok**

Feature Limitations

- The B2BUA method cannot be applied to direct 1pcc calls to agents. That is, if an agent has forwarding or simultaneous ringing configured, an incoming direct call to that agent cannot be answered and will be immediately cleared.
- The B2BUA method cannot be applied to 1pcc Single-Step Conference that is performed from a Skype for Business Client.
- The B2BUA method cannot be applied to an established originator leg during a TMakeCall request.
- The B2BUA method cannot be applied to any Call Supervision or Supervisor Assistance scenarios.
- This feature does not affect Remote Treatments and Remote Recording functionalities.
- If an agent using Workspace Desktop in suppression mode receives a forwarded call, there is no toast for this call to the agent. Therefore, Genesys does not recommend that you use B2BUA calls in an environment where agents are using Workspace Desktop in suppression mode.

Response Groups Limitations

- If CPN Digits are used for a B2BUA call to a Response Group that contains DNs handled by Genesys components, the call cannot be answered by a Response Group member agent.
- If CPN Digits are used for a B2BUA call to a Response Group that contains Skype for Business users not handled by Genesys components, the CPN Digits are displayed in the ringing toast, but the CPN Digits are replaced in the Skype for Business conversation window with the conference service portal name after the call is answered.
- The B2BUA feature is available only for Response Groups where either all the users are monitored by Genesys, or all the users are not monitored by Genesys. The Response Group members cannot be a mixture of users monitored by Genesys components and users not monitored by Genesys components.

Conference Resource Pools

Internally, the UCMA Connector for Skype for Business uses Skype for Business conference resources to manage each call, the creation of which is a resource intensive procedure. Therefore, the Connector does not delete these conference resources after each call is completed, but it will reuse them for subsequent calls until they are expired by Skype for Business (typically, in the region of 8 hours).

To improve performance and to ensure that conference resources are always available, the Connector can be configured to create and maintain a pool of ready conference resources at startup time. This will increase the time taken for the startup phase but it will guarantee that there are conference resources available for call handling, starting from the very first call.

To enable this feature, it is necessary to create a pool of Trusted Application Endpoints (TAE) in Skype for Business that will be used by the Connector to manage these pre-created conferences.

Conference Pool Management

To enable the Conference Pooling feature, follow these steps:

1. Create a pool of Trusted Application Endpoints (TAE) in Skype for Business as described in Creating Trusted Application Endpoints for Conference Pooling.
2. Set the conference-pool-size option to define the number of conference resources to be created in advance.

Calculating Resources for Conference Pooling

Use the following guidelines to calculate the recommended number of TAE that must be created in Skype for Business and the number of conferences that each Connector should create in advance. To do this, we need the following 3 factors:

1. Identify the maximum number of simultaneous calls that is expected to be handled by the system (maxCalls)
2. How many Connectors will be deployed (numConn)
3. The number of Connectors that may be stopped at any time (numStopped)

Guideline value of option conference-pool-size

The guideline value of the **conference-pool-size** option can be calculated as follows:

```
conference-pool-size = 1.2 * maxCalls / (numConn - numStopped )
```

For example:

- There are 3 Connectors of which 1 may be stopped at any time

- The maximum number of calls expected to be handled by the system is 100

In this case, 100 / (3 - 1) = 50. Adding 20% means the recommended **conference-pool-size** = `60`. This means that under normal conditions when all 3 Connectors are operational, there will be 180 pre-created conferences in the system.

Guideline number of Trusted Applications

The number of required TAEs is related to the value of the **conference-pool-size** option. When creating conferences, the Connector will spread them among the number of available TAEs. As a guideline, it is recommended that at least 10 pre-created conferences should be available per TAE.

```
Number of Trusted Application Endpoints = conference-pool-size / 10
```

If the number of conferences per Trusted Application Endpoint is less than 10, there might be delays experienced during conference allocation when call volumes are high.

The number of conferences per TAE can be increased, but the consequences of a TAE failure should be considered. In this case, it will take a little time for the Connector to redistribute the required conference resources to the remaining TAEs, meaning that the total number of conferences might fall below the minimum required value for a short period of time.

Creating Trusted Application Endpoints for Conference Pooling

The Connector uses **uri-pattern** matching to identify a sequence of Trusted Application Endpoints that will be used for conference pooling. Therefore, these should be created in Skype for Business using a sequential naming pattern and defined in the Connector using the uri-pattern and count options set on the Switch object.

For example, if `uri-pattern=sip:conf{DD}@skype.lab` and `count=99`, then you must create 99 endpoints with names from `sip:conf01@skype.lab` to `sip:conf99@skype.lab` in Skype for Business, where numbers from 01-99 are endpoint numbers.

Managing Outbound CLI

The Connector will use these resources to initiate outbound calls from the contact center. It is not possible to determine which one will be chosen for each call, so it is advised to consider what CLID will be presented to the call destination. To do this, you must configure the following:

1. All Conference Service Application Endpoints must have a LineURI defined in the Skype For Business configuration.
2. A Calling Number Translation Rule must exist in Skype for Business to transform the Conference Resource LineURI to the desired CLID for outbound calls.

For example:

- The CLID for outbound calls should be 16504661100, which would correspond to the main Routing Point for incoming calls in the contact center.
- Three Conference Resources are configured: Conf1, Conf2, and Conf3.
- The following LineURIs for the Conference Resources are defined:

- Conf1: LineURI=tel:16504669999;ext=01
- Conf2: LineURI=tel:16504669999;ext=02
- Conf3: LineURI=tel:16504669999;ext=03

In Skype for Business, define a Calling Number Translation Rule to transform ^16504669999$ into 16504661100 and add this to the Calling Number Translation Rules for all outbound trunks. The ext part of the LineURI will be ignored by the Translation Rule. Now all outbound calls that originate from the Conference Resources will arrive at the customer with the required dialable CLID 16504661100.

Disable Lobby Bypass

Description

It is possible to enable Skype for Business to use a lobby functionality. Enabling this feature in Skype for Business will result in callers being placed into a lobby rather than being directly admitted to a conference. The callers then need to be invited into the conference. This functionality is set on a Skype for Business Pool, and when configuring a new Pool by default the lobby feature is not enabled, meaning that callers will bypass the lobby and be directly admitted to a conference.

Background

Conferences are scheduled by the Skype for Business T-Server and are used to maintain Genesys call control. When scheduling conferences, the Skype T-Server specifies a LobbyBypass flag that automatically allows all callers to bypass a lobby and be directly admitted to a conference. However, this will cause issues when using the Skype for Business T-Server with a Skype for Business Pool that does not have lobby bypass enabled. Essentially, the Pool is configured to have callers wait in the lobby while T-Server is trying to pass a flag that allows callers to bypass the lobby. In order to prevent such issues a new option is introduced in the Skype for Business T-Server that will make it aware of whether a Pool is configured to use a lobby or has lobby bypass enabled.

Skype T-Server Configuration Options

Sections and options in this chapter are defined in the **Annex** tab of the **Switch** object of T-Server.

lobby-bypass-enabled

Section: conference-services
Default Value: True
Valid Values: true, false
Changes Take Effect: For next scheduled conference
Introduced: 8.5.001.67
Related Feature: Disable Lobby Bypass

Specifies whether the UCMA Connector enables a flag, lobby bypass, used for implementation of call control when scheduling conferences. When set to `true`, conferences created by the Connector allow participants to bypass a virtual lobby when joining private meetings. When set to `false`, conferences created by the Connector allow participants to join private meetings only through a virtual lobby.

PBX Configuration

The option that enables lobby bypass on a Skype for Business Pool is called **PstnCallersBypassLobby**, and this option is set in the Meeting Configuration. For more details please see:

- https://docs.microsoft.com/en-us/skypeforbusiness/manage/conferencing/meeting-configuration-settings

Limitations and constraints

The Skype T-Server will not be able to schedule conferences for new calls if the settings in Skype for Business and Skype T-Server configuration are inconsistent.

Emulated Agents

T-Server performs agent emulation providing a fully functional agent model that enables full agent support for T-Server desktop applications as well as for other Genesys solutions. All calls are considered as business calls.

T-Server emulates the following functionality:

- Login and logout
- Agent set Ready
- Agent set Not Ready (using various work modes)
- Automatic after-call work
- After call work in idle

Emulated Agent Login/Logout

You can configure T-Server to perform emulated login either always, never, or on a per-request basis. Use the following T-Server configuration options to configure emulated agent login:
emulated-login-state
agent-strict-id
agent-emu-login-on-call

Agent Logout on Client Unregistering from DN

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

When a client desktop or application disconnects from T-Server while an agent is still logged in, the 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).

This feature is enabled/disabled by the following configuration options:
logout-on-disconnect
logout-on-out-of-service

Automatic Agent Logout

T-Server can automatically log out an agent after a specified period of inactivity, ensuring accurate reporting of agent activity. The following options control the feature:

auto-logout-timeout
auto-logout-ready

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 mode 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

T-Server can apply emulated wrap-up (ACW) for agents after a call is released, unless the agent is still involved in another call.

Timed and Untimed ACW

T-Server applies emulated ACW for an agent after any 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, using the extension WrapUpTime. It is not indicated in EventRinging, because the value may change between call ringing and 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 EventAgentNotReady with workmode = 3 (AgentAfterCallWork), and it indicates the amount of ACW it will apply using the extension WrapUpTime.

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

Emulated ACW Period

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

ACW in Idle

An agent can activate wrap-up time on request when idle, by issuing a TAgentNotReady request with workmode = 3 (AgentAfterCallWork). You can configure this feature using the following options:
timed-acw-in-idle
acw-in-idle-force-ready

Extending ACW

An agent can request an extension to the amount of emulated ACW for a call while in emulated ACW.

The agent requests an extension to ACW by sending RequestAgentNotReady with workmode = 3

(AgentAfterCallWork). T-Server determines the period of the extended ACW from the extension WrapUpTime, as follows:

- Value = `0`—There is no change to the 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 EventAgentNotReady with workmode = 3 (AgentAfterCallWork), reporting the newly extended amount of ACW using the extension WrapUpTime.

Emulated Ringing

Microsoft Lync UCMA does not provide the notification about the transition of an endpoint into alerting state. So, straightforward UCMA approach does not allow notifying T-Client and providing corresponding attached data, when a call is delivered to the agent endpoint.

To address this issue, T-Server emulates EventRinging as soon as an invitation for a new conversation is sent to an agent. Emulation creates a race condition, between alerting phone and EventRinging on the desktop.

To resolve the race condition, the desktop application implements the following logic:

- If EventRinging arrives first at the desktop:
  - Stores value `Conversation-ID` from the AttributeExtensions of EventRinging.
  - Waits for a new conversation with `Conversation-ID` matching the `Conversation-ID` extension key in EventRinging.
  - Shows toast (screen pop) with call attributes and user data attached when a call reaches the destination.
- If a call arrives first at the desktop:
  - If this conversation should be handled (for example, as defined in "monitoring of direct calls"), the desktop stores the `Conversion-ID` in its memory.
  - Waits for EventRinging with `Conversation-ID` in the AttributeExtensions matching the `Conversation-ID` of a new Lync conversation.
  - When arrived, shows toast (screen pop) with attached data.

