Multimedia Connector for Skype for Business
Configuration of Microsoft Skype for Business platform

1. Executive Summary

This paper describes how to configure Microsoft Skype for Business or Lync 2013 for integration with Genesys.

Contents

2. Objectives

The Genesys Multimedia Connector for Skype for Business integrates with Microsoft Lync 2013 or Skype for Business to support the Genesys CX platform on top of Microsoft media. In order to deploy Genesys Multimedia Connector for Skype for Business, both the Genesys and Microsoft parts need to be configured.

The objective of deployment is to go from the situation shown in Figure 1 to the architecture shown in Figure 2:

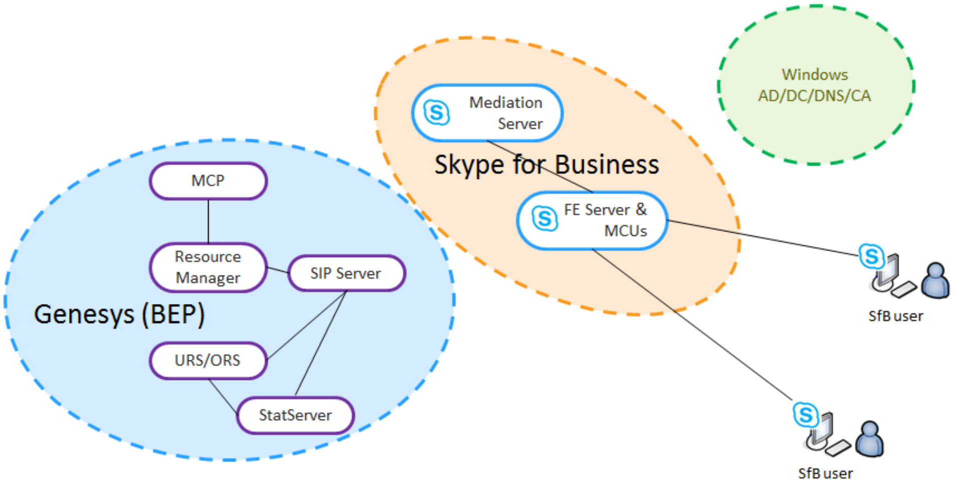


Figure 1: before

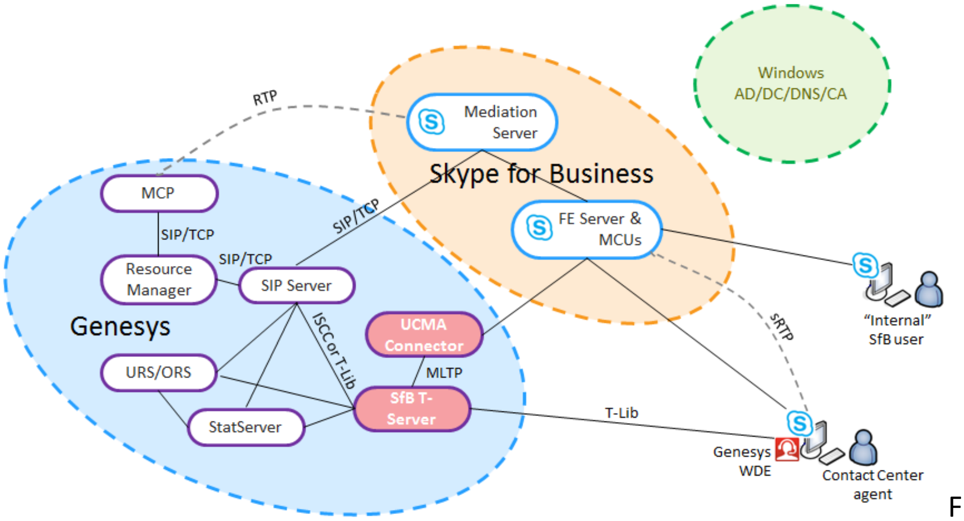


Figure 2: after

This document covers the configuration of the Skype for Business platform that allows it to talk with the Genesys components. Throughout this document, Skype for Business and Lync 2013 are treated interchangeably.

3. Sequence of operations

This section covers the deployment and configuration of:

- Single UCMA Connector,
- Single SIP Server (or a pair of Primary and Backup SIP Servers, leveraging a Virtual Host/IP address and takeover).

The configuration of HA (high availability using multiple UCMA Connectors) is slightly different. This section will present the case of a single UCMA connector; additional information for HA will be covered later in this document.

The operations to execute on Microsoft Skype for Business are the following:

1. Declare the host of the UCMA Connector as a Trusted Application Pool (Single Computer).
2. Declare the host of the SIP Server as a PSTN Gateway.
3. Provision a trunk between this gateway and the Skype for Business Mediation Server.
4. Define Policies, Voice Routes, and PSTN Usage.
5. Create a UCMA trusted application, assign it to the UCMA Connector Trusted Application Pool.
6. Create a set of Trusted Application Endpoints, used for conference reservation and for routing (Routing Points). Assign the Policies, Voice Route, and PSTN usage previously created to the Trusted Application Endpoints.
7. Request certificates for the SIP Server and UCMA Connector hosts.

You will use the following tools to make these changes: the Skype for Business Topology Builder, the Skype for Business Management Shell (an extension of Microsoft PowerShell), and the Skype for Business Control Panel.

In order to start setting up Skype for Business to integrate with Genesys, you'll need the following pieces of information up front:

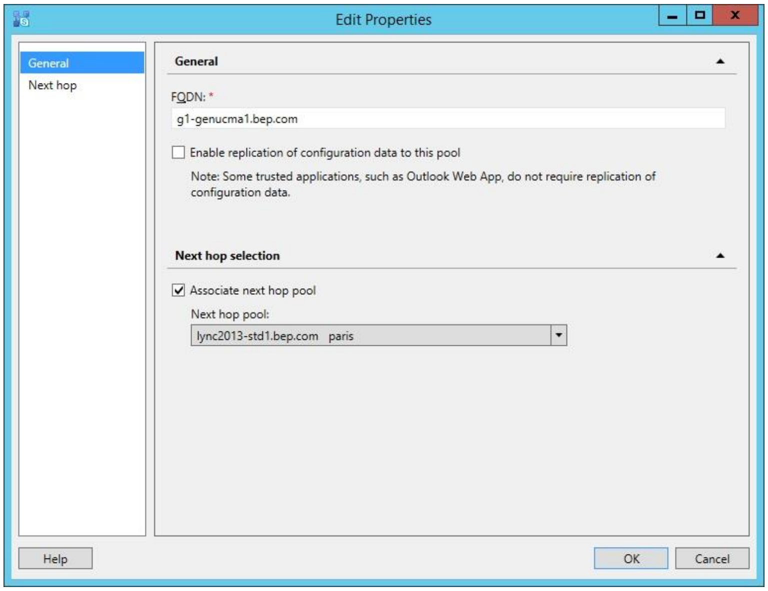
- FQDN (fully qualified domain name) and IP address of the server running the UCMA Connector.
- FQDN and IP address of the server running the SIP Server.

