Administrator's Guide
Recording notification for SFB

telisca

Applications pour
Skype for Business

Version: 1.X

HELP
Open a ticket with your logs on http://support.telisca.com for a prompt and efficient response!
Server: MENU>Support>Zip Logs

Summary

1 Recording notification SfB description

1.1 Overview

Recording Notification makes it possible to advise the incoming callers (internal or external) that the communication will be recorded which is a legal obligation.

The warning is broadcast via an audio message at the beginning of the call, on an incoming call or outgoing call.

Recording Notification reduces administration costs, as it is based on a list of recorded numbers and is compatible with any recording application.

1.2 Architecture

Each call is trigger an MSPL services, located on each Skype for business front-end server. If one protagonist must be notified for recording, the call is rerouted towards an UCMA application. The service adds a header containing the path of an audio files that must be played. Each MSPL service request periodically from telisca server the current Recorded Notification configuration.

The UCMA application is a Windows service that is responsible for playing audio files and connecting the two calling parties in a conference. It is located on a skype for business trusted application pool.

The telisca server, running on the same server as the UCMA application manage the Recording Notification configuration and provide it to the MSPL services.
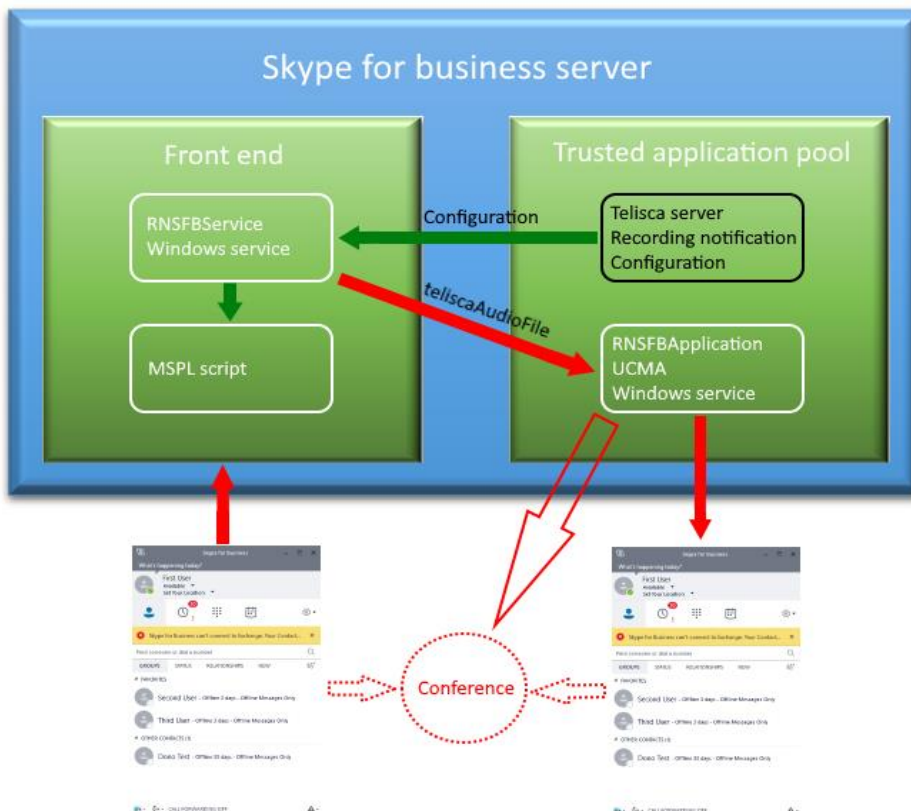
The application supports High Availability with a redundant telisca server.

1.3 Outbound scenario

In this scenario, A is the recorded line and A calls B.
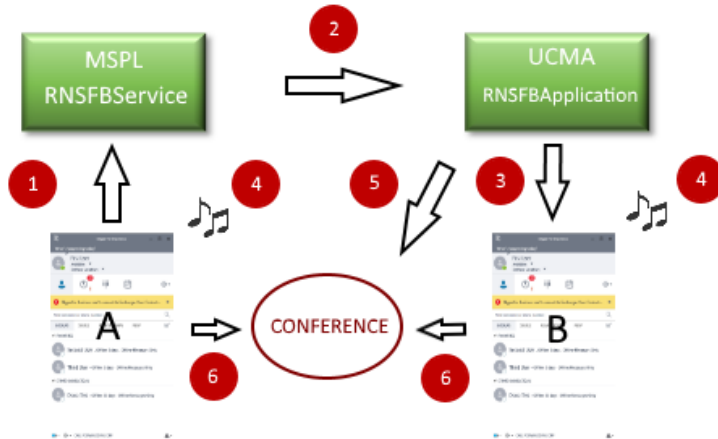
1   A calls B. The call trigger the MSPL service RNSFBService.