Handling Direct Calls

Direct calls are calls that are dialed directly to DNs, without being initiated from T-Server or passing through a Routing Point. To provide CTI support for direct calls, T-Server uses Skype for Business call forking functionality. On startup, T-Server requests a Connector to subscribe to all registered users and create endpoints for each of them. When a call arrives at a registered user, Skype for Business Server forks the call to all users' endpoints, including the Connector's endpoint. T-Server delivers the conversation ID of the forked call to Workspace Desktop in AttributeExtensions of EventRinging. The Workspace Plugin ignores inbound calls without appropriate conversation IDs and answers that call leg passed via Connector.

For calls initiated directly from the Skype for Business client, this entails a number of sometimes undesirable consequences, such as:

- Double toasts
- Blocked application sharing
- Direct calls appearing as conference
- Calls appearing to come from internal T-Server resources rather than the actual caller
- Exchange server could report rejected forked call legs as missed calls

To avoid such artifacts at times when a user is not logged in as a Genesys agent or is logged in but also uses a Skype for Business client window running in parallel mode, starting with version 8.5.001.23, T-Server provides the ability to configure how direct internal or inbound calls are handled. This feature enables users who use Workspace rarely or not at all to disable direct call handling at one of the following levels:

- On agent logout
- According to DN configuration

T-Server can be configured to take no action if:

- A destination DN is configured accordingly
- A destination has no logged-in agent

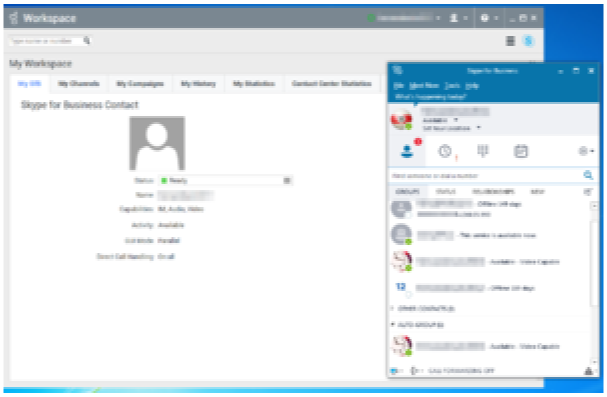
The following scenarios are processed and reported in the usual way:

- A call that passes through a Routing Point
- A call initiated using 3pcc by a Workspace Desktop agent

Using parallel and suppressed modes

Since the handling of direct calls by Genesys might cause undesirable effects on a Skype for Business client GUI when the Workspace plugin is running in a incompatible mode, the plugin can be configured to override the setting of handle-direct-calls in T-Server when it is started with a Skype for

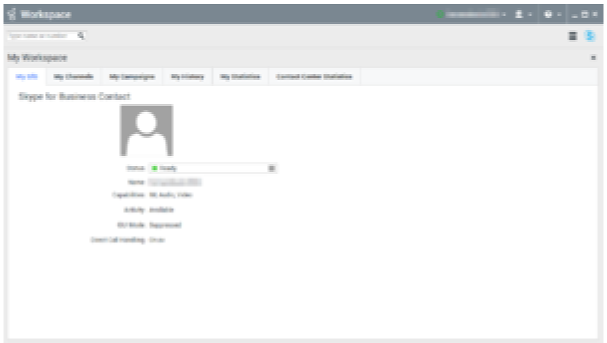
Business client in parallel mode. The required minimum versions are 8.5.001.65 for T-Server and 8.5.001.01 for the Workspace Plugin.



Status: Ready
Capabilities: IM, Audio, Video
Activity: Available
SfB Mode: Parallel

Parallel mode

In order for the Workspace Plugin to force T-Server to disable the handling of direct calls for its DN, the Workspace configuration option **interaction-workspace/lync.notify-startup-mode** must be set to `true`. In this case, the Workspace Plugin analyzes information about the handle-direct-calls setting received from T-Server at the time of registration and, if it detects that it is running with a Skype for Business client in parallel mode and the T-Server setting is other than `false`, it sends a request to T-Server to override its configuration option setting.



Status: Ready
Capabilities: IM, Audio, Video
Activity: Available
SfB Mode: Suppressed

Suppressed mode

Affects pre-8.5.001.65 only—When the Workspace Plugin uses a Skype for Business client in suppressed mode, it does not override the T-Server setting for **handle-direct-calls**. In this case, if **handle-direct-calls** is set to `false`, any incoming direct call can neither be answered nor rejected by the agent, but the agent can hear its alerting sound. Such a combination of settings should only be used in call centers where the business model excludes direct calls to agents.

From release 8.5.001.65—When the Workspace Plugin uses a Skype for Business client in suppressed mode, it overrides a `false` setting for **handle-direct-calls** in T-Server. You can also specify the media of the direct calls you want to handle by defining the new handle-direct-calls-media option. You can choose to handle audio/video (`av`), instant messaging (`im`) or all.

Notes on handle-direct-calls-media

- **handle-direct-calls-media** can be set on the Application and the device level.
- The plug-in also locks the mode of **handle-direct-calls-media** by the same request that locks **handle-**

direct-calls.

- An overridden direct call handling setting persists as long as WDE is connected to T-Server.

Presence Processing

If direct call handling is disabled for an agent, T-Server maps presence information to DND status and reports it for that agent. T-Server reads presence mapping if it is configured for the DN or for an agent in the appropriate profile. If the presence profile is not configured for an agent, T-Server uses the default availability range configured at the Application level by the default-availability-range option in the **[TServer]** section.

Because presence mapping and presence pushing are incompatible features, T-Server disables presence pushing for all DNs where direct call handling is disabled. Do not configure presence pushing in the presence profiles of these DNs.

Configuring direct call handling

In the T-Server for Skype for Business application, configure the following options:

- handle-direct-calls
- handle-direct-calls-media (from release 8.5.001.65)
- default-availability-range

To enable the feature for a particular DN, specify the handle-direct-calls option for that DN. The DN-level setting takes precedence over the Application-level setting.

Feature Limitations

- Skype for Business call statistics differ significantly from Genesys reporting for DNs that operate in non-suppression mode. Genesys does not monitor some direct calls.
- T-Server does not support side-by-side Skype for Business client configuration because of several deficiencies identified in Skype for Business clients while working with multiple audio/video devices.
- For calls routed to a destination with disabled direct call handling, alternate routing in case of no answer is disabled.

Handling Pass-Through Calls

There are several situations in which a call can end up in a configuration where there are no longer any T-Server controlled participants involved, and therefore the call is no longer visible to Genesys and is also no longer under CTI control. Starting with release 8.5.001.32, by using the **allow-pass-through-calls** option, T-Server can be configured to monitor situations such as these and, if possible, prevent them.

There are two main scenarios that could transform a call under Genesys CTI control to a call that Genesys CTI cannot access:

- The last Genesys CTI-controlled participant (Agent) leaves a conference session with three or more parties.
- Genesys CTI-controlled participant (Agent) performs a transfer or routing operation that leads to creating a call topology that does not have Genesys CTI control.

A call is considered to be *not controlled by Genesys CTI* when the participants in the call are external. This means that the participants are not in the list of DNs configured for this T-Server. When T-Server is configured to not allow pass-through calls, T-Server for Skype for Business will validate the call topology after handling CTI events that may have changed the call configuration. If T-Server finds that the call can no longer be controlled by CTI, it will release the call.

T-Server will also reject any CTI request that would create a call topology that does not remain under CTI control, and displays error messages as follows:

- For RequestCompleteTransfer, error 98: `Cannot Complete Transfer`
- For RequestSingleStepTransfer, error 1148: `Privilege violation on called device`
- For RequestRouteCall, error 705: `Prohibited Route Call To External`

ISCC calls

When T-Server is operating in an environment where it is connected to SIP Server using Inter-Server Call Control (ISCC), T-Server can be configured to continue handling multi-site calls to DNs controlled by SIP Server, even if no locally monitored participants stay in the call. The `iscc` value of the **allow-pass-through-calls** option enables this behavior.

Configuring Pass-Through Calls Handling

In the T-Server for Skype for Business application, configure the allow-pass-through-calls option at the Application level.

To enable the feature for a particular DN, specify the allow-pass-through-calls option for that DN. The DN-level setting takes precedence over the Application-level setting.

Feature Limitations

T-Server cannot distinguish between external users behind the SIP trunk and unmonitored internal Skype for Business users. These users are counted as external call participants.

Hiding Sensitive Data

T-Server and Connector for Skype for Business components can print customer sensitive information in log files in:

- CTI link messages (both components)
- T-Library messaging (T-Server component)
- Specific debug information added for troubleshooting

The sensitive content includes:

- User Data in T-Events
- Content of Collected Digits
- Instant messages
- Treatment prompts

T-Library messaging

The option that controls whether potentially sensitive data is printed in the T-Server log file is hide-sensitive-data, which is configured in the **[TServer]** section of the T-Server Application. The default value of this option is `true`, meaning that the following sensitive data will be hidden in the T-Server log file:

- AttributeCollectedDigits, AttributeLastDigit, AttributeDTMFDigits, AttributeTreatmentParms will be hidden in T-Library requests and events.
- The headers “Data” and “Treatment-Params” will be hidden in CTI link messages. Instead of printing the actual data transmitted between T-Server and Connector, the log file will contain a string: `**** (length:`*`nn`*`)`, where *nn* is the length of the original data.

This feature can be disabled by setting the option value to `false`.

CTI Message Headers

The CTI messages used by T-Server and Connector contain various Microsoft Lync TServer Protocol (MLTP) message headers. The Connector can be configured with a list of MLTP message headers that might contain potentially sensitive data and should not be printed in the log file. Instead of printing the actual data transmitted between T-Server and Connector, the log file will contain a string: `**** (length:`*`nn`*`)`, where *nn* is the length of the original data.

To hide message headers, in the Annex tab of the Switch configuration object, in the **[log]** section, set the **hide-header** option to a comma-separated list of MLTP message headers that must not be printed in the log file.

For example:

```
[mslync] handle MLTP message
PARTY_CREATED * MLTP/1.0
media: voice
from: sip:user1@domain.com
to: sip:user21@domain.com
party-state: ALERTING
```

If **hide-header**=`media,from,to,party-state`, the following would be printed instead in the log file:

```
[mslync] handle MLTP message
PARTY_CREATED * MLTP/1.0
media: **** (length:5)
from: **** (length:21)
to: **** (length:21)
party-state: **** (length:8)
```

IM Treatments

The following treatment types can be applied for IM calls (MediaType=5) on a Routing Point:

- TreatmentCollectDigits (6)
- TreatmentPlayAnnouncement (7)
- TreatmentPlayAnnouncementAndDigits (7)

AttributeTreatmentParams for treatments with types TreatmentPlayAnnouncement and TreatmentPlayAnnouncementAndDigits must contain the following values:

```
'PROMPT' (list) =
        '1' (list) =
                'TEXT'(string) = 'Here is treatment text'(string)
...
        'NN' (list) =
                'TEXT'(string) = 'Here is treatment text'(string)
```

AttributeTreatmentParams for treatments with types TreatmentCollectDigits and TreatmentPlayAnnouncementAndDigits could contain the following value:

```
'TOTAL_TIMEOUT'(string) = timeout (integer)
```

If the TOTAL_TIMEOUT parameter is set to 15, T-Server waits for a customer's input for 15 secs, and then a treatment will be finished with EventTreatmentEnd.