  Note: if using Business Edition Premise (BEP), the server may be the same for both. Using the same FQDN for both a UCMA trusted application and a gateway is not allowed in Lync or Skype for Business, however an alias can be used (another A record, or a CNAME record).
- Decide on the UCMA Connector details (Skype for Business Trusted Application).
  - Example: ID = GenUCMA1; SIP Port = 6027; MLTP Port = 6037
  - Example of a URI pattern for conference services: sip:conf-{dd}-genucma1@bep.com; number = 3
- Assign the SIP Server SIP Port – for example, 5060.

Populate the Trusted Application Pool

Using the Skype for Business Topology Builder:

1. UCMA Connector: Declare the host(s) where UCMA Connector will be running as Trusted Application Pool.
2. From the Skype for Business Server 2015 Topology Builder, go to Skype for Business Server 2015 → Trusted application servers → New Trusted Application Pool.
3. Assign the Pool FQDN with the UCMA Connector host name.
4. Select "This pool has one server (Single Computer Pool)".
5. Associate the next hop pool: the Skype for Business FE server FQDN.



General

FQDN: *
g1-genucma1.bep.com

□ Enable replication of configuration data to this pool

Note: Some trusted applications, such as Outlook Web App, do not require replication of configuration data.

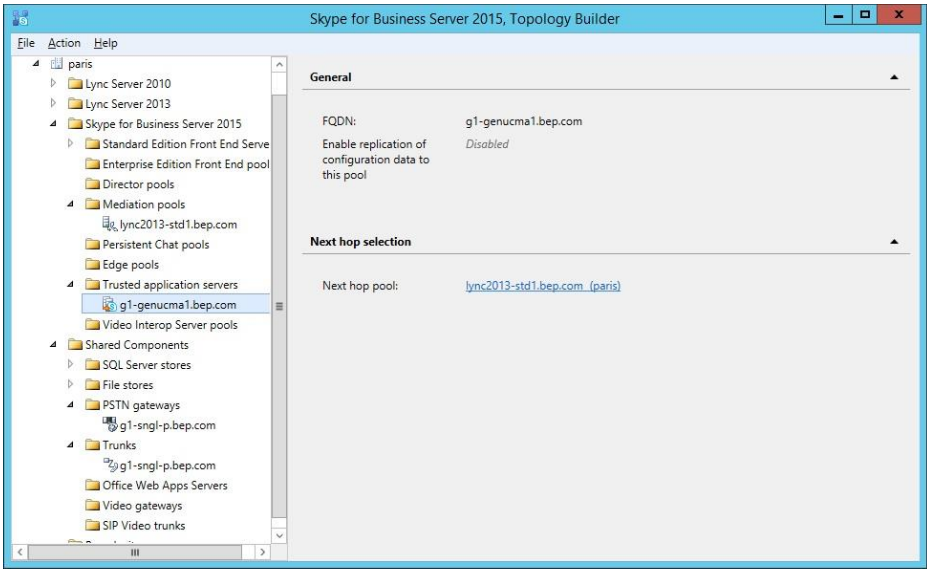
Next hop selection

☑ Associate next hop pool

Next hop pool:
lync2013-std1.bep.com paris

6. Replication is not necessary (because we use manual provisioning for the UCMA Connector Trusted Application):
   - Edit the Properties for the UCMA Connector host FQDN.
   - Keep replication of configuration data for this pool disabled.

At the end of the process, the newly created Application Pool should look like this:



General

FQDN: g1-genucma1.bep.com

Enable replication of configuration data to this pool: *Disabled*

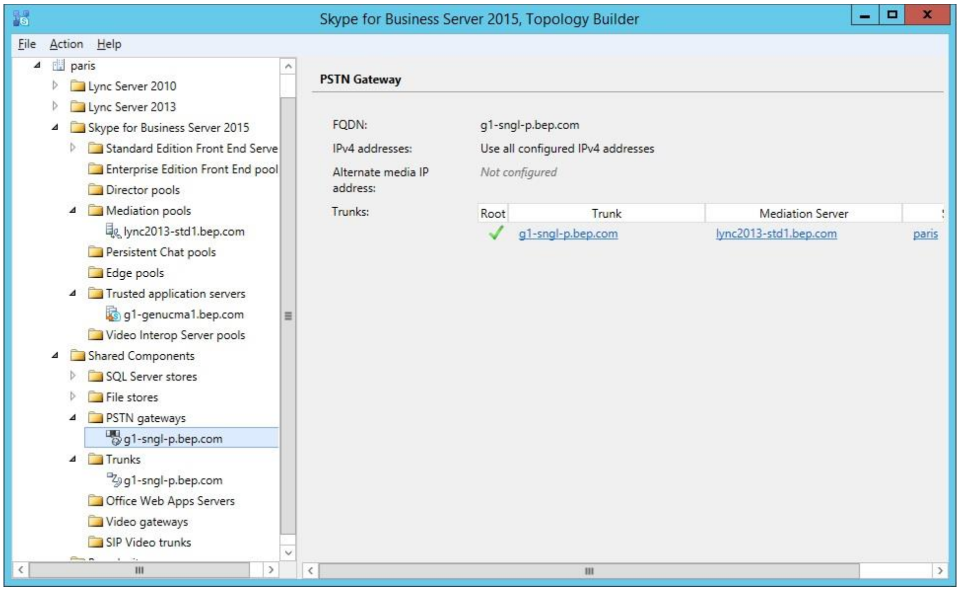
Next hop selection

Next hop pool: lync2013-std1.bep.com (paris)

Declare the SIP Server host as PSTN Gateway and provision the trunk with Lync Mediation Server

Using the Skype for Business Topology Builder, declare the host where SIP Server is running as the PSTN Gateway:

1. From the Skype for Business Server 2015 Topology Builder, go to Shared Components → PSTN gateways → New IP/PSTN Gateway.
2. Enter the FQDN of the SIP Server host.



PSTN Gateway

FQDN: g1-sngl-p.bep.com

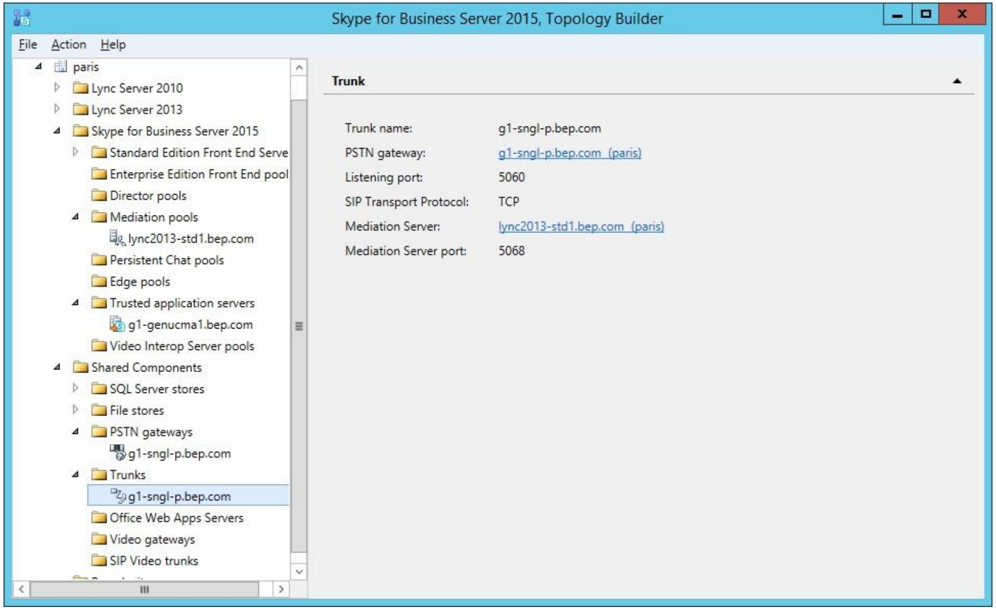
IPv4 addresses: Use all configured IPv4 addresses

