ShoreTel
Brilliantly simple™

ilink
computer meets telephone

Advanced Troubleshooting Guide for ilink Microsoft Lync ShoreTel CSTA Server

Release 1.5

ilink Kommunikationssysteme GmbH
Charlottenstrasse 4
10969 Berlin, Germany
+49 (30) 285 26-0
www.ilink.de/en

March 2015
Software release 1.5, document revision 4

Contents

1. Introduction

This document assumes familiarity with the documentation describing product installation and configuration:

- *ShoreTel CSTA Server Planning and Installation Guide*
- *Microsoft Lync Server 2010 Deployment Guide or Lync Server 2013 Deployment Guide*

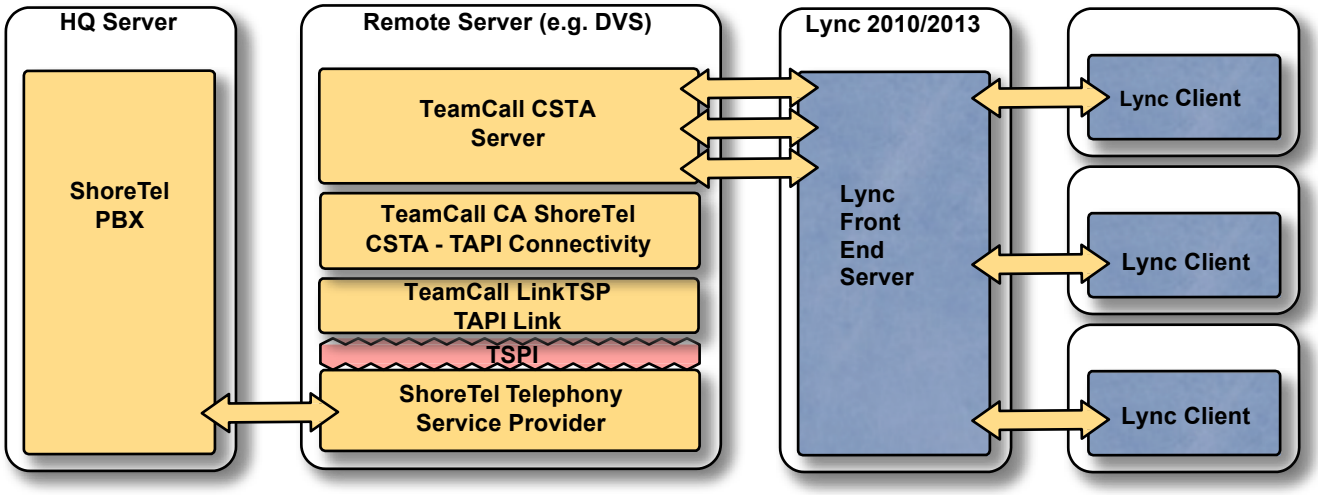
Read these documents carefully as they provide enough information to find and fix the most common issues. This document is intended to be used as an advanced troubleshooting guide for administrators and support professionals with experience in troubleshooting MS Lync 2010 and 2013 environments. It suggests strategies and techniques for resolving problems with deployments of ShoreTel CSTA Server with a specific focus on Lync Server 2010.

The following terms and abbreviations are used in this document.

Term	Definition
Lync FE	Microsoft Lync Server 2010 / 2013
Lync client	Microsoft Lync desktop PC client
CA	Connectivity Adaptor
LinkTSP	Link TAPI Service Provider
AD	Active Directory
DVS	Distributed Voice Server, also known as a TAPI Application Server

2. The Environment

Various components are involved in the process of integrating the CSTA telephony capabilities.



Each of these components needs to be properly configured and for each of these components it is possible that configuration settings lead to a failure:

- ShoreTel System
- ShoreTel CSTA Server components (installed on a TAPI Application Server or DVS)
- Microsoft Lync Server 2010/2013 Standard Edition
- Microsoft Lync Client 2010/2013
  Lync 2013 Basic clients are not supported.
  For Lync 2013 clients the Lync 2013 update 15.0.4551.1005: November 7, 2013 must be installed.

There are additional components - like Microsoft Active Directory or Microsoft SQL Server, Domain controllers etc., which are implicitly used. The proper configuration for these additional components is assumed. This document focuses on the ShoreTel IP phone remote call control integration aspect only. The assumption is that Lync users are already configured for Lync usage in Active Directory.

3. Troubleshooting Strategy

The approach for narrowing down an RCC issue depends on the context:

- Initial Phone Integration (“first time”) – does not work
- Existing Phone integration environment (partially) stopped working

3.1 Existing Phone Integration

Choose a top down approach:

- Check Lync settings regarding “RCC (remote call control)”
- Global settings like static routing (Get-CsStaticRoutingConfiguration)
- User specific settings like telURI, User is set up for Remote Call Control
- Check CSTA settings
- General system availability
- Licensing
- Valid extension

3.2 Initial Phone Integration

Choose a bottom up approach

- Check CSTA settings
- General system availability
- Licensing
- Valid extension
- Check Lync Server settings regarding “RCC (remote call control)”
- Global settings like static routing, trusted application
- If Lync user specific settings like Line URI are in canonical format (+14085551212), corresponding Extension Translation Table entries need to exist in DialPlan.conf.
- Remote call control must be enabled Line URI sip:callcontrol@<domain>.com

3.3 Ruling Out User Error—Dialing Formats

Users may complain that they are unable to dial certain numbers. Before commencing troubleshooting of the configuration, first confirm that the user is entering the numbers to be dialed correctly and that numbers entered into directories and databases being used are correctly formatted.