If TOTAL_TIMEOUT is not included, T-Server waits for a customer's input indefinitely.

For example, a treatment with AttributeTreatmentType = TreatmentPlayAnnouncementAndDigits(7) and following AttributeTreatmentParams:

```
'PROMPT' (list) =
'1' (list) =
                'TEXT' = 'What kind of help do you need?'
        '2' (list) =
                'TEXT' = 'We could show your account information or connect to Operator'
        '3' (list) =
                'TEXT' = 'What do you prefer?'
'TOTAL_TIMEOUT' = 15
```

will result in these messages in a customer's IM window:

- What kind of help do you need?
- We could show your account information or connect to Operator
- What do you prefer?

T-Server waits 15 secs for the customer's response.

IM Suppression

Currently routing and reporting is not able to operate correctly in a configuration where Skype for Business IM and Genesys eServices chat are handled by the same agents. To allow chat to be deployed for agents using Multimedia Connector for Skype for Business it is necessary to suppress T-Server reporting for IM interactions. IMs can then function normally, but without Genesys having any knowledge of IM events, which means that such events cannot be reported and IMs cannot be routed. Agents continue to be reachable by IM, but IM routing will not be handled by Genesys.

Availability

This feature requires:

- T-Server for Skype for Business version 8.5.001.65.
- Workspace Plugin for Skype for Busines 8.5.001.01.

T-Server configuration

A new configuration option enables/disables this feature:

im-reporting

Section: TServer
Default Value: default
Valid Values: default, disabled
Changes Take Effect: After restart

Specifies the type of reporting for IM calls in T-Server:

- `default`—T-Server will generate reporting for IM calls with Media Type=5 in Genesys T-Library events
- `disabled`—T-Server will suppress reporting for IM calls.

The value of option is read only on start-up.
If no value is present, the default value is assumed.
This value will be synchronized from the primary to the backup T-Server and the state of reporting will not be changed after an HA switchover.

T-Library extension

A new T-Library extension supports this feature:

- **Keyname**—im-reporting
- **Type**—string
- **Valid values**—`default, disabled`
- **Used in**—EventRegistered / EventAddressInfo for every device.
- **Description**—The value of the extension indicates the mode of IM reporting currently configured in T-Server.
    - `default`—T-Server reports Skype for Business IM calls in T-Library reporting as calls with AttributeMediaType = 5.
    - `disabled`—T-Server does not generate reporting for Skype for Business IM calls.

Workspace configuration

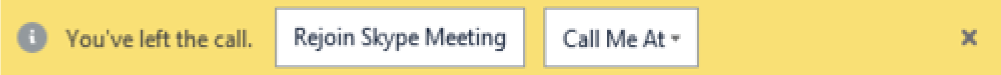
- The Workspace Plugin for Skype for Business must be configured in parallel mode for this feature to function correctly. If it is configured in suppression mode, the following error is generated:
  ```
  Current mode of GUI Suppression will result in IM message not seen by WDE GUI.
   Please reconfigure plugin to Parallel mode.
  ```
- If the T-Server option **lync.sfb-window-state** is set to:
    - `show`, the conversation window will always be shown, whether it contains voice only or voice+IM.
    - `hide`, this will hide any conversation containing voice only. If an Agent had a voice-only call whose conversation window was hidden, then the call was escalated to add IM, the conversation window will be unhidden and will show both voice+IM.
- The T-Server DN-level option **multimedia** must be set to `false` or deleted, otherwise the IM button will still be displayed in WDE but will not function correctly.

Workspace plugin behavior when IM suppression is enabled

- For IM calls, the Agent will need to accept a Skype toast.
- No WDE interactions will be shown or transcripts recorded by UCS.
- For any calls which began as voice then were escalated to IM, the Skype for Business client conversation window will be popped up. The Agent can exchange IM only via the Skype for Business client conversation window.

Constraints

- IM calls will have to be controlled manually on the Skype for Business client when IM suppression is enabled.
- WDE must be running in parallel mode to use IM suppression. If WDE is running in suppression mode with this feature enabled, the agent will not receive any IMs.
- If the Skype for Business client displays a **Rejoin Skype Meeting** banner, the options it offers must not be selected because the Agent might connect to a unrelated call.


You've left the call.

Music On Hold

The music-on-hold file is specified in the musicOnHoldFilePath option of the **connector** section.

The music is played by the Connector application directly to a main or consultation call when it is placed on hold. The music-on-hold file must be reachable and available for the Connector application.

In the environment with multiple Connectors, the music-on-hold file must be available for every Connector. Consider placing the file on a shared resource or mapped drive.

If the path to the music-on-hold file is not specified in musicOnHoldFilePath, no music-on-hold is played.

The music-on-hold can be recorded or excluded from the recording. See Remote Recording for details.

No-Answer Supervision

The No-Answer Supervision feature controls how to manage agent when call is not answered on a 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 a failure.

The no-answer-action option defines the action if a logged-in agent fails to answer a call within the defined timeout. The 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 Agent Login object
2. The **[TServer]** section of the Extension DN object
3. The **[TServer]** section of the T-Server Application object

The option no-answer-timeout defines the timeout (in seconds) that T-Server waits for a call ringing on a destination device to be answered. When the timeout expires, T-Server cancels dialing out and reports EventError with the error code TERR_DN_NO_ANSWER. A ringing party is removed/released from the routing destination and the call can be routed again.

The option no-answer-timeout is configured in the **[TServer]** section of the T-Server Application object.

The **no-answer-action** and **no-answer-timeout** option values could be overridden by the extension key NO_ANSWER_ACTION and NO_ANSWER_TIMEOUT, respectively, in the TRouteCall request. This method allows the no-answer behavior to be determined in a routing strategy.

Keep in mind that T-Server ignores a value of `0` (zero) for the NO_ANSWER_TIMEOUT extension key. You cannot turn off the functionality by the request, although you can specify a long timeout to minimize its effect.

Presence

Presence is used by Skype for Business to indicate the status of a user and their availability for communication. T-Server allows to configure a presence profile which will determine how it interacts with Skype for Business presence. There are 2 modes supported:

- Pull presence mode: T-Server reflects the presence status of a user provided by Skype for Business in Genesys DND device statuses.
- Push presence mode: T-Server updates the presence status of a Skype for Business user based on the Genesys status.

If presence propagation is activated, it is necessary to choose whether to use presence pushing or pulling as it is not possible to use both.

Skype for Business Presence Availability

Skype for Business Presence consists of Availability (a number in the range of 0 and 18000 inclusive) and an Activity string. The general description of Skype for Business Availability Value ranges is provided in the following table.

Availability	Value	Description
None	0	The availability is not set
Online	3000	Free
IdleOnline	4500	The User state is Online and the Device state is Away
Busy	6000	Busy
IdleBusy	7500	The User state is Busy and the Device state is Away
DoNotDisturb	9000	Do not disturb
BeRightBack	12000	Temporarily unalertable
Away	15000	Unalertable
Offline	18000	Unavailable

Configuring the Presence Profile

- **Create a VoIP Service DN under the Switch object:**
  The options used by T-Server for a Presence profile are configured in the **[TServer]** section of the Annex tab of a Voice Over IP (VoIP) Service DN. The **service-type** option of this VoIP Service DN must be set to `presence-profile`. You can create multiple VoIP Service DNs in order to create different

profiles but only one will be active at any time as configured using the T-Server option **presence-profile**.

- **Configure T-Server with details of the VoIP Service DN:**
  The presence-profile option determines which VoIP Service DN T-Server uses for a Presence profile. This option can be configured globally in the **[TServer]** section of the T-Server application; by device in the **[TServer]** section in the Annex tab of an Extension DN; or by a login session by providing the key `presence-profile` in the AttributeExtensions of RequestAgentLogin. By using this hierarchical option and creating multiple VoIP Service DNs, it is possible to create different profiles.

Now decide whether T-Server will use **Pull Presence Mode** or **Push Presence Mode**.

Pull Presence Mode

When T-Server receives a Presence update from Skype for Business, it can use the Availability Value attribute provided by Skype for Business, as shown in the Presence Availability table above, to map this Presence update into Genesys DND states. T-Server propagates the result to T-Library clients with EventDNDOn and EventDNDOff.

Additionally, the presence-availability-range option (in the presence profile) can be used to specify a range of the Availability Value attributes that T-Server will consider as the user being available and propagate EventDNDOff to T-Library clients. For example, a value of `3000-5999` would consider a user in Online or IdleOnline states as available and T-Server would propagate EventDNDOff on receiving an Availability Value from Skype for Business that was within this range. This option accepts comma-separated values, so several ranges can be configured that will be considered as Available by T-Server.

Configure the following options in the **[TServer]** section of the Annex tab of the VoIP Service DN:

- **service-type** = `presence-profile`
- map-presence-to-dnd=`true`
- presence-availability-range

Push Presence Mode

Presence publishing allows for Genesys agent and device states to be mapped to Skype for Business presence and pushed to Skype for Business. Presence publishing uses an XML file that defines a list of Genesys agent and device states that are mapped to Skype for Business presence Availability and Activity values. These values are pushed to Skype for Business and displayed on the Skype for Business user’s endpoint client. The agent state and device state can be combined into an aggregate state. For example, all states with a call present on the agent can be mapped to a state INCALL.

Configure the following options in the **[TServer]** section of the Annex tab of the VoIP Service DN:

- map-presence-to-dnd=`false`
- agent-presence-map
- aggregated-states

- **Provide details of aggregated states:**
  The aggregated states are configured in the aggregated-states option as a list of comma-separated values. The following table demonstrates the mapping of 15 Genesys states into aggregated states.

#	Agent State	T-Server Device State	Aggregated State ID
1	Logout	Idle	IDLE_OUT
2	Ready	Idle	IDLE_READY
3	NotReady	Idle	IDLE_NOTREADY
4	ACW	Idle	IDLE_ACW
5	Walk_Away	Idle	IDLE_AWAY
6	Logout	Busy	INCALL
7	Ready	Busy	INCALL
8	NotReady	Busy	INCALL
9	ACW	Busy	INCALL
10	Walk_Away	Busy	INCALL
11	Logout	OOS	OOS
12	Ready	OOS	OOS
13	NotReady	OOS	OOS
14	ACW	OOS	OOS
15	Walk_Away	OOS	OOS

For example, to set the option to reflect the example in the table above, the option would be set like this:

aggregated-states= `1=IDLE_OUT, 2=IDLE_READY, 3=IDLE_NOTREADY, 4=IDLE_ACW, 5=IDLE_AWAY, 6=INCALL, 7= INCALL, 8=INCALL, 9=INCALL,10=INCALL,11=OOS, 12=OOS, 13=OOS, 14=OOS, 15=OOS.`

- **Configure the XML file:**
  An XML file must be configured that contains an entry for each of the aggregated states configured in the aggregated-states option. The XML file contains details of what Skype for Business Availability and Activity are mapped to a particular aggregated state. This information will then be pushed to Skype for Business and displayed on the Skype for Business user’s client endpoint. The XML file must start with the following two lines:

```
<?xml version="1.0"?>
<agentStates xmlns="http://schemas.genesys.com/09/2014/mslyncteserver/agentStates">
```

And must end with the following line:

```
</agentStates>
```

To continue the example, when an agent is idle and ready (which is configured as `2=IDLE_READY` in the aggregated-states option example above) T-Server pushes an Available state to Skype for Business and displays an appropriate message in the Skype for Business user’s endpoint. The XML could contain an entry like this:

```
<?xml version="1.0"?>  <agentState ID="IDLE_READY" availability="3501">
    <activity LCID="1033">I am available</activity>
  </agentState>
```

If the agent is on a call, T-Server pushes a Busy state to Skype for Business with an appropriate message, the XML could contain an entry:

```
<?xml version="1.0"?> <agentState ID="INCALL" availability="7001">
    <activity LCID="1033"> Working with customer, do not disturb </activity>
</agentState>
```

The attributes LCID of the Activity element specifies the Microsoft Locale ID. If a contact center is deployed in a multilingual company, where agent desktops are configured for using their native languages, it is possible to publish presence according to locales used in the call center.