Alternate media IP address: *Not configured*

Trunks:

Root	Trunk	Mediation Server	
✓	g1-sngl-p.bep.com	lync2013-std1.bep.com	paris

3. Define the root trunk:
   - Default trunk name – in the figures, *g1-sngl-p.bep.com*.
   - Listening port for IP/PSTN gateway: 5060 (the previously defined SIP Server port).
   - SIP Transport Protocol: TCP.
   - Associated the Mediation Server: FQDN of Mediation Server.
   - Associated the Mediation Server port: for example, 5068.



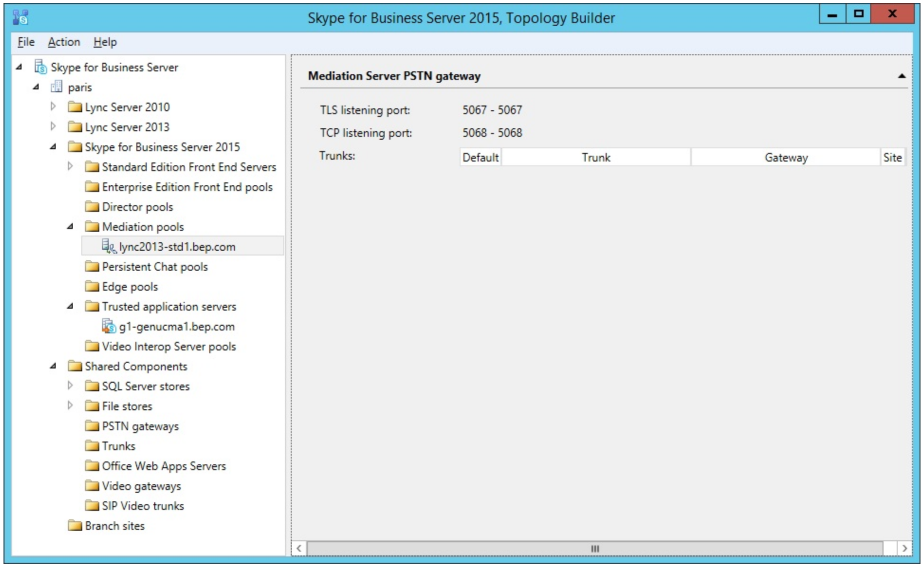
Trunk

Trunk name: g1-sngl-p.bep.com
PSTN gateway: g1-sngl-p.bep.com (paris)
Listening port: 5060
SIP Transport Protocol: TCP
Mediation Server: lync2013-std1.bep.com (paris)
Mediation Server port: 5068

Note: If TCP is not offered as a SIP transport protocol during trunk definition, it means that it has not been enabled on the Mediation Server.

To enable TCP on the Mediation Server pool:

1. Go to Skype for Business Server 2015 → Mediation Pools→ [FQDN of mediation pool] (as in the following figure):

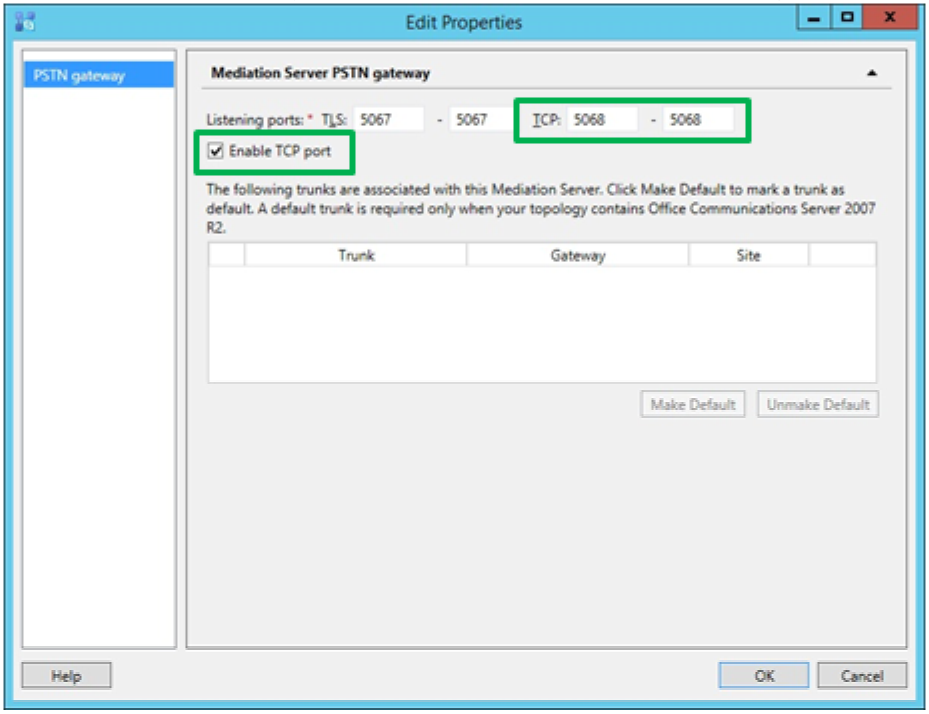


Mediation Server PSTN gateway

TLS listening port: 5067 - 5067
TCP listening port: 5068 - 5068
Trunks:

Default	Trunk	Gateway	Site

2. Select the Enable TCP port check box (as illustrated in the figure below).



Mediation Server PSTN gateway

Listening ports: * TLS: 5067 - 5067 TCP: 5068 - 5068

☑ Enable TCP port

The following trunks are associated with this Mediation Server. Click Make Default to mark a trunk as default. A default trunk is required only when your topology contains Office Communications Server 2007 R2.

	Trunk	Gateway	Site	

Publish the topology

When you publish the topology, you may have an alert in the Skype for Business Topology Builder if you have used an FQDN that was not declared as a computer in Active Directory. This may happen when you use a second A or a CNAME record used to declare the SIP Server, if it runs on the same host that UCMA Connector (see page 3 above for when this is necessary). This is not an error and can be ignored.