2   RNSFBService redirects the call towards RNSFBApplication with a "teliscaAudioFile" header.

3   RNSFBApplication calls B. A still hears the ringing tone.

4   When B answers the call, the recording notification audio file is played. In the meantime, RNSFBApplication picks answers the call from A side and plays the "outgoing call waiting audio file" in loop. (c.f. chapter 2.6)

5   As soon as the recording notification audio file is played once, the outbound call is escalated to a conference.

6   At last, A & B join the conference.

1.4 Inbound scenario

In this scenario, A calls B and B is a recorded line.

1 A calls B. The call triggers the MSPL service RNSFBService.

2 RNSFBService redirects the call towards RNSFBApplication with a "teliscaAudioFile" header.

3 RNSFBApplication answers the call and plays the recording notification audio file.

4 RNSFBApplication calls B. Meanwhile, A listens to "ingoing call waiting audio file" in loop. (c.f. chapter 2.6)

5 As soon as B picks up the call, the outgoing call is escalated to a conference.

6 At last A & B join the conference.

1.5 Requirements

- Supported Windows Servers:
- Windows Server 2012 or 2012 R2 Essentials, EN/FR,
- Windows Server 2012 or 2012 R2 Standard, EN/FR,
- Windows Server 2016 Essentials, EN or FR
- Windows Server 2016 Standard, EN or FR
- Windows Server 2019 Essentials, EN/FR
- Windows Server 2019 Standard, EN/FR

- Microsoft .Net 4.5.1 to 4.6.2
- Minimum Hardware: 1vCPU, 4GB memory (RAM) and 70GB disk.
- Supported on VMware vSphere, HyperV.

Skype for Business 2015 client is supported.

1.6 Fault tolerant operation

Recording notification SFB supports **an optional** fault tolerant operation in Hot Standby. The two server's configuration are synchronized. The MSPL services is able to connect to the backup server in case of failure.

2 Administration

2.1 Overview

Administration is Web-based and secured by an administrator's login/password.

Administration is used to define the system configuration in order to be able to interact with Skype for Business Server.

The Administration is used to define recorded lines and their associated profiles.

2.2 Login

Administration Web interface is supported with Internet Explorer 7, 8, or 9.
   Note: Internet Explorer 6 may also be used but will have some cosmetic display issues due to CSS and JavaScript limitations.

Administration URL is
http://xxx.xxx.xxx.xxx/IPSCFG/admin
or
https://xxx.xxx.xxx.xxx/IPSCFG/admin.

IPS Administration requires a local administrator login/password that must be part of the "Administrators" or "teliscaAdmin" group.
If user is part of the group "teliscaProd," he/she can only access the Assistant's and manager's subscriptions.

   Note: The administration has been designed to be used by one administrator at a time. Concurrent updates are not supported.

2.3 Administration access

telisca ▾	Skype for Business config	Recording profiles	Recorded lines
Global configuration			
Support			
Desktop Popup			
Manager Assistant SfB			
Recording Notification SfB ①			
Logout			

3   Close   Update license files

5.3.0.0
.0.0
: 5.2.1.0
: 5.2.1.0
.2.1.4
...sued to: CN=DESKTOP-SUP7UJ9.teliscatest.local. Issued by:CN:

DSKPOPUP : 16 IP Phones - Expiration date : No limit - Version :
IPSFT : HOT STANDBY - Expiration date : No limit
MAS4B : 30 IP Phones - Expiration date : No limit - Version :
Recording Notification - Skype for Business : 16 IP Phones - Expiration date : No limit - Versio
Copyright telisca 2004-2018