Following on from the INCALL example above, the multi-language entry could be:

```
<?xml version="1.0"?>
   <agentState ID="INCALL" availability="7001">
    <activity LCID="1033">Working with customer, do not disturb</activity>
     <activity LCID="3082">Trabajar con los clientes, no molestar</activity>
     <activity LCID="1049">Работа с клиентом, не беспокоить</activity>
     <activity LCID="1036">Travailler avec le client, ne pas déranger</activity>
  </agentState>
```

Using the example table from the Provide details of aggregated states section and the example values for the option aggregated-states above, the final XML file could look like this:

```
<?xml version="1.0"?>
<agentStates xmlns="http://schemas.genesys.com/09/2014/mslyncteserver/agentStates">
  <agentState ID="IDLE_OUT" availability="18000">
    <activity LCID="1033">Logged out</activity>
  </agentState>
  <agentState ID="IDLE_READY" availability="3501">
    <activity LCID="1033"> I am available </activity>
  </agentState>
  <agentState ID="IDLE_NOTREADY" availability="6001">
    <activity LCID="1033"> I am not available </activity>
  </agentState>
  <agentState ID="IDLE_ACW" availability="6001">
    <activity LCID="1033">I am in After Call Work, do not disturb me</activity>
  </agentState>
  <agentState ID="IDLE_AWAY" availability="4501">
    <activity LCID="1033">I am away from my desk</activity>
  </agentState>
  <agentState ID="INCALL" availability="7001">
    <activity LCID="1033">Working with customer, do not disturb</activity>
     <activity LCID="3082">Estoy trabajando con los clientes, no molestar</activity>
     <activity LCID="1049">Работа с клиентом, не беспокоить</activity>
     <activity LCID="1036">En travaillant avec les clients, ne pas déranger</activity>
  </agentState>
  <agentState ID="OOS" availability="18000">
    <activity LCID="1033">The device is out of service</activity>
  </agentState>
</agentStates>
```

- **Configure T-Server with location of XML file:**
  Once the XML has been configured and stored in a location accessible by T-Server then the agent-presence-map option must be configured with a value corresponding to the location of the XML file. For example: **agent-presence-map** = `C:\Genesys\Presence\<XML file name>.xml`. T-Server does not re-load the XML file after starting. Any changes made to a XML file will require a T-Server restart in order for the changes to take effect.

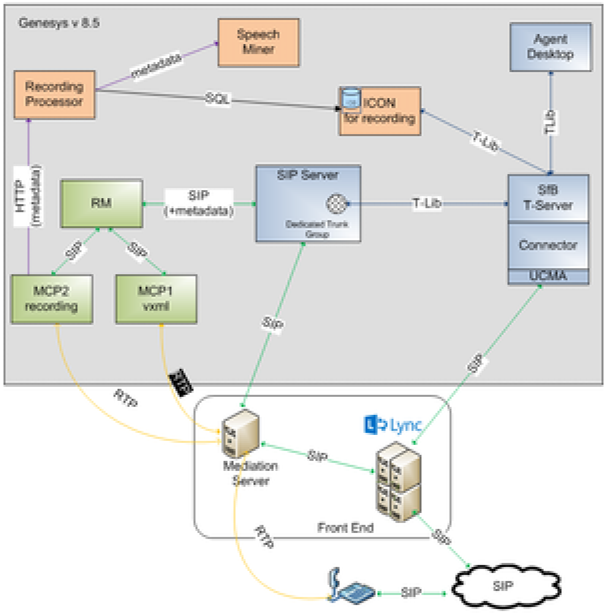
> ### Important
>
> Pushing presence to Skype for Business functionality and mapping Skype for Business presence into Genesys DND are incompatible. If you set **map-presence-to-dnd** to `true` in a profile, T-Server ignores the value of the **agent-presence-map** option for that profile.

Remote Recording

Starting with version 8.5.001.17, T-Server for Skype for Business supports remote recording of established calls using recording capabilities of SIP Server version 8.1.102.65 or later. Unlike SIP Server, T-Server always records a mixed voice stream that is not separated by parties. Call recording starts after a call is established. It does not result in any changes to the call itself, to event processing, or to any other generated TEvent.

When call recording is configured on T-Server, it creates an internal T-Library client that communicates with SIP Server and provides all required information about calls to be recorded. When recording is requested, T-Server initiates an additional leg to SIP Server on a dedicated resource. T-Server supports integration with the Genesys Interaction Recording solution. The figure shows the high-level architecture of a remote recording solution. It suggests that GVP utilize one MCP for recording and another MCP for call establishment.

Remote Recording



T-Server utilizes a preconfigured range of telephony numbers (called *recording ports*) on SIP Server for dialing purposes. When the recording leg arrives at SIP Server, SIP Server reports the recording port number as AttributeDNIS in T-Library messaging. T-Server uses the AttributeDNIS to match the original call in order to perform recording dynamically, propagate User Data updates, and control a recording progress. T-Server associates the internal recording port with each call while the call is on a Trunk Group (for an entire recording process). When T-Server stops recording and releases the recording leg, the recording port is freed up (and can be re-used for another call).

Recording ports in T-Server are configured as a pattern that consists of a <prefix>, digits, and a URI suffix. The <prefix> is a permanent prefix that enables to match a call and to configure a dial-plan rule on the SIP Server side.

T-Server performs and controls remote recording for an established party/call:

- Automatically if any participating DN is configured for mandatory recording (the DN-level **record** option)
- Based on the **record** key in AttributeExtensions in a TRouteCall request
- On demand at a client's request

Configuring remote recording

SIP Server and DNs

Configuring SIP Server and DNs

1. Configure the SIP Server application in accordance with Deploying SIP Server for GIR.
2. On the Connections tab of the SIP Server application object, add an ISCC connection to T-Server for Skype for Business.
3. Create a dedicated **Trunk Group** DN with the name set to **annc**. In the **[TServer]** section, configure the following configuration options:
    - **contact**—If a single instance of Resource Manager is deployed, set this option to `<Resource Manager IP address>:<Resource Manager port>`. Note that the IP address and port are separated by a colon.

      If Resource Manager is deployed in an Active-Active High-Availability cluster, set this option to `::msml`. For more information about a Resource Manager Active-Active High-Availability cluster, see the Framework 8.1 SIP Server Deployment Guide.
    - **sip-uri-params**=`play=music/silence`.
4. Create an inbound DN of type **Trunk**. In the **[TServer]** section, configure the following options:
    - **contact**—Specify the IP address of the Skype for Business Mediation Server. To use Secure Real-time Transport Protocol (SRTP), configure a _TLS SRV record to represent the Mediation Server Pool and use this for the trunk configuration as described the Framework 8.1 SIP Server Deployment Guide.
    - **sip-proxy-headers-enabled**=`false`.
5. Create an MSML DN of type **Voice over IP Service**. In the **[TServer]** section, configure the following options:
    - **contact**=`<Resource Manager host:port>`
    - **cpd-capability**=`mediaserver`
    - **make-call-rfc3725-flow**=`1`
    - **predictive-timerb-enabled**=`false`
    - **prefix**=`msml=`
    - **refer-enabled**=`false`
    - **ring-tone-on-make-call**=`false`

- **service-type**=`msml`
- **userdata-map-filter**= *
- **userdata-map-format**=`sip-headers-encoded`

6. Configure a dial plan to forward inbound calls from Skype for Business with a preconfigured destination prefix to the dedicated Trunk Group **annc** created in Step 3.

T-Server for Skype for Business

Configuring T-Server

1. On the Connections tab of the T-Server for Skype for Business application object, add an ISCC connection to SIP Server.
2. On the Options tab, create the **[remote-recording]** section and configure the following options in that section:
    - server-application = <The SIP Server Application name from the Connection tab>
    - trunk-group = <The name of the Trunk Group DN dedicated to a remote recording service that is configured on the Switch assigned to SIP Server>
    - uri-pattern = `[sip]:{<prefix>{DDDDDDD}}[@<urisuffix>]`
    - reestablish-recording-tout = set to 5 sec by default
    - recording-filename = <A pattern that is used to generate a filename for call recording>

Genesys Voice Platform

Configuring GVP

1. Configure GVP as described in Deploying Genesys Voice Platform for GIR.
2. Configure mono recording.

Full-time call recording

Enabling full-time call recording

To enable full-time call recording on an Extension or Routing Point DN, set the record configuration option in the **[TServer]** section.

Dynamic call recording

Enabling dynamic call recording

To enable dynamic call recording during an ongoing conversation, configure one of the following:

- In the routing strategy, configure the TRouteCall request to include the key **record**, with the values:
  - `destination`: recording continues until the destination of TRouteCall is present on the call.
  - `source`: recording continues until an originator is present on the call.
  - `disabled`: recording does not start even if the destination of TRouteCall has mandatory recording configured.
- In the T-Library client, configure the TPrivateService request to include the key **record**, with one of the values:
  - `source` for recording ThisDN
  - `destination` for recording OtherDN
- In the Workspace Desktop application, use recording control buttons.

To enable mid-call recording control during an established session, configure TPrivateService to include the key `AttrPrivateMsgID`, using one of the following values:

- GSIP_RECORD_START (3013)
- GSIP_RECORD_STOP (3014)
- GSIP_RECORD_PAUSE (3015)
- GSIP_RECORD_RESUME (3016)

Recording without music-on-hold

Enabling call recording without music-on-hold treatment

Starting with version 8.5.001.29, T-Server provides the ability to record a call without recording a music-on-hold treatment when a call is placed on hold. This functionality also applies to call transfers: the recording is paused when a transfer is initiated, and resumed when the transfer is completed.

When several agents are involved in a call and the call is placed on hold, T-Server pauses the recording at the first invocation of the hold operation and resumes the recording at the first invocation of the retrieve call operation.

To enable call recording without music-on-hold treatment, in the T-Server for Skype for Business application, set the record-moh option to `false` in the **[remote-recording]** section.

Skype for Business

Configuring Skype for Business

Configure outbound call routing settings to send calls to numbers with the specified <prefix> to the trunk configured for SIP Server in the Skype for Business Server Topology. See step 10 in the Deployment Summary section.

For Remote Recording, you must configure Dial Plan, Voice Policies, Voice Routes, and PSTN usage. See details at: https://technet.microsoft.com/en-us/library/gg398272(v=ocs.16).aspx.