Define Skype for Business policies

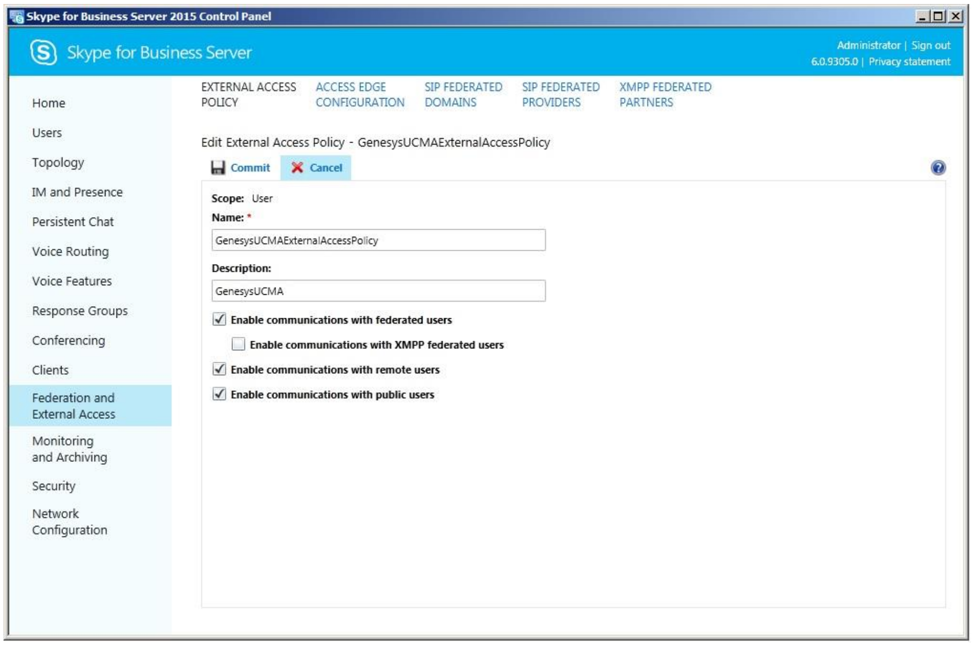
Next, you have to configure the policies that allow Multimedia Connector for Skype for Business to manage the incoming sessions and route them to agents. These include:

- Conferencing policies
- Voice policies: routes, PSTN usage
- External Access policies
- Dial plan

You can create policies using either the Skype for Business Management Shell, or the Skype for Business Server 2015 Control Panel, but you can only assign them to Trusted Application endpoints using the Management Shell.

You need to create a separate voice route and PSTN usage to direct calls to the SIP Server for media services (announcements, music, collect digits, etc.). This is prefix-based.

The following figure shows the Skype for Business Control Panel screen that is used to configure an external access policy. Note that it’s not necessary to enable communications for federated, remote, or Skype (Public) users (as is shown in the figure), if you don’t need to enable federated, remote, or Skype users to call into the system.



Edit External Access Policy - GenesysUCMAExternalAccessPolicy

Scope: User

Name: * GenesysUCMAExternalAccessPolicy

Description: GenesysUCMA

☑ Enable communications with federated users

☐ Enable communications with XMPP federated users

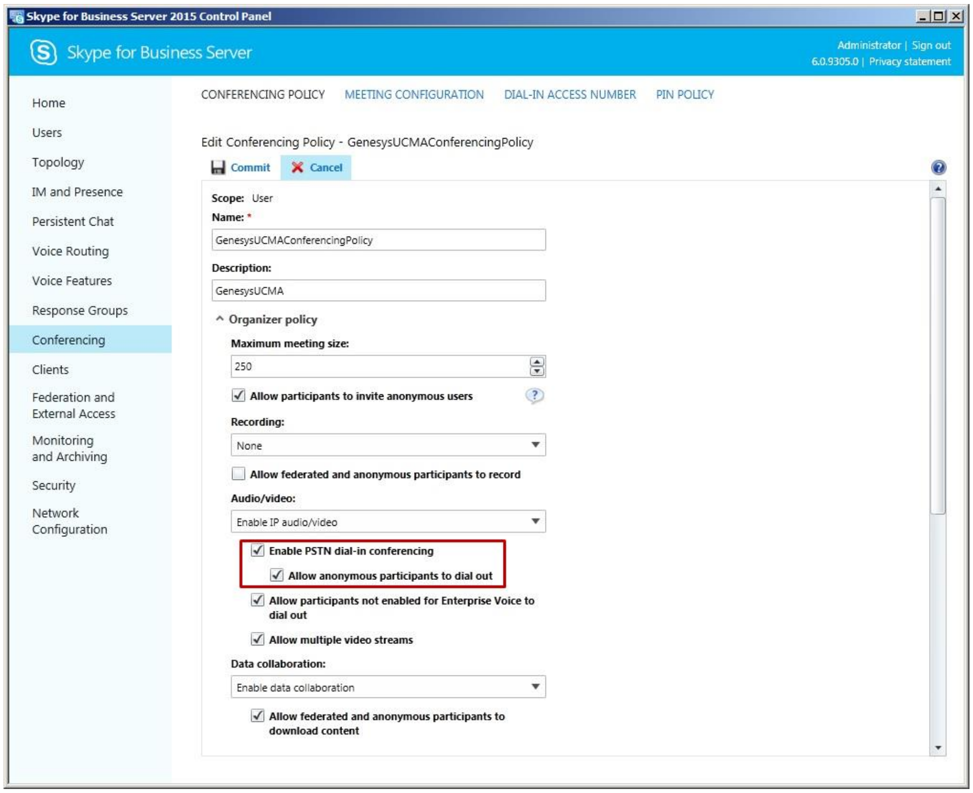
☑ Enable communications with remote users

☑ Enable communications with public users

The next figure shows an example of how to set up the conference policy for integration with the Multimedia Connector for Skype for Business.

Note that:

- The two options highlighted by the red rectangle must be selected.
- You can also disable or limit data collaboration for conferences to only the supported media (for example, voice and video).



Edit Conferencing Policy - GenesysUCMAConferencingPolicy

Scope: User

Name: * GenesysUCMAConferencingPolicy

Description: GenesysUCMA

^ Organizer policy

Maximum meeting size: 250

☑ Allow participants to invite anonymous users

Recording: None

☐ Allow federated and anonymous participants to record

Audio/video: Enable IP audio/video

☑ Enable PSTN dial-in conferencing

☑ Allow anonymous participants to dial out

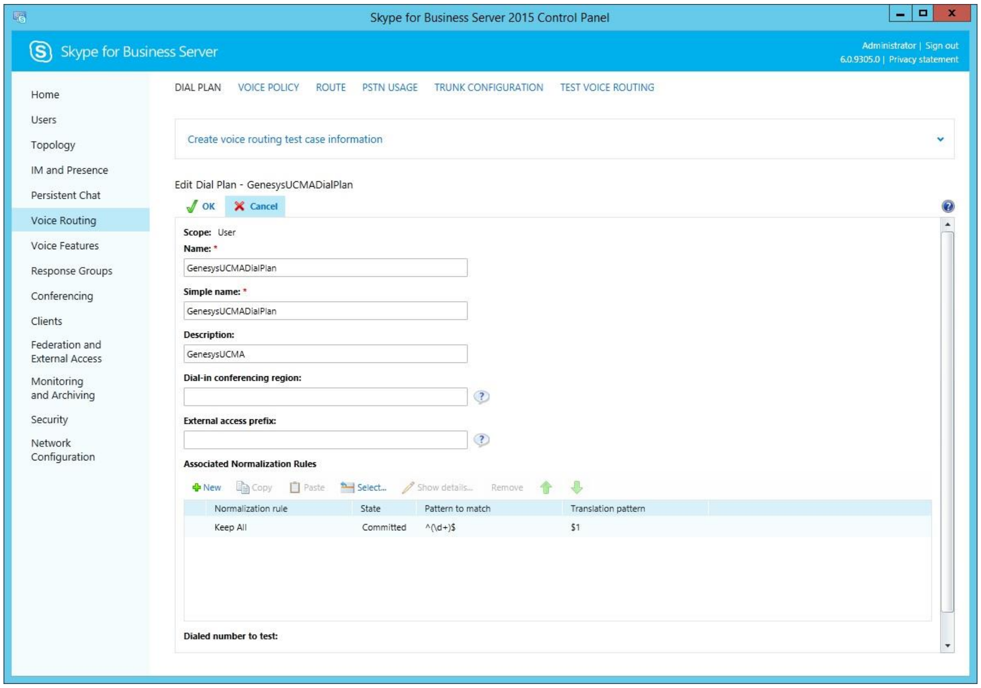
☑ Allow participants not enabled for Enterprise Voice to dial out