① Configuration access to recording notification for skype for business

2.4 General configuration

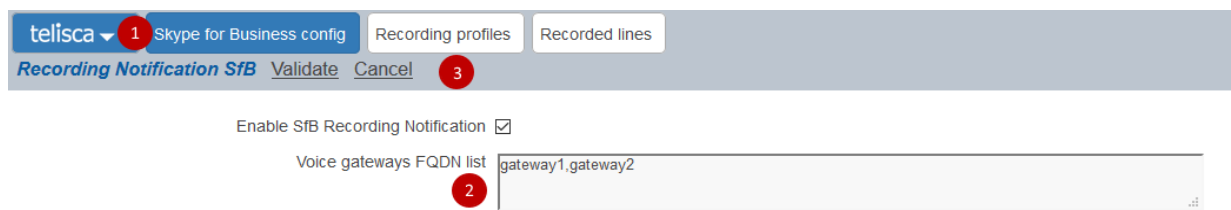| 1	Button to access general configuration
2	List of voice gateways that will considered as internal by the application. The list is comma separated.
3	Validate or cancel changes.

2.5 Profiles list

Recording notification for skype for business uses profiles to configure notification behavior. Hence, multiple users can have the same profile
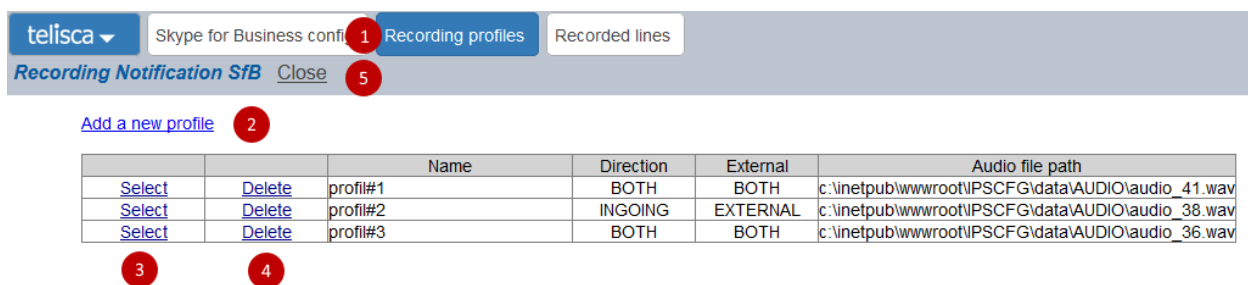
1	Button to access profiles list
2	Allows the creation of a new profile (c.f. 2.6 Profile)
3	Allows the current profile update or display (c.f. 1.6 Profile)
4	Delete the current profile
5	Close the current screen

2.6 Profile

This screen is displayed by selecting an existing profile, or creating a new one (c.f. 1.5 Profiles list)

Profile name. Each profile name should be unique.

2 Decides if ingoing calls, outgoing calls, or both will be notified on the recorded line.

3 Decides if internal call, external call or both will be notified on the recorded line. To specify if a call is internal or external, c.f. 2.4. General configuration

4 Audio message played at the called party member that is not aware of the recording.

5 When calling a recorded line, and after playback of the recording notification, audio message played while waiting for the called party to pick up.

6 When a recorded line makes a call, audio message played while the called number is listening to the recording notification message.

7 One can choose several languages; each text or uploaded file will be played one after another.

8 Select the language and specify the text that will be interpreted by Text to Speech.

9 Or upload an existing audio file.

10 the interpreted text or downloaded audio file can be listened to.

11 Validate or cancel changes made to the profile.

2.7 Recorded lines configuration

This screen allows you to specify a text file path, accessible via a network path in which the application will read a list of recorded lines, as well as their associated profile. The file must be a CSV text file, semi-colon separated.

1 Button to access the recorded lines configuration.

2 Path to the text file.

3 Credentials used to connect to network folder.

2.8 Recorded lines

1. Button to access the recorded lines.

2. This button refreshes and displays the content of the file configured in the configuration screen (c.f. chapter 2.7).

3. Current file content.

4. Close the current screen.

2.9 Backup of configuration data

System and user configuration data are stored in files with « .xml » or « .bin » extension located in sub-directories « data » of the different virtual directories associated to Telisca applications (by default : "C:\inetpub\wwwroot\IPSCFG\data\").

> **Note**: the system configuration is saved in an XML file IPSCFG_cfg.xml, in "C:\inetpub\wwwroot\IPSCFG\data". A copy of this file is saved each night with an YYMDD postfix. Older files are purged after 14 days.

In case of multi-cluster installation, following directories must be back up too:
- directory "c:\inetpub\wwwroot\MCADMIN\data»;
- directory "data" of each cluster, example "c:\inetpub\wwwroot\01\IPSCFG\data", "c:\inetpub\wwwroot\02\IPSCFG\data".