> **Important**
>
> The Dial Plan configured for Skype for Business Server must not change the dialed number. That is, the dial plan must not change prefixes, suffixes, or dialed numbers. Otherwise, the Remote Recording feature will not work correctly.

> **Important**
>
> To use SRTP for this connection, the PSTN Gateway in Skype for Business must be configured using the full FQDN of the host where SIP Server is located to ensure that certificate exchange is successful.

Failure processing

- If the Connector is not able to establish a connection to a remote SIP Server (due to network issues or misconfiguration), T-Server does the following:
    - Stop the ongoing scenario for recording initiation.
    - Report EventError to a client if recording was initiated at the client’s request.
- When T-Server loses an existing T-Lib connection to SIP Server, T-Server attempts to establish a new connection to a remote recording application, as defined by parameters Reconnect Timeouts and Reconnect Attempts in the Server Info tab of the SIP Server application object. If there are ongoing recording sessions in progress, they will be kept intact and will not be disconnected unless a recording session is dropped by the remote recording server. If the connection is dropped, T-Server cleans up a connection to the remote server without any interruptions to the current call.
- For Skype for Business Front End server or Connector failovers, T-Server might not be able to restore a recording session. However, in any failure scenario, T-Server attempts to release an orphaned recording leg when a referenced call is deleted or in an unmanageable state.

Feature limitations

- Recording is supported only for the audio part of a call.
- T-Server records a mixed audio stream only of the entire call.
- Recording of a call is not affected if any party connects to the call or disconnects from the call, as long as there are at least two established parties in the call and the configuration allows for continued recording. This includes escalation scenarios and scenarios involving supervision.
- An additional recording session is not created if a call is already being recorded, regardless of any other conditions.
- Recording of parties in consultation calls is not supported.
- Because of the mixed sound, GIR associates a recording session with the first DN that originated this session only.
- Remote recording is not supported in a SIP Server Business Continuity environment.
- Supervisor cannot be responsible for recording initiation. T-Server ignores the supervisor recording configuration.
- If an established call is being recorded and T-Server is stopped and started again, the recording of this call after the T-Server restart is currently not supported. The call recording session will only be terminated by T-Server when the call being recorded is released.
- SIP Server supports only one Trunk Group object for remote recording.
- Screen Recording is not supported.

Feature comparison chart

The following table compares support for recording and other features by SIP Server and Multimedia Connector for Skype for Business.

Y—Supported
N—Not supported

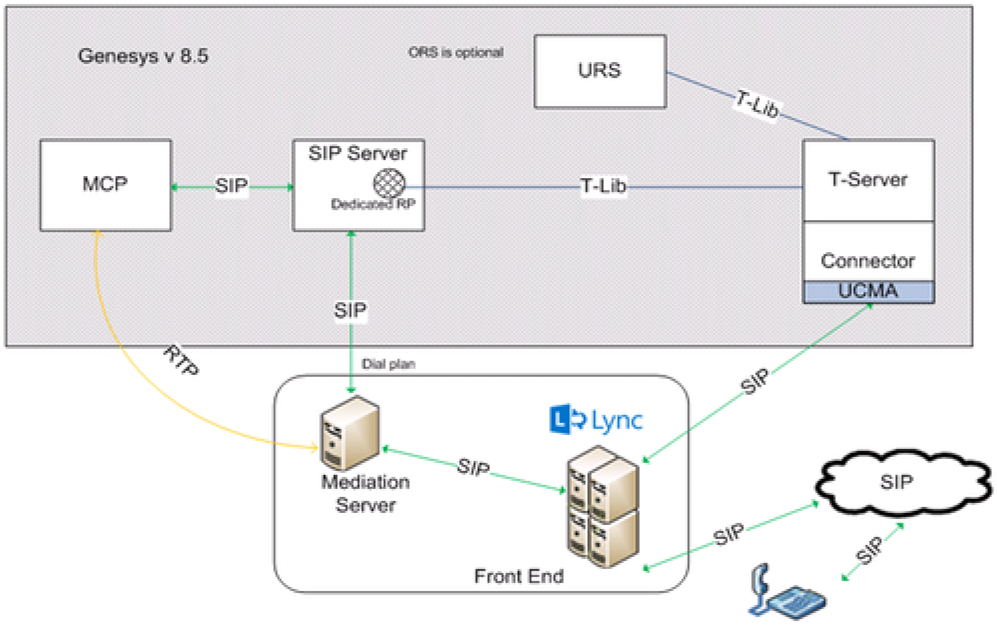
Failures		
Feature	**SIP Server**	**Multimedia Connector for Skype for Business**
Dynamic call recording	Y	Y
Mid-call control of the recording session (pause/resume/stop)	Y	Y
Recording control using TRouteCall extensions	Y	Y
DN configuration for recording	Y	Y

Failures		
Trunk recording	Y	N/A
Conference recording	Y	Y
Continuous recording for transfer scenarios	Y	Y
Consult call recording	Y	N
Recording calls without music-on-hold treatment	Y	Y
IVR recording	Y	Y
Emergency call recording	Y	N/A
MSML-based recording	Y	Y
GIR integration	Y	Y
Call recording—geo-location	Y	Y
Call recording alarms	Y	Y
DTMF clamping in a conference	Y	N/A
MCP failure	Y	Y
Connectors failover	N/A	partial Note: A recording session might not be completely restored. However, T-Server will release any orphan recording session.
Front End failover	N/A	partial Note: A recording session might not be completely restored. However, T-Server will release any orphan recording session.
Recording SIP Server failover	N/A	partial Note: T-Server will release any orphan recording session.
Deployments		
Single site	Y	Y

Failures		
Multisite recording control	Y	N
Business Continuity	Y	N

Remote Treatments

T-Server for Skype for Business supports remote call treatments using SIP Server version 8.1.102.65 or later. T-Server creates a leg to SIP Server for a routed call on a dedicated Routing Point, and then proxies all treatment requests to SIP Server. Treatments provided by SIP Server depend on your version of SIP Server. See the Framework 8.1 SIP Server Deployment Guide for details.



Configuring remote treatments

1. On the SIP Server side:
    1. On the Connections tab of the SIP Server application object, add an ISCC connection to T-Server for Skype for Business.
    2. Configure a dedicated Routing Point on the Switch object assigned to SIP Server.
        - On the Annex tab, create a section with the URS Application name. In that section, add the **event_arrive** option and set it to none. Create a similar section with **event_arrive**=none for each URS that is connected to SIP Server, including backup URS instances. (That way, URS does not control the corresponding DN.)
    3. Configure a DN of type Trunk with a dedicated prefix and **sip-proxy-headers-enabled** set to `false`.
    4. Create an MSML DN of type **Voice over IP Service**. In the **[TServer]** section, configure the following options:

- **contact**=`<Resource Manager host:port>`
- **cpd-capability**=`mediaserver`
- **make-call-rfc3725-flow**=`1`
- **predictive-timerb-enabled**=`false`
- **prefix**=`msml=`
- **refer-enabled**=`false`
- **ring-tone-on-make-call**=`false`
- **service-type**=`msml`
- **userdata-map-filter**= `*`
- **userdata-map-format**=`sip-headers-encoded`

5. Configure a dial-plan rule to forward treatment calls to the dedicated Routing Point by the prefix.

2. In the T-Server application:
   1. On the Connections tab, add an ISCC connection to SIP Server.
   2. On the Options tab, create the **[remote-treatment]** section and configure the following options in that section:
      - **server-application** = <The SIP Server Application name from the Connection tab>
      - **route-point** = <The name of the Routing Point configured on the Switch assigned to SIP Server>
      - **uri-pattern** = `[sip]:{<prefix>{DDDDDDD}}[@<urisuffix>]`
        where:
        - `<prefix>` is a permanent prefix which allows to match a call and configure a dial-plan rule on the SIP Server side;
        - `{DDD…}` is a random number generated by T-Server with the configured length;
        - `[sip:]` and `[@urisuffix]` are optional parts, and depend on the configuration of outbound routing on Skype for Business Server.

        For example: `sip:{+1999{DDDDDDD}}@lyncdco.lab`

        or

        `{+1999{DDDDDDD}}`

3. On the Skype for Business side:
   - Configure outbound call routing settings to send calls to numbers with the specified `<prefix>` to the trunk configured for SIP Server in the Skype for Business Server Topology. See step 10 in the Deployment Summary section.

For remote treatments, you must configure voice routes and PSTN usage. See details at: https://technet.microsoft.com/en-us/library/gg398272(v=ocs.16).aspx.

Transport Layer Security

T-Server supports the standard Transport Layer Security (TLS) Protocol, which offers confidentiality, integrity protection, and data compression to client/server applications. T-Server also supports TLS connections with Management Framework, T-Library clients, and between internal T-Server components (T-Server and UCMA Connector). Any matching TLS certificates can be used for secure connection (not just produced by Genesys). For a detailed description of how the TLS protocol works, see the relevant RFCs:

- RFC 5246—The Transport Layer Security (TLS) Protocol
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)

You can also find a more general description of TLS and how Genesys uses the protocol in the *Genesys Security Deployment Guide*.

Configuring TLS Between T-Server and Connector

Configuring the TLS Connection for the Connector

The UCMA Connector supports two different ways of configuring TLS connection:

- The value of the certificate thumbprint, or its *friendly* name can be configured in the **[startupOptions]** section of the connector's configuration file. For example:

```
<startupOptions>
   <add key="connectorCertificate" value="416af925efade88309cdf203813e1e3b19f6"/>
     </startupOptions>
```

- The value of certificate thumbprint, or its *friendly* name can be provided in the command line. The command line option name is **-connectorCertificate**. For example:

```
    Mslync_connector.exe –connectorCertificate "416af925efade88309cdf203813e1e3b19f6"
```

Important

The option in the command line takes precedence over the value set in the configuration file.

Configuring the TLS Connection for T-Server

T-Server uses the Application-level conn-certificate option for configuring the secure connection. The value of the option is used each time T-Server performs a connection to any connector. In the **[TServer]** section of the T-Server Application object, set the **conn-certificate** option to a valid thumbprint—for example, `416af925efade88309cdf203813e1e3b19f6c283`, or `6a f9 25 ef ad e8 83 09 cd f2 03 81 3e 1e 3b 19 f6 c2 83`.

Note that you can provide two formats for the thumbprint. As shown in the above example, both forms are acceptable as long as the value corresponds to the thumbprint of a valid certificate available in the Certificate store. The spaces are for convenience.

UTF-8 Encoding

UTF-8 data encoding enables T-Server and the Connector to work with multi-language data that is encoded with UTF-8. This support applies to attached data, IM treatments, and usernames.

Log Files

The Genesys log library supports transparent printing of UTF-8 strings. However, it does not print byte order mark (BOM) at the beginning of log files. To represent data properly, the log viewer must have default encoding “UTF-8” (or "UTF-8 without BOM"). Some text editors (like notepad++) allows to switch between encoding modes. T-Server, by default hides sensitive data (for example, treatments parameters), and prints the attribute length only.

The UCMA Connector requires additional configuration to print non-ASCII characters in a log. In the **[Log]** section, set the **fileEncoding** option to `utf-8` to enable this feature.