☑ Allow multiple video streams

Data collaboration: Enable data collaboration

☑ Allow federated and anonymous participants to download content

The next figure shows how you create a dial plan in the Skype for Business Control Panel. Skype for Business and Lync Administrators can add the necessary rules they want to apply (i.e., deployment specific) in this empty dial plan. Or they can reuse and apply existing dial plans (user level) if they have any already defined.



Edit Dial Plan - GenesysUCMADialPlan

Scope: User

Name: * GenesysUCMADialPlan

Simple name: * GenesysUCMADialPlan

Description: GenesysUCMA

Dial-in conferencing region:

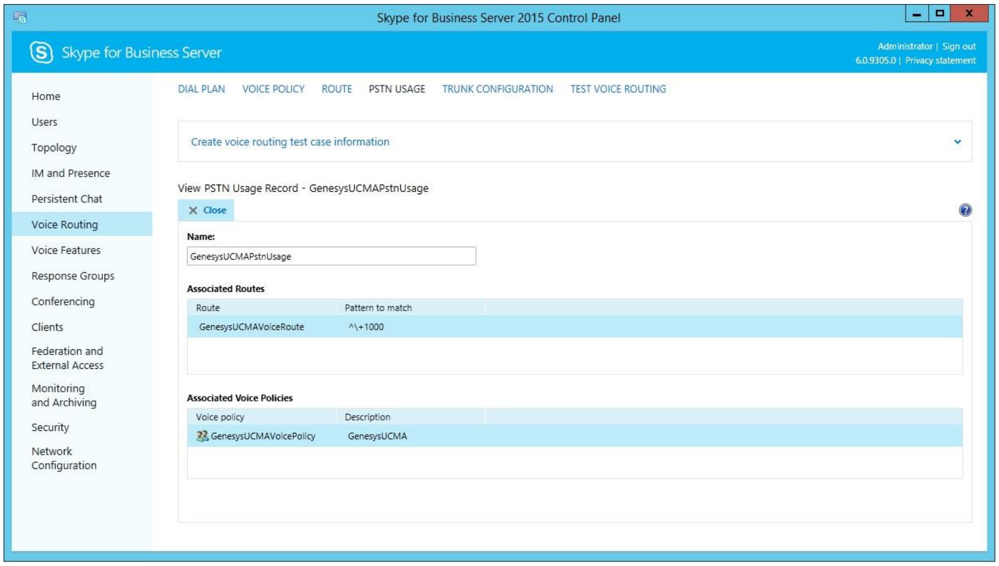
External access prefix:

Associated Normalization Rules

Normalization rule	State	Pattern to match	Translation pattern
Keep All	Committed	^(\d+)$	$1

Dialed number to test:

Another element that needs to be configured is the PSTN usage. You can create a dedicated PSTN usage record and associate it with previously created routes and voice policies, using the screen shown in the following figure.



View PSTN Usage Record - GenesysUCMAPstnUsage

Name: GenesysUCMAPstnUsage

Associated Routes

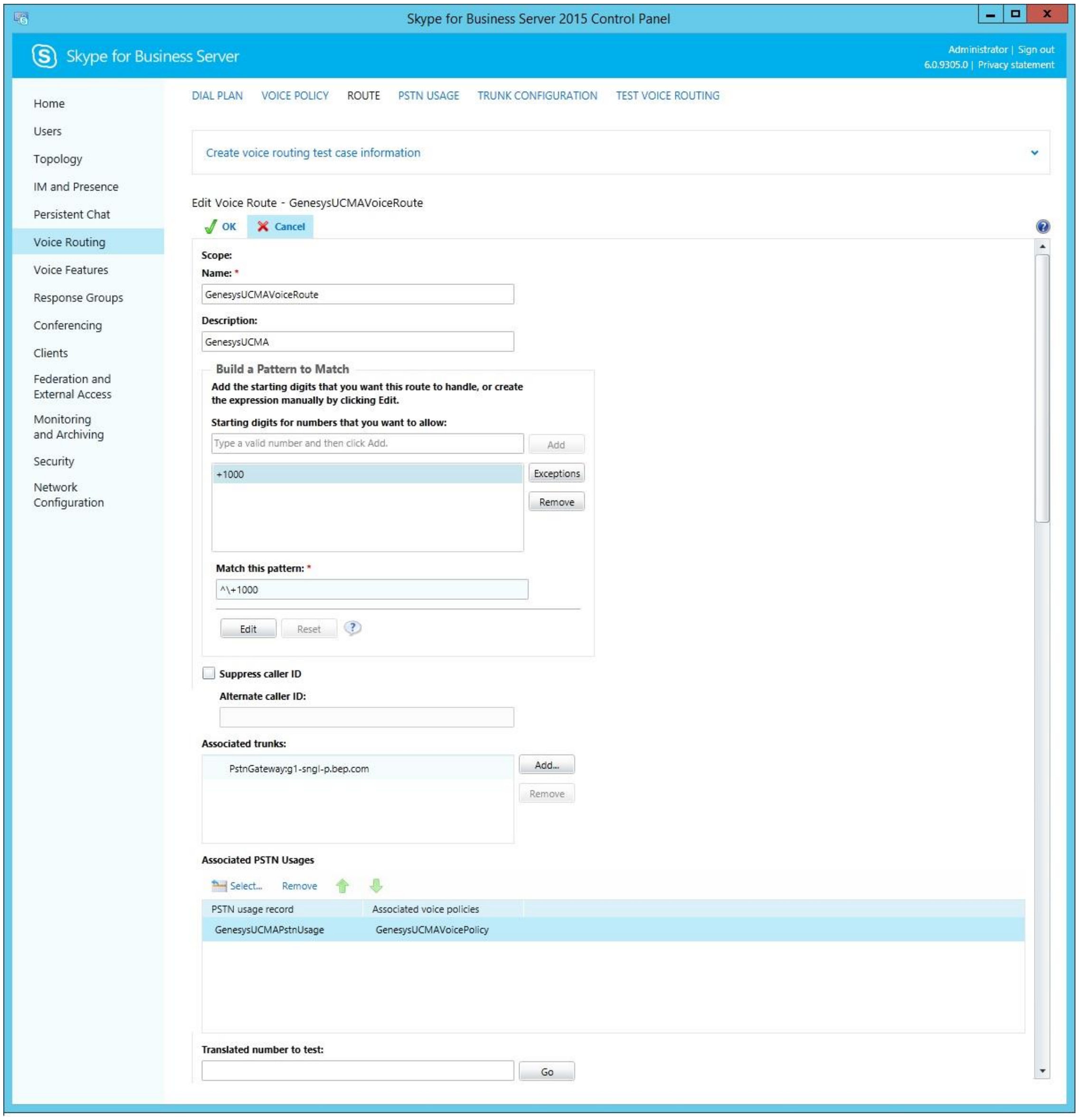
Route	Pattern to match
GenesysUCMAVoiceRoute	^\+1000

Associated Voice Policies

Voice policy	Description
GenesysUCMAVoicePolicy	GenesysUCMA

You can also create and configure a voice route using the Control Panel. In its simpler form, the voice route has a name and one or more prefixes that route the call to an associated PSTN usage and voice policy. The voice route comes in from a named trunk.