Backup of all these directories do not require to stop the applications.

2.9.1 Restoring configuration data

Data can be restored by a simple copy to their original place.

Configuration data in « .xml » files are automatically reloaded on detection of a file update. Data of other configuration file types are reloaded at ASP.Net applications start up (after a restart of the « World Wide Web publication Service »).

2.9.2 Application backup, reinstallation

All the applications are installed in IIS directory (default is c:\inetpub\wwwroot):

- C:\inetpub\wwwroot\IPSCFG

To back up all the applications and their data, both directories listed here-above must be saved.

To ease reinstallation, it is recommended to also back up the Setup and license files used to install the application as well as any installed patch files.

In this case, a restore process on a fresh server would be as follows:

- Reinstall IIS
- Reinstall .Net 4.5
- Run SETUP, which will ask for the license files
- Copy patched DLL in the correct directories (search file in installed directories)
- Copy backup data in C:\inetpub\wwwroot\IPSCFG\data
- Start telisca IPS Startup Service and telisca CTI Server service

Another solution as an alternative to a complete re-installation is to perform a disk image. This image can be reinstalled on another machine without any limitation due to the license; indeed, the license is not bound to any hardware parameter of the machine, as the disk where the installation is performed or the network card.

The applications can run under a virtual machine VMWare ESX. In such case, it is possible to create a snapshot which can be restarted on another server.

2.9.3 Debugging, support

All application processes descriptions are saved in log files.

The administration log files are located in "c:\inetpub\wwwroot\instance\IPSCFG\logs\IPSCFGAdminXXX.log"
The web service log files are located in "c:\inetpub\wwwroot\instance\IPSCFG\logs\ IPSCFGWSXXX.log"

The RNSFBApplication log files are located in the folder "logs" where the application was installed.
The RNSFBService log files are located in the folder "logs" where the services were installed, **on each front-end**

3 Installation on Skype for Business server

The goal is to install a windows service on each front-end server and the trusted application pool.

There are 3 steps during the installation

1. Installation of a trusted application pool.
2. Installation of RNSFBApplication on this trusted application pool.
3. Installation of RNSFBService on each front-end.

The installation of the trusted application pool is done manually.
For points 2 and 3 the installation can be done automatically, semi-automatically or manually.

The application delivered contains three folders: RNSFBApplication and RNSFBService, related to the UCMA and MSPL part of the application, and RNSFBInstaller that contains the global installer.

3.1 Installation of a trusted application pool

Please refer to Microsoft Documentation

3.2 Manual installation on Skype for Business server

Here is the description for a full manual installation.

3.2.1 UCMA application topology.

First, create the trusted application using the previous trusted application pool.

New-CsTrustedApplication -ApplicationId "urn:application:notificationrecordingapp" -TrustedApplicationPoolFqdn "trusted_application_pool_fqdn" -Port 15001	
trusted_application_pool_fqdn	Trusted application pool FQDN

Then, create an application endpoint

New-CsTrustedApplicationEndpoint -ApplicationId "urn:application:notificationrecordingapp" -TrustedApplicationPoolFqdn "trusted_application_pool_fqdn" -SipAddress "sip:teliscaRNSFB@domain" -DisplayName "RNSFBApplication"	
trusted_application_pool_fqdn	Trusted application pool FQDN
domain	Domain name

3.2.2 UCMA application user and service.

Create an AD user that will log on to the service.

New-AdUser "user_name" -Enable $True -accountPassword(ConvertTo-SecureString -AsPlainText "user_password" -Force) -PasswordNeverExpires $True -UserPrincipalName user_name@domain	
domain	Domain name
user_name	AD user created
user_password	AD user password

This user has restricted local rights. He must be granted the following:

- **RTC Component Local Group**: Includes service accounts used to run A/V Conferencing Servers, Web Services, Mediation Server, Archiving Server, and Monitoring Server.
- **RTC Local Administrators**: RTC domain server administrators get local Central management database access
- **RTC Local Config Replicator**: Skype for Business replication services are granted permission to participate in Skype for Business replication
- **RTC Local Read-Only Administrators**: Get local central management database access
- **RTC Local User Administrators**: get local DCOM permissions
- **RTC Server Applications**: Skype for Business Server applications are granted appropriate local permissions
- **RTC Server Local Group**: Grant access to Skype for Business Server settings (not to pool settings).

```
net localgroup "RTC Component Local Group" domain\user_name /add
net localgroup "RTC Local Administrators" domain\user_name /add
net localgroup "RTC Local Config Replicator" domain\user_name /add
net localgroup "RTC Local Read-Only Administrators" domain\user_name /add
net localgroup "RTC Local User Administrators" domain\user_name /add
net localgroup "RTC Server Applications" domain\user_name /add
net localgroup "RTC Server Local Group" domain\user_name /add
```