Presence Activity

T-Server is able to set the presence state of a Lync user to a state that depends on transactions on the Genesys side. For instance, if a Contact Center agent becomes unavailable because of After Call Work, T-Server publishes the appropriate presence value to Lync for that agent. Microsoft Lync supports Locale IDs referenced for a particular "activity" string. For more information, see Presence.

Attached User Data

Workspace Desktop Edition uses UserData with the predefined key **IW_FirstMessage** to deliver the first IM message in toast on the E-Ringing event. T-Server does not execute coding/ encoding of the string User Data values. It provides transparent transmission (byte to byte) of the User Data between the T-Clients and servers through ISCC data propagation.

IM Treatments

T-Server transmits UTF-8 data into the Lync via Connector for Instant Message treatments. The Connector considers all IM treatment texts as UTF-8 encoded.

DN Names

T-Server considers and utilizes DN names as user SIP URIs. Although, T-Server does not have special restriction on URI symbols, Microsoft Lync Server 2013 allows only ASCII characters in URIs, as well as in User names, domain names, etc. Therefore, this release does not support non-ASCII characters in DN names.

Supported Media Types

T-Server supports the following media types:

- Audio
- Instant Messaging (IM)
- Video

Audio Calls

T-Server supports all general features, such as call origination, consultation calls, transfers, conferences, single-step operations, hold/retrieve operations (including ones originated from a Skype for Business Client), routing, merge operations. T-Server reports an audio call as a call with AttributeMediaType 0 (TMediaVoice). See the list of available features and requests in Features and T-Library Functionality Support sections.

T-Server does not support the following for audio calls:

- 3pcc Answer operation and initiation of a consultation call for a consultation call
- 1pcc single-step operations

T-Server uses TMuteOn/Off to execute switching between supervision modes only.

For more information, see Using Workspace Plugin for Skype for Business.

IM Calls

T-Server reports an IM call as a separate T-Library call with AttributeMediaType 5.

T-Server supports a limited number of call operations. An IM call can be initiated:

- As an inbound call from a customer via a distributed device (Routing Point)
- As an internal 3pcc call initiated by a TMakeCall request
- As an internal 1pcc call initiated by a Skype for Business Client

> ### Important
> To originate a 3pcc IM call, the desktop must add the Extension key **chat**=true to the request.

T-Server supports a limited set of T-Requests for IM calls:

- Routing IM calls from a Routing Point to an agent or another distribution device

- Transferring IM calls from one agent to another by using TSingleStepTransfer requests
- Establishing a conference with another agent by using TSingleStepConference requests

T-Server provides the ability to create a consultation call by using a 3pcc TMakeCall request.

When an IM conference is created, the IM MCU records the first 40 seconds of the IM Conference, and replays the messages back to the participants that join within that 40-second timeframe. This is done to facilitate the conference startup timeframe where users may join at different times but have a reasonable expectation to be treated as joining at the same time as other users. After the 40 seconds that precede the beginning of the IM conference, there is no buffer. It is assumed that new participants will only be concerned with what occurs after they actually join the conference.

> Warning
>
> Skype for Business Server releases an unused IM session after 10 minutes of inactivity. This is the default behavior which cannot be overridden on the Genesys T-Server and UCMA Connector for Skype for Business side. Contact the Skype for Business vendor for details.

For more information, see Using Workspace Plugin for Skype for Business.

Limitations

T-Server does not support the following for IM calls:

- TInitiateTransfer and TInitiateConference requests
- Merge of main and consultation IM calls
- IM consultation call for an audio call
- Supervision
- No-Answer Supervision
- 1pcc operations (except call origination)
- 3pcc Answer
- Historical reporting

Video Calls

T-Server reports a video call as a call with AttributeMediaType 0 (TMediaVoice). No T-Library message or attribute is reported to indicate a Video stream presence and, therefore, there is no way to distinguish between an Audio only call and an Audio/Video call.

> Important
>
> Video is available only in a Skype for Business environment, and not with Lync 2013.

For more information, see Using Workspace Plugin for Skype for Business.

Supported Media Escalations

- Escalation between IM call and audio call
- Escalation between audio call and video call

Escalation Between IM Call and Audio Call

T-Server supports escalation operations from an IM call to an audio call and de-escalation from an audio call to an IM call. During escalation T-Server creates a new separate call object with a new Connection ID. A new call inherits a Conversation ID from the parent call. However, T-Server does not set up the main-consultation relationship between the escalated call and the new call. When an audio call is placed on hold, the held party cannot receive instant messages.

> ## Important
>
> - There is no unique event reported by T-Server to indicate that an escalation scenario has occurred. The only way, in T-Server events, to identify calls that are related to an escalation scenario is by the **Conversation-ID** extension key. All those calls will have the same **Conversation-ID**. See Attribute Extensions for more information.
> - When a consultation call is initiated from an escalated call with voice and IM sessions, an IM conference is created in which messages from the customer are received by all participants, but IMs from agents are not seen by the customer. IMs are seen by all remaining participants after the transfer or conference is completed.

Limitations

- TReleaseCall for an escalated IM call releases the whole conversation (IM and audio calls).

Escalation Between Audio Call and Video Call

T-Server supports escalation operations from an audio call to a video and de-escalation from a video call to an audio call. If the customer wants to add video, Multimedia Connector for Skype for Business does not generate and send a second EventQueued/EventRouteRequest for the new media. After the agent accepts the video, the underlying call stays the same.

Handling User Data

Starting with release 8.5.000.87, user data can be propagated from an original call into an escalated call in media escalation scenarios. The escalation-user-data option enables this feature and provides backward compatibility.

Capacity Rules

Since T-Server for Skype for Business supports calls with different media types, business rules used for routing may be such that an agent busy on an IM call should be considered available to receive a voice or video call and vice versa. In such cases, it is important to configure and use capacity rules as described in the Genesys 8.1 Resource Capacity Planning Guide.

Limitations

In an environment where the same agent handles Skype for Business calls and e-Services interactions, whenever the agent has no Skype IM call, the Skype for Business channel will be considered to have capacity for Chat type interactions and Chat interactions may be routed to the agent even if the agent is not ready on the Chat channel.

Non-supported Media (T-Server Limitation)

- T-Server does not support screen sharing and file transfers. These operations, however, are available in the Microsoft Skype for Business client. They do not interfere with T-Server activity.

T-Library Functionality

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

- N—Not supported
- Y—Supported
- E—Event only supported
- I—Supported, but reserved for Genesys Engineering
- An asterisk (*) indicates the event that contains the same Reference ID as the request

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

When a set of events is sent in response to a single request, the events are listed in an arbitrary order. For more information, refer to the Genesys Events and Models Reference and the Platform SDK .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.

Feature Request	Request Subtype	Corresponding Events	Supported
General Requests			
TOpenServer		EventServerConnected	Y
TOpenServerEx		EventServerConnected	Y
TCloseServer		EventServerDisconnected	Y
TSetInputMask		EventACK	Y
Registration Requests			
TRegisterAddress[1]		EventRegistered	Y
TUnregisterAddress[1]		EventUnregistered	Y
Call-Handling Requests			
TMakeCall	Regular	EventDialing*	Y
TAnswerCall			N
TReleaseCall		EventReleased	Y
TClearCall		EventReleased	Y
THoldCall		EventHeld	Y

Feature Request	Request Subtype	Corresponding Events	Supported
TRetrieveCall		EventRetrieved	Y
Transfer/Conference Requests			
TInitiateTransfer²		EventHeld EventDialing*	Y
TCompleteTransfer		EventReleased* EventPartyChanged	Y
TInitiateConference²		EventHeld EventDialing*	Y
TCompleteConference		EventReleased* EventRetrieved EventPartyAdded EventPartyChanged	Y
TDeleteFromConference		EventPartyDeleted* EventReleased	Y
TReconnectCall		EventReleased EventRetrieved*	Y
TAlternateCall		EventHeld* EventRetrieved	Y
TMergeCalls	ForTransfer	EventHeld EventReleased* EventRetrieved EventPartyChanged	N
	ForConference	EventHeld EventReleased* EventRetrieved EventPartyChanged EventPartyAdded	N
TSingleStepTransfer²		EventReleased* EventPartyChanged **Note:** This T-Server generates EventReleased on the transferring DN only after a call is connected on the recipient DN.	Y
TSingleStepConference		EventRinging* EventEstablished EventPartyAdded	Y
Call-Routing Requests			
TRouteCall	Unknown	EventRouteUsed	Y
	Default		Y
	Reject		Y
	CallDisconnect		Y

Feature Request	Request Subtype	Corresponding Events	Supported
Call-Treatment Requests			
TApplyTreatment	PlayApplication	EventTreatmentApplied + EventTreatmentEnd)/ EventTreatmentNotApplied	Y
	Music		Y
	RingBack		Y
	Silence		Y
	Busy		Y
	CollectDigits		Y
	PlayAnnouncement		Y
	PlayAnnouncementAndDigits		Y
	RecordUserAnnouncement		Y
	FastBusy		Y
TGiveMusicTreatment		EventTreatmentApplied	N
TGiveRingBackTreatment		EventTreatmentApplied	N
TGiveSilenceTreatment		EventTreatmentApplied	N
Agent & DN Feature Requests			
TAgentLogin		EventAgentLogin	Y
AgentLogout		EventAgentLogout	Y
TAgentSetIdleReason		EventAgentIdleReasonSet	N
TAgentSetReady		EventAgentReady	Y
TAgentSetNotReady		EventAgentNotReady	Y
TMonitorNextCall	OneCall	EventMonitoringNextCall	Y
	AllCalls		Y
TCancelMonitoring		EventMonitoringCanceled	Y
TSetMuteOff		EventMuteOff	Y[3]
TSetMuteOn		EventMuteOn	Y[3]
Query Requests			
TQueryCall[1]	PartiesQuery	EventPartyInfo	N
	StatusQuery		Y
TQueryAddress[1]	DNStatus	EventAddressInfo	Y
TQueryLocation	AllLocations	EventLocationInfo	I
	LocationData		I
	MonitorLocation		I
	CancelMonitorLocation		I
	MonitorAllLocations		I

Feature Request	Request Subtype	Corresponding Events	Supported
	CancelMonitorAllLocations		I
TQueryServer[1]		EventServerInfo	Y
User-Data Requests			
TAttachUserData		EventAttachedDataChanged	Y
TUpdateUserData		EventAttachedDataChanged	Y
TDeleteUserData		EventAttachedDataChanged	Y
TDeleteAllUserData		EventAttachedDataChanged	Y
ISCC (Inter Server Call Control) Requests			
TGetAccessNumber[2]		EventAnswerAccessNumber	I
TCancelReqGetAccessNumber		EventReqGetAccessNumberCanceled	I
Special Requests			
TReserveAgent		EventAgentReserved	I
TSendEvent		EventACK	I
TSendEventEx		EventACK	I
TSetCallAttributes		EventCallInfoChanged	I
TSendUserEvent		EventACK	Y
TSendDTMF		EventDTMFSent*	Y
TPrivateService		EventPrivateInfo*	Y
TNetworkSingleStepTransfer		EventNetworkCallStatus	N
TNetworkPrivateService		EventNetworkPrivateInfo	N
ISCC Transaction Monitoring Requests			
TTransactionMonitoring		EventACK	Y
		EventTransactionStatus	E

Table notes:

- 1—Only the requestor receives a notification of the event associated with this request.
- 2—This feature request may be made across locations in a multi-site environment. However, if the location attribute of the request contains a value relating to any location other than the local site—except when the response to this request is EventError—there will be a second event response that contains the same reference ID as the first event. This second event will be either EventRemoteConnectionSuccess or EventRemoteConnectionFailed.
- 3—T-Server supports TSetMuteOn and TSetMuteOff only for established conferences, to allow for service observing.