The following figure shows the window used to configure the required voice route to SIP Server (for Media Services/Treatments). The "+1000" prefix will connect the call to SIP Server.



Edit Voice Route - GenesysUCMAVoiceRoute

Scope:

Name: *

GenesysUCMAVoiceRoute

Description:

GenesysUCMA

Build a Pattern to Match

Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

Starting digits for numbers that you want to allow:

Type a valid number and then click Add.

+1000

Match this pattern: *

^\+1000

☐ Suppress caller ID

Alternate caller ID:

Associated trunks:

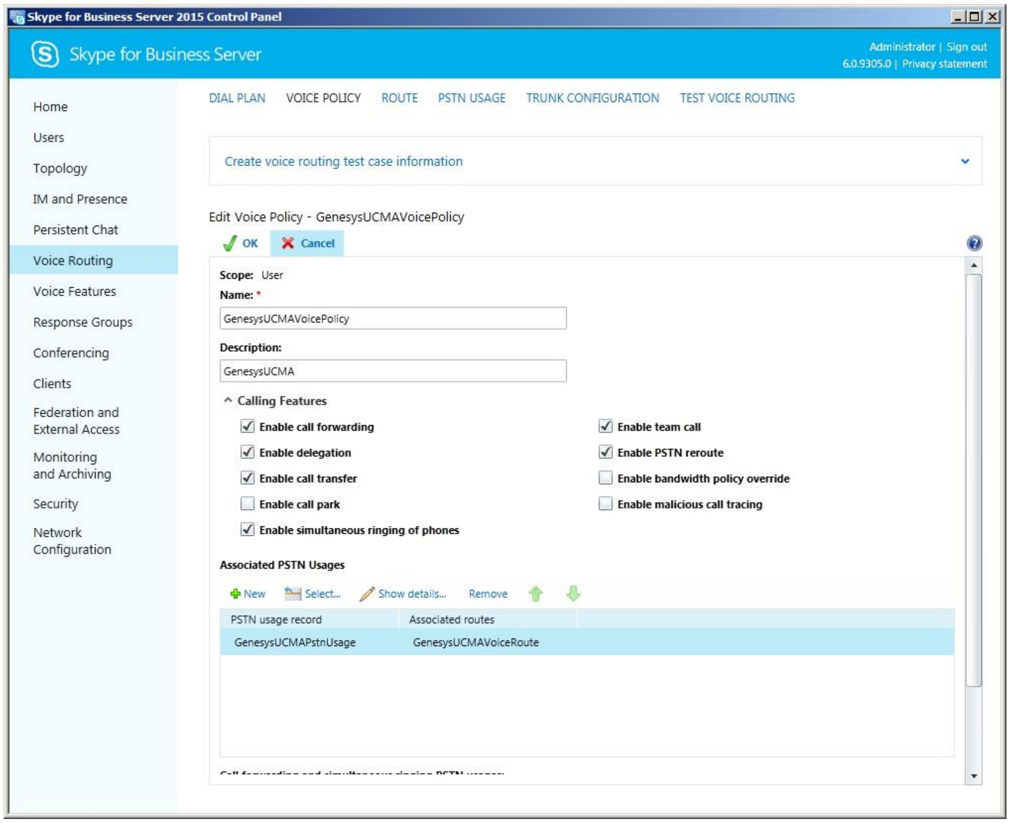
PstnGateway:g1-sngl-p.bep.com

Associated PSTN Usages

PSTN usage record	Associated voice policies
GenesysUCMAPstnUsage	GenesysUCMAVoicePolicy

Translated number to test:

A voice policy has a number of options for the services to provide for a certain PSTN usage. These are actions such as forwarding and transferring calls, enabling team calls, etc. The window used to define a voice policy and associate it with a PSTN usage is shown in the following figure.



Edit Voice Policy - GenesysUCMAVoicePolicy

Scope: User

Name: *

GenesysUCMAVoicePolicy

Description:

GenesysUCMA

Calling Features

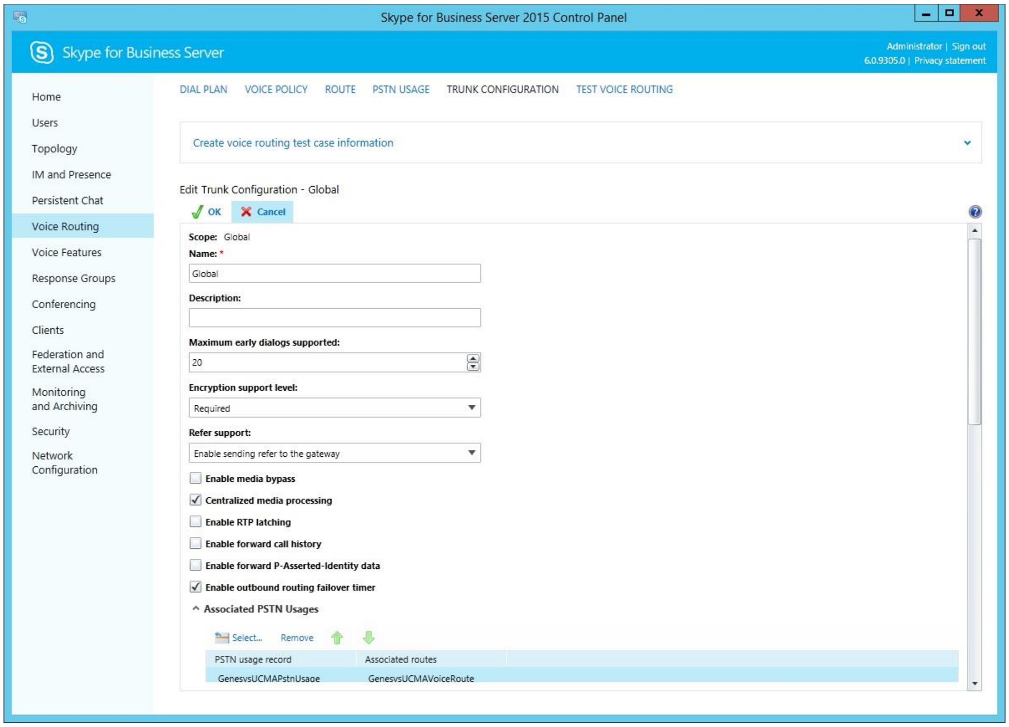
☑ Enable call forwarding	☑ Enable team call
☑ Enable delegation	☑ Enable PSTN reroute
☑ Enable call transfer	☐ Enable bandwidth policy override
☐ Enable call park	☐ Enable malicious call tracing
☑ Enable simultaneous ringing of phones	

Associated PSTN Usages

PSTN usage record	Associated routes
GenesysUCMAPstnUsage	GenesysUCMAVoiceRoute

Call forwarding and simultaneous ringing PSTN usages:

Finally, the trunk needs to be configured. The following figure demonstrates how.