user_name	AD user created
domain	Domain name

Put the RNSFBApplication folder delivered with the binaries at an appropriate location on the server that belonged to the trusted application pool. Then install the service:

```
sc create RNSFBApplication binpath="service_location\RNSFBApplication.exe"
DisplayName= "telisca Recording Notification for Skype for business" obj=
"domain\user_name" password= "user_password" start= auto
```

service_location	Folder containing the service RNSFBApplication
user_name	AD user created
user_password	AD user password
domain	Domain name

The AD user must be granted full access to the chosen service location.

```
icacls "service_location" /grant "domain\user_name:(OI)(CI)F" /T
```

user_name	Local user created
service_location	Folder containing the service
domain	Domain name

One can launch the service:

```
sc start RNSFBApplication
```

3.2.3 MSPL topology

On each skype for business pool, an MSPL script must be declared.

The RNS4B MSPL script must be run with a lower priority than UserServices, usually 4.
In order to get the UserServices priority, one can execute this PowerShell command:

```
Get-CsServerApplication
```

For instance, here it is for the pool pool_name:

```
Identity     : Service:Registrar:pool_name/UserServices
Priority     : 4
Uri          : http://www.microsoft.com/LCS/UserServices
Name         : UserServices
Enabled      : True
Critical     : True
ScriptName   :
Script       :
```

Then, one can register RNS4B script with skype topology using the following command. Note that it takes the previous priority, and must be launched **for each pool**:

```
New-CsServerApplication -Identity "Service:Registrar:pool_name/RNS4B" -Uri
"http://telisca.com/RNS4B" -Critical $False -Enable $True -Priority userservices_priority
```

pool_name	Pool on which the script is installed
userservices_priority	UserServices priority on this pool

3.2.4 MSPL user and service

On each front-end one must create a local user

```
net user user_name user_password / add
```

user_name	Local user created
user_password	Local user password

This user has restricted local rights. He must be granted the following:

```
net localgroup "RTC Component Local Group" user_name /add
net localgroup "RTC Local Administrators" user_name /add
net localgroup "RTC Local Config Replicator" user_name /add
net localgroup "RTC Local Read-Only Administrators" user_name /add
net localgroup "RTC Local User Administrators" user_name /add
net localgroup "RTC Server Applications" user_name /add
net localgroup "RTC Server Local Group" user_name /add
```

user_name	Local user created

Select a location on each front-end and put the RNSFBService folder.
Then install the service:

```
sc create MASFBService binpath="service_location\MASFBService.exe" DisplayName=
"telisca Manager Assistant Skype for business" obj= ".\user_name" password=
"user_password" start= auto
```

service_location	Folder containing the service
user_name	Local user created
user_password	Local user password

Grant the user the corresponding rights to MASFBService folder (PowerShell syntax)

```
icacls "service_location" /grant "user_name:(OI)(CI)F" /T
```

user_name	Local user created

service_location	Folder containing the service

One can launch the service:

```
sc start RNSFBService
```

Finally, in the data folder, a configuration file settings.json has been created and needs to be configured. The process is described on chapter 3.5 and 3.3.2.

3.3 Semi-automatic installation on Skype for Business server

Here is a description of a semi-automatic deployment. Each executable RNSFBApplication.exe and RNSFBService.exe can take parameters and commands that allows a faster and secure installation.