Attribute Extensions

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

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

Extension		Used In	Description
Key	**Type**		
Call-related Requests and Events			
Conversation-ID	String	EventHeld EventRetrieved EventError EventAbandoned EventDialing EventDiverted EventEstablished EventNetworkReached EventPartyAdded EventPartyChanged EventPartyDeleted EventQueued EventReleased EventRinging EventRouteRequest EventRouteUsed EventTreatmentApplied EventTreatmentEnd	Enables to identify different media calls as members of the same Lync conversation. The Conversation-ID could be changed during the duration of the call—for example, as a result of call merge.
Cookie	String	TMakeCall	For internal usage.
chat	String	TMakeCall	Specifies media for a call. Valid values are `true` and `false`.
pass-transcript-to-agent	String	TRouteCall	Governs whether the target agent of a routed IM call receives a transcript of the message exchange between the customer and IM treatments prior to the agent’s connection. • If set to `true`, a transcript of the message exchange between the customer and IM treatments is passed to the targeted agent after the call is established.

Extension		Used In	Description
			• If set to `false`, the agent does not receive the initial interaction between the customer and treatments. **Note:** If set, it overrides the pass-transcript-to-agent Application-level configuration option.
USER_ANN_ID	String	EventTreatmentEnd	Specifies the message identifier, an integer, recorded by the user specified with USER_ID.
INTERRUPTED	String	EventTreatmentEnd	Valid values: • `NO`—If the announcement is not interrupted. • `KEYPAD`—If it is interrupted by keypad entry. • `VOICE`—If it is interrupted by the caller speaking something.
COMPLETION_STATUS	String	EventTreatmentEnd	Valid values: • `NORMAL`—If the treatment is completed normally (optional). • `TIMEOUT`—If the digit collection is timed out before all required digits could be collected. • `CANCELLED`—If the treatment is cancelled by a request from the router.
VERIFICATION_STATUS	String	EventTreatmentEnd	Valid values: • 1—The result of digits verification is successful.

Extension		Used In	Description
			• 0—The result of digits verification is not successful.
cause	String	EventDNOutOfService	Introduced in 8.5.001.14. Specifies the cause of DN unavailability in text form, for troubleshooting purposes, when T-Server unregisters a device on the Connector, and consequently on Skype for Business Server, when a DN is deleted or disabled in the Configuration Layer.
DN-related Requests and Events			
PresenceType	String	EventRegistered EventAddressInfo EventDNBackInService EventDNOutOfService EventDNDOn EventDNDOff	Introduced in 8.5.001.44. Indicates the type of presence that the Connector currently monitors for the DN device. The following values are supported: • local—indicates that the Connector monitors a local presence of a device and allows to change it. • remote—indicates that the Connector monitors a remote presence of a device and rejects attempts to change it.
Emulated Agents			
WrapUpTime	Integer	TAgentLogin TAgentNotReady	Specifies whether T-Server applies the automatic wrap-up timer when an agent sends the TAgentNotReady request while in idle state.

Extension		Used In	Description
LegalGuardTime	Integer	TAgentLogout	Specifies a legal-guard time (in seconds) for agents to postpone the transition to the Ready state after a business call or after timed ACW.
LogoutOnDisconnect	Boolean	TRegisterAddress	Specifies how the EventLogout message is distributed. If it is `true`, the EventLogout message is distributed as soon as the client that requested the login disconnects from T-Server or unregisters the DN in question. The EventLogout message is distributed when T-Server distributes EventOutOfService.
Presence-profile	String	TAgentLogin	Specifies the profile name that is assigned for the DN during a particular agent session.
LegalGuardTime	Integer	TAgentLogout	Specifies a legal-guard time (in seconds) for agents to postpone the transition to the Ready state after a business call or after timed ACW.
Call Supervision			
MonitorMode	String	TMonitorNextCall TRouteCall TSetMuteOn TSetMuteOff EventPrivateInfo	Specifies the monitoring mode as follows: • `mute, normal`—A mute connection. • `connect`—A three-party conference call (open supervision). • `coach`—Only the agent can hear the supervisor (whisper coaching). If MonitorMode is set to coach in the TSetMuteOff or TSetMuteOn request, the monitoring mode is changed to whisper coaching for the current supervision session. Note: TSetMuteOn and

Extension		Used In	Description
			TSetMuteOff support only the coach value.
MonitorScope	String	TMonitorNextCall TRouteCall	Specifies the required intrusion/observation scope. Values: • agent—The monitoring is initiated for a specific agent. The supervisor is disconnected when the call is transferred or released, but will be connected to the next call that is routed to the same agent. • call—The monitoring is initiated to track an entire customer call. If the call is transferred to another agent, queue, or VRU, the monitoring function continues with the call until the customer disconnects the call.
AssistMode	String	TSingleStep-Conference	Specifies the required assistance mode. Values: • connect—This is the default value - a three-party conference call. • coach—Only the agent can hear the supervisor (whisper coaching).
Call Recording			
record	String	TRouteCall	Values: • destination—Recording

Extension		Used In	Description
			continues until the destination of TRouteCall is present on the call. - `source`—Recording continues until an originator is present on the call. - `disabled`—Recording does not start even if the destination of TRouteCall has mandatory recording configured.
No-Answer Supervision			
NO_ANSWER_ACTION	String	TAgentLogin	Values: - `none`—SIP Server takes no action on agents when calls are not answered. - `notready`—SIP Server sets agents to NotReady when calls are not answered. - `logout`—SIP Server automatically logs out agents when calls are not answered.
NO_ANSWER_TIMEOUT	Integer	TRouteCall	If set, the value of this key overrides any value set in the `no-answer-timeout` configuration option for the current call.

Hardware Sizing Guidelines and Capacity Planning

This section describes the results of testing Skype for Business release 8.5.000.87, and serves as a guideline when optimizing capacity, sizing, and resource usage. Before deploying in a production environment, you must test Skype for Business in a test environment under a production load to ensure its performance meets your expectations and that it is sized properly.

Architecture Used for Testing

500px

This figure depicts the architecture of the single data center Skype for Business (Microsoft) solution, and the call flow between it and the Genesys environment.

The Microsoft enterprise deployment includes:

- A pool of Mediation Servers—Translates signaling between the solution infrastructure and the PSTN gateway or SIP Trunk. The Front End Pool hosting the Genesys Contact Center applications must not be deployed using collocated Mediation Servers.
- A DNS balanced pool of Front End Servers—Shares the load. Each Front End Server maintains its own database that is synchronized with other Front End Servers.
- A Back End server and Domain Controller.

Minimum Hardware Requirements for Multimedia Connector for Skype for Business

T-Server for Skype for Business:

- 1 core CPU
- 4 GB memory

UCMA Connector:

- 6 core CPU
- 8 GB memory

See system requirements and recommendations for more information.

Test Results

Tests were performed on the following environment:

- 1 Mediation pool with 4 Mediation servers
- 1 Front End pool with 8 Front End servers
- 1 Trusted Applications pool with 8 UCMA Connectors
- 1 T-Server for Skype for Business

Genesys recommends reserving at least 2 Front End servers for HA needs.

At peak load, 1200 simultaneous calls in all scenarios were sent through the environment, and 2000 simulation agents were logged-in and engaged in the calls during the testing.

The calls-per-second rate sustained by the solution is not directly dependent on the number of deployed components or CPUs. Each new call created at the T-Server requires that you allocate resources for such activities as conference scheduling. The number of conferences created at the same time can be limited; for more information, see the Microsoft limitation. Therefore, it is not possible to achieve higher call rates, even taking into account CPU availability and load sharing among multiple components.

In general, a single instance of the T-Server with a pool of Connectors can support the following:

- Up to 1200 simultaneous calls in regular load (including at least 200 calls parked at Routing Points or processed by IVRs)
- Up to 1000 registered agents
- Up to 6 calls per second
- Up to 100 updates of attached data per call

Note that consultation calls, transfers, and conferences increase the load.

Error Messages

This table presents the complete set of error messages T-Server distributes in EventError, which T-Server generates when it cannot execute a request because of an error condition.

Code	Symbolic Name	Description
40	TERR_NOMORE_LICENSE	No more licenses are available.
41	TERR_NOT_REGISTERED	Client has not registered for the DN.
42	TERR_RESOURCE_SEIZED	Resource is already seized
43	TERR_IN_SAME_STATE	Object is already in requested state.
50	TERR_UNKNOWN_ERROR	Unknown error code. Request cannot be processed.
51	TERR_UNSUP_OPER	Operation is not supported.
52	TERR_INTERNAL	Internal error.
53	TERR_INVALID_ATTR	Attribute in request operation is invalid.
55	TERR_PROTO_VERS	Incorrect protocol version.
56	TERR_INV_CONNID	Connection ID in request is invalid.
57	TERR_TIMEOUT	Switch or T-Server did not respond in time.
58	TERR_OUT_OF_SERVICE	Device is out of service.
59	TERR_NOT_CONFIGURED	DN is not configured in the Configuration Database.
61	TERR_INV_CALL_DN	DN in request is invalid.
71	TERR_INV_CALD_DN	Invalid called DN.
93	TERR_DEST_INV_STATE	Destination Invalid State.
111	TERR_TOO_MANY_REQ	Too many outstanding requests.
123	TERR_DN_NOT_EXIST	DN for association does not exist.
177	TERR_TARG_DN_INV	Target DN Invalid.
223	TERR_BAD_PARAM	Bad parameter is passed to function.
226	TERR_OUT_OF_MEM	Out of memory (local).
236	Timeout performing operation	Request failed as no response from Connector (hence from SfB) for requested service received during timeout.
237	Call has disconnected	Request failed due to the main call being disconnected.

Code	Symbolic Name	Description
291	Other telephony operation in progress	Request failed because there is still pending request for the same call/device/etc in progress.
415	TERR_INV_DEST_DN	The destination DN in the request is invalid.
470	TERR_PARTY_NOT_ON_CALL	Party in request is not involved in a call.
481	TERR_NOT_SIGNED_AGENT	The destination agent is not signed in.
496	TERR_INV_CALL_STATE	Party in request is in the call state.
563	TERR_NO_CALL	No call.
565	TERR_INVALID_STATE	Invalid State.
1140	TERR_CSTA_OPER_REQ_INCOMPAT	Request incompatible with object.
1703	TERR_SOFT_AGENT_WRONG_ID	Agent has a wrong ID.
1706	TERR_SOFT_AGENT_ALREADY_LOGGED_IN	Agent has already logged in.
1707	TERR_SOFT_AGENT_NOT_LOGGED_IN	Agent has not logged in.