Edit Trunk Configuration - Global

Scope: Global

Name: *

Global

Description:

Maximum early dialogs supported:

20

Encryption support level:

Required

Refer support:

Enable sending refer to the gateway

☐ Enable media bypass

☑ Centralized media processing

☐ Enable RTP latching

☐ Enable forward call history

☐ Enable forward P-Asserted-Identity data

☑ Enable outbound routing failover timer

Associated PSTN Usages

PSTN usage record	Associated routes
GenesysUCMAPstnUsage	GenesysUCMAVoiceRoute

Note that the SIP Server connected to the Skype for Business Mediation Server for media does not support media bypass, so that check box must be left cleared.

UCMA trusted application

The UCMA Connector for Skype for Business must be declared as a trusted application, and assigned to the previously defined Trusted Application Pool (Populate the Trusted Application Pool).

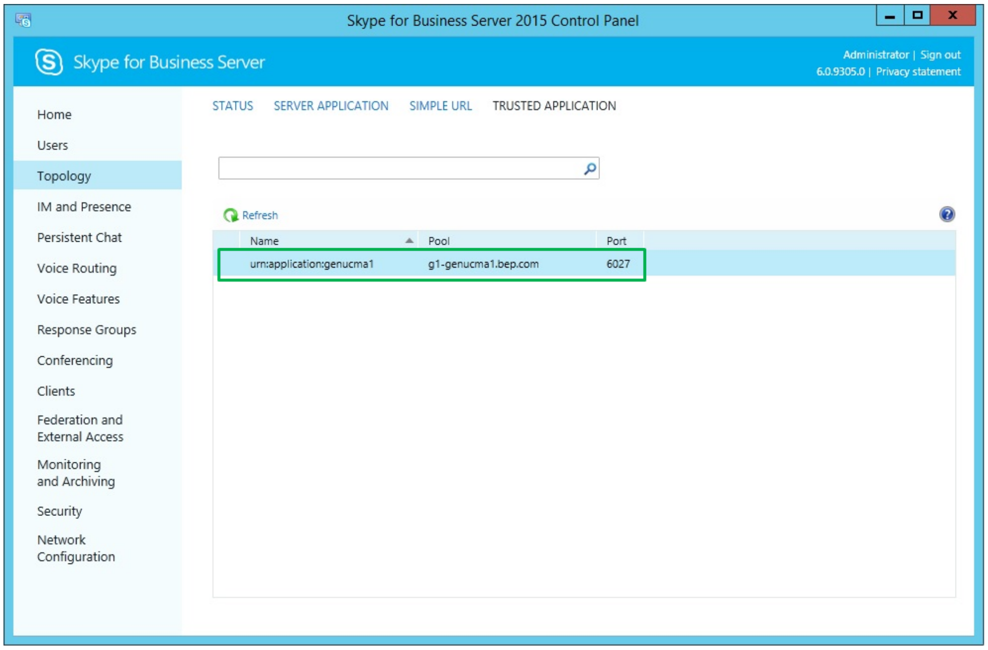
A Trusted Application must be named, and assigned a listening port. This is done through the Skype for Business (or Lync) Management shell:

- *New-CsTrustedApplication -ApplicationId* genucma1 *-TrustedApplicationPoolFqdn* g1-genucma1.bep.com *-Port* 6027
- *Enable-CsTopology*

In this example, the names and port number not in italics are given as examples.

A UCMA trusted application also needs a certificate. One should be created and assigned to the UCMA Connector to enable MTLS connectivity with the Skype for Business FE Servers.

Once you have completed the previous step and the new Trusted Application has been created, it can be seen in the Skype for Business Control Panel (under Topology, on the Trusted Applications tab), as displayed in the following figure.



Name	Pool	Port
urn:application:genucma1	g1-genucma1.bep.com	6027

Create Trusted Application Endpoints

The Trusted Application endpoints are used or Routing Points and for Conference Services.

The Trusted Application endpoints for Conference Services

Because every call in the Multimedia Connector is a conference call, these are the endpoints that manage all agent calls.
They need to be assigned a SIP URI, for example: sip:conf-*[dd]*-genucma1@bep.com, where *dd* can be any number from 00 to 99.

The Skype for Business shell commands that are needed to create these endpoints and assign them properties are:

- *New-CsTrustedApplicationEndpoint –SipAddress sip:conf-01-genucma1@bep.com -DisplayName "Pod01 Conf01" -TrustedApplicationPoolFqdn g1-genucma1.bep.com -ApplicationId genucma1 –LineURI "tel:+18654012001"*
- *Grant-CSDialplan …; Grant-CsVoicePolicy …; Grant-CsConferencingPolicy …; Grant-CsExternalAccessPolicy …* for every endpoint.

For example:
Grant-CsDialPlan -Identity "sip:conf-01-genucma1@bep.com" -PolicyName GenesysUCMADialPlan
Grant-CsExternalAccessPolicy -Identity "sip:conf-01-genucma1@bep.com" -PolicyName GenesysUCMAExternalAccessPolicy
Grant-CsVoicePolicy -Identity "sip:conf-01-genucma1@bep.com" -PolicyName GenesysUCMAVoicePolicy
Grant-CsConferencingPolicy -Identity "sip:conf-01-genucma1@bep.com" -PolicyName GenesysUCMAConferencingPolicy

You can use a script to speed up the provisioning of the endpoints.

The Trusted Application endpoints for Routing Points and External Routing Points

Genesys Route Points (RP) and External Route Points (ExtRP) will need to follow the same procedure:

- Creation using the Skype for Business Management Shell.
- Assignment of Dial-Plan and Policies using the Skype for Business Management Shell.

Take care to assign correct *-LineURI* values that match the associated DNs assigned to the corresponding RPs and ExtRPs in CME.

Certificates for the UCMA Connector

Next, you need to obtain and install SSL certificates for the UCMA Connector host. This can be done using the Microsoft Management Console (MMC), a Certificate Authority Web site, and the Skype for Business Management Shell.

On the Skype for Business Management Shell:

```
Request-CsCertificate -New -Type Default -FriendlyName "Cert_GenesysUCMA1" -CA
"dc2012r2.bep.com\bep-DC2012R2-CA" -ComputerFQDN g1-genucma1.bep.com -
PrivateKeyExportable $True -DomainName "g1-sngl-p.bep.com" -Verbose
```

Once the certificate is obtained, export it to a pfx file using MMC:

- Navigate to Certificates Snap-In → Computer Account → Local Computer → Certificates (Local Computer)\Personal\Certificates
- Export the certificate to a PFX file (select “yes, export the private key”)
  - The “Include all certificates in the certification path if possible” option should be selected.
  - The “Export all extended properties” option should be selected.