3.3.1 UCMA installation

RNSFBApplication usage syntax, with parameters

RNSFBApplication.exe -command /flags user_name user_password	
command	{install, uninstall, help}
flags	{u, o, s, r}
user_name	AD user
user_password	AD user password

Available commands :

install	Will install the application at the current location
uninstall	Will uninstall the application
help	Shows help

Only the install command is interesting in this part. Here is a list of available flags :

u	Will create the AD user with appropriate permissions
o	Will create the trusted application on skype topology
s	Will install the windows service
r	Launch the service

For instance, the command lines including in 3.2.1 and 3.2.2 chapters are equivalent to the following :

```
RNSFBApplication.exe -install /uosr user_name user_password
```

3.3.2 MSPL installation

RNSFBService usage syntax, with parameters

RNSFBService.exe -command /flags user_name user_password	
command	{install, uninstall, help, settings}
flags	{u, s, r}
user_name	Local user
user_password	Local user password

Available commands:

install	Will install the application at the current location
uninstall	Will uninstall the application
settings	Prompt the user and create a new configuration file
help	Shows help

Only two commands are interesting in this part. The settings command, that takes no flag; and the install command. Here is a list of available flags:

u	Will create the local user with appropriate permissions
s	Will install the windows service
r	Launch the service

As MSPL script is pool related, the skype topology is not changed by the current executable that is launched on a specific skype for business front-end server. The MSPL script referencement is done during the automatic installation, in the next chapter.

Concerning the settings command, here is the prompt given to the user :

```
C:\SkypeShare\Release\RecordingNotification>rnsfbservice -settings
Enter primary host: http://server1/instance
Enter secondary host: http://server2/instance
Enter timeout (ms) [default:1500]:
Enter fault tolerance periode (ms) [default:30000]:
Enter the service GRUU of the UCMA application: sip:srvskype05.teliscatest.local
@teliscatest.local;gruu;opaque=srvr:notificationrecordingapp:60FFwfq_UFOl17IApAT
C7AAA
Command settings completed successfully
```

A complete description of these settings is available in chapter 3.5
In order to reproduce manual steps in 3.2.4 one can run:

RNSFBService.exe -settings
RNSFBService.exe -install /usr user_name user_password

3.4 Automatic installation

The following installation needs to be run as a domain administrator.
Unzip the whole package on a skype for business server, with powershell installed with the skype and AD module.

Then run the following command:

```
RNSFBInstaller.exe -install
```

The skype topology is explored and the user will be prompted:

- Service configuration.
- In which pool install RNSFB.
- Install location on Skype frontends for both UCMA and MSPL part
- User login and password for RNSFBService and RNSFBApplication

For more details about service configuration, see chapter 3.5
Finally, all created services on each frontend pool selected will be launched. The UCMA application will also be launched.

3.5 Service configuration

HOST_1	URL to primary telisca server.	string
HOST_2	URL to secondary telisca server (redundancy)	string
FT_PERIOD	Time between two KEEP_ALIVE to telisca server	integer
TIMEOUT	Timeout for http request to telisca server	integer
DEBUG	Will trace SIP requests content on log files	boolean
UCMAServiceGRUU	Parameter of the installed UCMA application	string

Concerning the parameter UCMAServiceGRUU, it will be known after the creation of the UCMA application on skype topology. It is not required during automatic installation, cause the installer get it after creating it. But it will be mandatory to launch the following command for both manual and semi-automatic installations :

```
Get-CsTrustedApplication -Identity
"server_trusted/urn:application:notificationrecordingapp"
```

server_trusted	UCMA application server

This should return the RNSFBApplication description on skype topology:

```
Identity                     : srvskype05.teliscatest.local/urn:application:notificationrecordingapp
ComputerGruus                : {srvskype05.teliscatest.local
                               sip:srvskype05.teliscatest.local@teliscatest.local;gruu;opaque=srvr:notificationrecordingapp:60FFwfq_UFOl17IApATC7AAA}
ServiceGruu                  : sip:srvskype05.teliscatest.local@teliscatest.local;gruu;opaque=srvr:notificationrecordingapp:60FFwfq_UFOl17IApATC7AAA
Protocol                     : Mtls
ApplicationId                : urn:application:notificationrecordingapp
TrustedApplicationPoolFqdn   : srvskype05.teliscatest.local
Port                         : 15001
LegacyApplicationName        : notificationrecordingapp
```

3.6 Update of an existing solution

3.6.1 Automatic update

RNSFBInstaller is delivered with an upgrade process:

```
RNSFBInstaller.exe -update
```

it will ask the user on which pools the MSPL service update should be done. It will asks also for the UCMA application.
The interruption of service is minimal, between 5s and 10s on each server.

3.6.2 Manual update.

On each frontend server

- stop the service RNSFBService.
- overwrite the RNSFBService folder with the new content.
- Restart the service RNSFBService.

On the trusted application server

- Stop the service RNSFBApplication
- overwrite the RNSFBApplication folder with the new content.
- Restart the service RNSFBApplication.