Known Limitations and Workarounds

The following known limitations apply to the Multimedia Connector for Skype for Business 8.5.0 release:

Domain	Capability	Support	Details/Limitations
Platform	Microsoft	Lync 2013 Server Skype for Business Server Client versions	See software requirements, minimum versions.
	Genesys	Genesys 8.x suite	See prerequisites for Workspace Plugin for Skype for Business. See Multimedia Connector sellable item and prerequisites.
	Performance	1,000 concurrent sessions	See hardware sizing guidelines.
	Architecture	Genesys High Availability: • T-Server hot standby • Connectors in load balancing	See HA architecture, including: • T-Server HA limitations • Connector HA limitations No Genesys SIP Business Continuity support. No built-in Disaster Recovery support. No graceful shutdown and in-service upgrade of Connector.
		Partitioning	Only one T-Server is supported per Skype for Business deployment. It is not possible to make calls between devices that are controlled by different T-Servers connected to the same Skype for Business deployment.
		Multiple Front End Pools	• All connectors must be connected to a single Front End pool. • Agents can be

Domain	Capability	Support	Details/Limitations
			distributed among multiple Front End pools. See Skype for Business topology.
		Front End Pool Pairing	Front End Pool Pairing is supported for agent pools only. Agents will experience a service interruption while an agent pool failover/failback is executed. Front End Pool Pairing is not supported for any Front End pool that is hosting Connectors. See Paired Front End Pools.
		Skype for Business Federation	See Federation Platform with Microsoft Office 365 Cloud.
		Skype for Business SBA/SBC	See SBA/SBS support.
		Collocated Mediation Servers	Not supported in production environments in the Front End Pool that is hosting Genesys UCMA Connector applications. A dedicated Mediation Server Pool must be used.
	Multi-site support	Multi-site support	Multi-site support with SIP Server and other T-Servers, but no support with other instances of T-Server for Skype for Business. See multi-site support.
Functional	Customer access	PSTN • via Mediation Server • via SIP Server in-front	
		Skype for Business client • Internal user • Federated user	No Skype consumer. No webSDK support. No appSDK support. See Federation Platform with Microsoft Office 365 Cloud.
	Channel – IM	Routing	See the following topics:

Domain	Capability	Support	Details/Limitations
		Treatment 3pcc Supervision Reporting	• IM features • IM Transcripts • IM calls • T-Library support
	Channel - Voice	Routing Treatment 3pcc Supervision Reporting Recording	See the following topics: • Supported Features • Voice Interactions - Plugin • Call Supervision limitations • Remote Recording limitations • T-Library support • Comparison table with SIP Server
	Channel - Video	Routing No treatment 3pcc Reporting No recording	Not supported with Lync 2013 Server See the following topics: • Video calls • Video interactions • T-Library support
	Multimodal	Escalation	See the following topics: • Escalation limitations • Media types not supported
	Desktop	Workspace Desktop Edition	No GPlus adapter support. No custom desktop (SDK) support. No hardphone support. See WDE documentation.
	Presence propagation	Direction configurable	See Presence.
	Tel URIs	Not supported	See Configuring Skype for Business User Endpoints.
Genesys applications	Framework	Genesys TLib	

Domain	Capability	Support	Details/Limitations
support		applications: URS, Stat Server, ICON...	
	GVP	SIP in-front architecture.	See SIP Server in Front.
	Recording	Genesys Interaction Recording	No 3rd party recording connector support. See Remote Recording limitations. See GIR documentation.
	Outbound	SIP in-front architecture All dialing modes	See Trusted Application Endpoints for conference services.
	Voicemail	SIP in-front architecture	No Message Waiting Indicator.
	SmartLink	Not supported	
Skype for Business application support	Voice Response Group	Support was provided for Response Groups with the introduction of the B2B feature in version 8.5.001.63. Not supported for earlier versions.	For versions earlier than 8.5.001.63, Skype for Business does not allow a call that is monitored by Genesys to be delivered to a Voice Response Group. Possible workarounds: • Handling Direct Calls • Recommended Workarounds: Working with Workspace Intercommunication Options
	Voicemail	Not supported	Skype for Business does not allow a call that is monitored by Genesys to be delivered to Voicemail. Only direct calls that are not managed by Connector will reach such destinations.
	Forwarded extensions/ Simultaneous ringing	Support is provided for Forwarding/ Simultaneous Ringing with the introduction of the B2B feature in version 8.5.001.63. Not supported for earlier versions.	For versions earlier than 8.5.001.63, Skype for Business does not allow a call that is monitored by Genesys to be delivered to another Skype for Business user with Forwarding or Simultaneous riging activated. Only direct

Domain	Capability	Support	Details/Limitations
			calls that are not managed by Connector will reach such destinations.

Skype For Business Front End Server Maintenance

If a Front End Server is stopped or failover is invoked, the remaining Skype for Business Front End Servers initiate actions to redistribute the roles of the stopped Front End Server between themselves. In this instance the following applies:

- If the Front End Server is stopped (for example, by rebooting the server or invoking **Stop-CsWindowsService**), it will take at least 5 minutes before the remaining Front End Servers have completely synchronized. If the stopped Front End Server is restarted before the synchronization between the remaining Front End Servers is completed, it can lead to de-synchronization between the UCMA Connectors and the Front End Servers. There must be at least 5 minute delay before restarting a stopped Front End Server.
- If the **Invoke-CsComputerFailOver** command is issued while UCMA Connector is running, it can take up to 20 minutes or longer for the failover to successfully complete. This means the **Invoke-CsComputerFailBack** command should not be invoked for at least 20 minutes.
- Active calls that are being managed by the Front End Server being stopped or failed over may be reported as released by T-Server.
- T-Server may reject call related requests for calls for that were managed by the stopped Front End Server until all states have been redistributed and re-synchronized.

Recommended Workarounds: Working with Workspace Intercommunication Options

There are several limitations that cannot be managed directly by the Multimedia Connector for Skype for Business. To properly manage these, it is necessary to work with the routing-based calling feature using the intercommunication options in Workspace Desktop Edition (WDE). See this topic for details.

These limitations include the following:

- Inability to manage the CLID for outbound calls: Calls made from a T-Server monitored user to either a non-monitored Skype for Business user or to an external user using PSTN will arrive at the destination with the CLID of the internal resource used by the Multimedia Connector to manage this call, instead of the CLID of the actual caller.
- Inability to cancel an outbound call before it has been answered: Skype for Business does not allow Multimedia Connector to cancel an outbound call before it rings.
- Inability to make calls to Skype for Business Response Groups: Skype for Business will block any attempt to establish a call between 2 conference resources. Because both Multimedia Connector and Response Groups rely on conferencing resources, it is not possible for a Genesys agent to directly call a

Response Group.

Using this Workspace feature, it is possible to make use of the Genesys SIP Server to work around these missing capabilities. The basic call flow will be as follows:

1. An agent initiates an outbound call using Genesys Workspace.
2. Workspace sends this call to a designated Routing Point on Skype for Business. The actual intended final destination is attached as user data in the key **IW_RoutingBasedTargetId**.
3. At this Routing Point, a strategy is loaded that routes the call to a designated Routing Point on SIP Server.
4. From this SIP Server Routing Point, it is possible to use the capabilities of SIP Server to manage the call.

Configuration Procedure

The following procedure enables the basic capability to enable a routing-based calling feature in Workspace to work in a Skype for Business environment.

1. Deploy SIP Server and create a Trunk DN to enable calls between Skype for Business and SIP Server. Ensure calls can be passed between Skype for Business and SIP Server.
2. Configure ISCC between SIP Server and T-Server for Skype for Business as described in Chapter 9, Multi-Site Support, of the SIP Server Deployment Guide. Note that T-Server for Skype for Business supports only **cast-type**=`route`.
3. Configure a dedicated Routing Point on the Switch object assigned to SIP Server.
4. Configure a dedicated Routing Point on the Switch object assigned to T-Server for Skype for Business. On the Annex tab of this Routing Point, in the **[TServer]** section, create the **override-call-type** option and set it to 3.
5. Configure the following Workspace options:
   - **contact.ucs-interaction.voice.use-dialed-phone-number** = `true`
   - **intercommunication.voice.routing-points** = <Skype for Business Routing Point from Step 4>
   - **intercommunication.voice.routing-based-targets** = `TypeDestination,Contact`
   - **intercommunication.voice.routing-based-actions** = `MakeCall,OneStepConference, InitConference,OneStepTransfer,InitTransfer`

Managing CLID for outbound calls

When the call initiated using the routing-based calling feature arrives at SIP Server, it will have the following user data keys:

- **PhoneNumber**
- **IW_RoutingBasedTargetId:** Provides the original called target

This information can be used in a routing strategy loaded on the SIP Server Routing Point to adjust the CLID according to requirements and route the call to the final destination provided in **IW_RoutingBasedTargetId**.

Enabling cancellation of outbound calls

Skype for Business requires that an outbound call be established before it can be abandoned or cancelled. To enable outbound calls to be cancelled when there is no answer at the destination, the routing strategy loaded on the SIP Server Routing Point must apply a silence treatment and then immediately route the call to the final destination provided in the user data key **IW_RoutingBasedTargetId**. This silence treatment will establish the call before it is routed to the final destination so that T-Server is able to cancel this call.

Calling Skype for Business Response Groups

If the Response Group (RG) is a vital part of your business process, you can utilize a workaround architecture, taking into account the following limitations:

- An agent (a user registered in the configuration environment) cannot accept a call from the RG. Only unmonitored Skype for Business users can be RG members.
- The RG can accept only direct calls from the client or from the trunk. Dialing out from the conference and conference invitation are rejected.
- The RG member (an unmonitored Skype for Business user) who answers a call from the RG cannot invite a monitored agent into this conference.

To allow calls to be made from a Genesys controlled agent to a Skype for Business Response Group, the call must be passed via SIP Server. This means that when the call arrives at the Response Group, it is coming from SIP Server rather than from another conference resource that was blocked by Skype for Business.

Configuration Procedure

All Response Groups that are accessible for a Genesys agent must be configured in the places described below. This example assumes that agents are able to call Response Group `group1@company.com`:

1. Ensure that the Workspace option **intercommunication.voice.routing-based-targets** contains the additional value ACD Queue.
2. Create a DN with the number `sip:group1@company.com` of type ACD Queue under the T-Server for Skype for Business DNs. This DN must have the **register** flag set to `False`.
3. Create a SIP Server dial plan entry that sends calls to this group back to Skype for Business using the SIP Server Trunk DN pointing at Skype for Business and the TEL number of the group.
   For example: `dial-plan-rule-`*`N`*`: sip:group1@company.com=>99+123456789`
4. Create a routing strategy loaded on the SIP Server Routing Point:
   - Set the extension **UseDialPlan**=`full`.
   - Route a call to the target provided in the User Data key **IW_RoutingBasedTargetId**.
5. If pass-through calls are not allowed, ISCC must be configured between T-Server for Skype for Business and SIP Server, and the **allow-pass-through-calls** option must be set to `iscc` for the Routing Point on Skype for Business. Otherwise, calls routed or transferred to Response Groups might be dropped.

To make a call to a Response Group, an agent searches for the group in the Workspace contacts. This search might return two results, one for the actual Skype for Business Response Group contact and the other for the corresponding ACD Queue configured in Step 1. The agent must select the entry corresponding to this ACD Queue for the call to be successful.