The resulting file is called Cert_GenUCMA1.pfx.

Exporting the Skype for Business information

Once you have arrived to this point, Skype for Business has been configured for integration with Genesys. You will need some of the information to configure the Multimedia Connector for Skype for Business as well. So, it’s good practice to export the configuration into a format that can be used.

Using the Skype for Business Management Shell, enter:

```
Get-CsTrustedApplication -ApplicationId genucma1 -TrustedApplicationPoolFqdn g1-
genucma1.bep.com > .\genucma1_info.txt
```

This creates a text file (*genucma1_info.txt*) with the related configuration.

Similarly, you can get information about the Trusted Application endpoint by entering the following in the Skype for Business Management Shell:

```
Get-CsTrustedApplicationEndpoint -Identity sip:conf-[nnn]-genucma1@bep.com |
Select-Object *
```

Repeat this for all endpoints.

4. Multiple UCMA Connectors

This section explains how to set up a pool of UCMA Connectors (for Lync or Skype for Business) to be seen as a single entity by the Microsoft platform. This section builds on the information about configuring a single UCMA Connector that was provided above.

In order to balance the load among UCMA Connectors, you use the DNS load-balancing feature of Skype for Business. In this scheme, requests for an FQDN can return multiple entries, and Skype for Business will send requests to one of the pool endpoints.

Creating the pool of UCMA Connectors

To create the pool of UCMA Connectors, you will use the Management Shell. You will need to separate the pool FQDN from the computer FQDN, as follows:

New-CsTrustedApplicationPool –Identity ***[the FQDN of the pool]*** *-Registrar* ***[the registrar in use]*** *-Site 1 –ComputerFqdn* ***[server 1 FQDN]***

For example:
New-CsTrustedApplicationPool –Identity genucmapool.bep.com -Registrar fe_pool1.bep.com -Site 1 –ComputerFqdn g1-genucma.bep.com

This creates a new pool FQDN and adds the first server to it. Next, you'll need to add the other servers that need to be in the pool:

New-CsTrustedApplicationComputer –Pool ***[FQDN of the newly created pool]*** *-Identity* ***[server 2 FQDN]***

For example:
New-CsTrustedApplicationComputer –Pool genucmapool.bep.com -Identity g2-genucma.bep.com

You need to repeat this for all the servers that are part of the pool. After that, you can configure the applications and endpoint in the same way as for a single server.

Note that the application GRUU (Generally Routable UA URI) must be different for each computer it is on (or for each instance of the Connector), but it should be the same as the GRUU of the computer.

Certificates

With a single server, the subject name of the certificate is the FQDN of the Application server, but with a pool it is different. With a pool, the subject name needs to be the name of the pool

FQDN. The certificate you request should be the same for all servers that are part of the pool, so you should mark the keys as exportable. As well, the certificate should contain the FQDN of the individual servers as Subject Alt Name entries. This will makes things a bit more complex when you add a server to the pool; you will have to request new certificates for that.

Please see Section 3 above for details on how to request a certificate.

DNS considerations

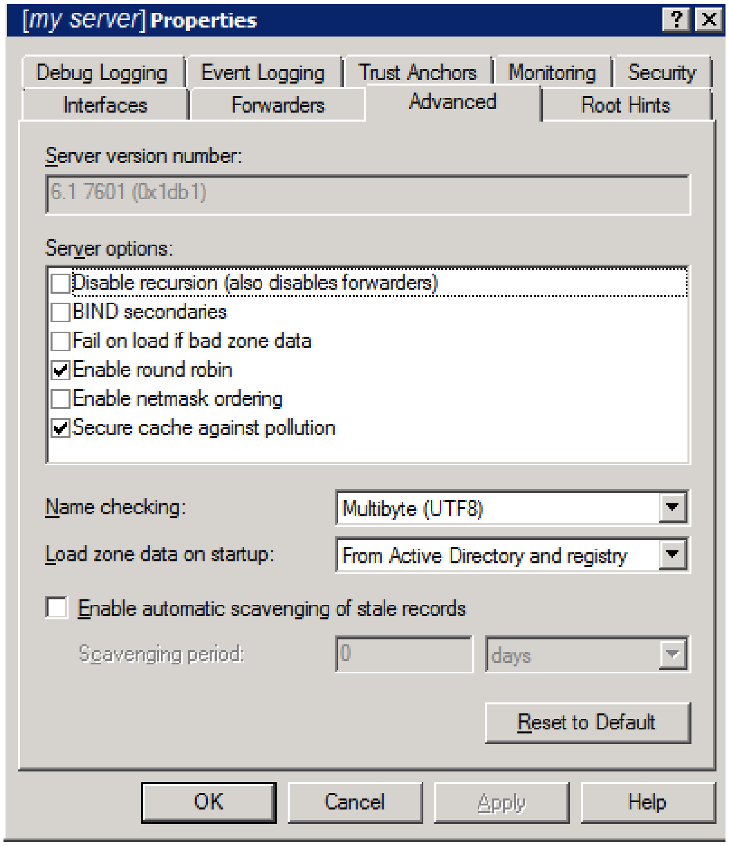
The Microsoft DNS can be used for load balancing in a UCMA environment. To load balance, you need to add entries to the DNS server table: one entry for each server and an entry for the pool that resolves to each server's IP address. We describe how to do this for the Windows Server 2008 R2 DNS server. With other implementations, the procedure can be different.

The goal is to configure the DNS server to associate all the IP addresses of the servers that compose the pool with the pool FQDN, and resolve the FQDN of the pool to point to all of the component servers in round-robin.

These settings are also required for a fast switchover if a connector is unreachable.

To load balance on a Windows Server 2008 R2 DNS server:

1. On your Windows Server, click Start→Control Panel→Administrative Tools and open DNS.
2. Right-click the server name in the tree, and select "Properties".
3. Select the "Advanced" tab.



Server version number: 6.1 7601 (0x1db1)

Server options:

- ☐ Disable recursion (also disables forwarders)
- ☐ BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☐ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

4. Ensure the following options are set properly:
   - Enable Round Robin: The Enable Round Robin check box should be selected.
   - Enable Netmask Ordering: The Enable Netmask Ordering check box should be cleared. Actually disabling netmask ordering is not essential. But it helps load-balancing, because it favors computers in your own subnet if the FQDN resolves in addresses both in the same subnet and in different ones.

Another optimization that is important for load balancing is setting the time-to-live of the DNS record to zero. For efficiency, Windows remembers the DNS lookup results for a certain time. IP addresses change rarely, so it makes sense to go directly to the same address for the same service, if you are not load-balancing. But if you are load-balancing, this is not the behavior you want.

To set the time to live of the DNS record to zero:

1. Open the DNS Manager on the Windows Server where the DNS service resides.
2. Select the View menu.
3. Select Advanced.
4. Open the pool entry that you had previously configured.
5. At the bottom of the form, set the Time to live (TTL) to 0.

This will force a re-query every time that the service is requested which will trigger the round-robin feature.