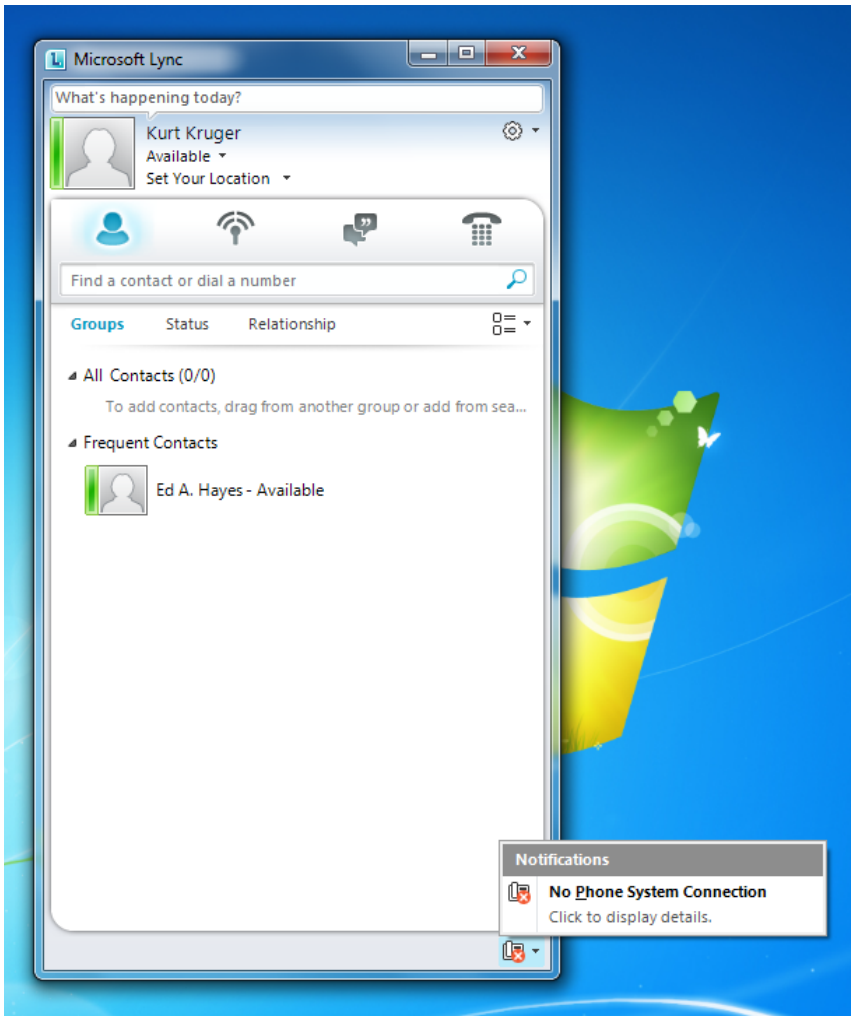
Lync numbers must be in a canonical format, for example, +14085551234

4. Lync Client Diagnostics

The Lync client knows three different states regarding the phone integration. The two failure states are immediately reflected by visual feedback within the GUI, but in the normal state there is nothing visible in the Lync client.

Fail State 1: Phone Integration Not Enabled

In this case the Lync client shows an error notification icon at the bottom right corner of the window:



Phone System Error

More information about the error is displayed via the ***info icon***. Clicking on the Notification item will open a window with more detailed information about the error.

Fail State 2: Phone Integration Enabled but Phone System Error Occurred

In this case the Lync client also shows an error via the ***info icon*** at the bottom right corner of the window.

Symptoms of this scenario are the ***Info icon*** indicates a failure “No Phone System Connection”

Cause: Lync or CSTA environment not properly configured

Solution: Verify Dial plan in CSTA server. Verify client is pointed at the right trusted application pool. Verify the static routing configuration is correct. Verify that the CSTA Services are running on the CSTA Server host.

5. CSTA Diagnostics

The ShoreTel CSTA Server consists of three subcomponents

- TeamCall CSTA Server – the CSTA Server
- TeamCall CA ShoreTel – Connectivity Adaptor
- TeamCall LinkTSP – TAPI bridge

Each of these software components runs as a distinct Microsoft Windows System Service, so first check to be sure that all of these services are up and running (this is explained below).

Note: The term "CSTA Server" generally refers to the top level component which is the TeamCall CSTA Server system service. The other two components (TeamCall CA ShoreTel and TeamCall LinkTSP) do not expose "public capabilities" and are only used internally by the TeamCall CSTA Server component.

5.1 Diagnostic Session Facilities

The CSTA Server has two built-in diagnostics session facilities. Both of them are accessible using a standard Telnet program such as the one included with the Microsoft Windows operating systems.

Note: In the examples of Telnet use in this manual the address of the server is specified as the loopback address **localhost** to illustrate Telnet running on the same host as the CSTA server. Telnet could be running on an computer with network access to the CSTA server which would then be identified by its IP address.

Note: These examples also use the default value of the CSTA server's port number which is 26535. A different port number can be configured for the CSTA server by changing the appropriate entry in the CSTA server's *Default.conf* configuration file. (This is described later in this manual.)

The SuperVisor Session

The SuperVisor session can be used to check licensing, PBX reachability, and version information.

```
telnet localhost 26535
SuperVisor
BYE
```

(connects to the CSTA Server)
(login to a SuperVisor session)
(ends a SuperVisor sessions)

The STLI Session

The STLI session can be used to check basic telephony features (e.g. device monitors).

```
telnet localhost 26535
STLI
BYE
```

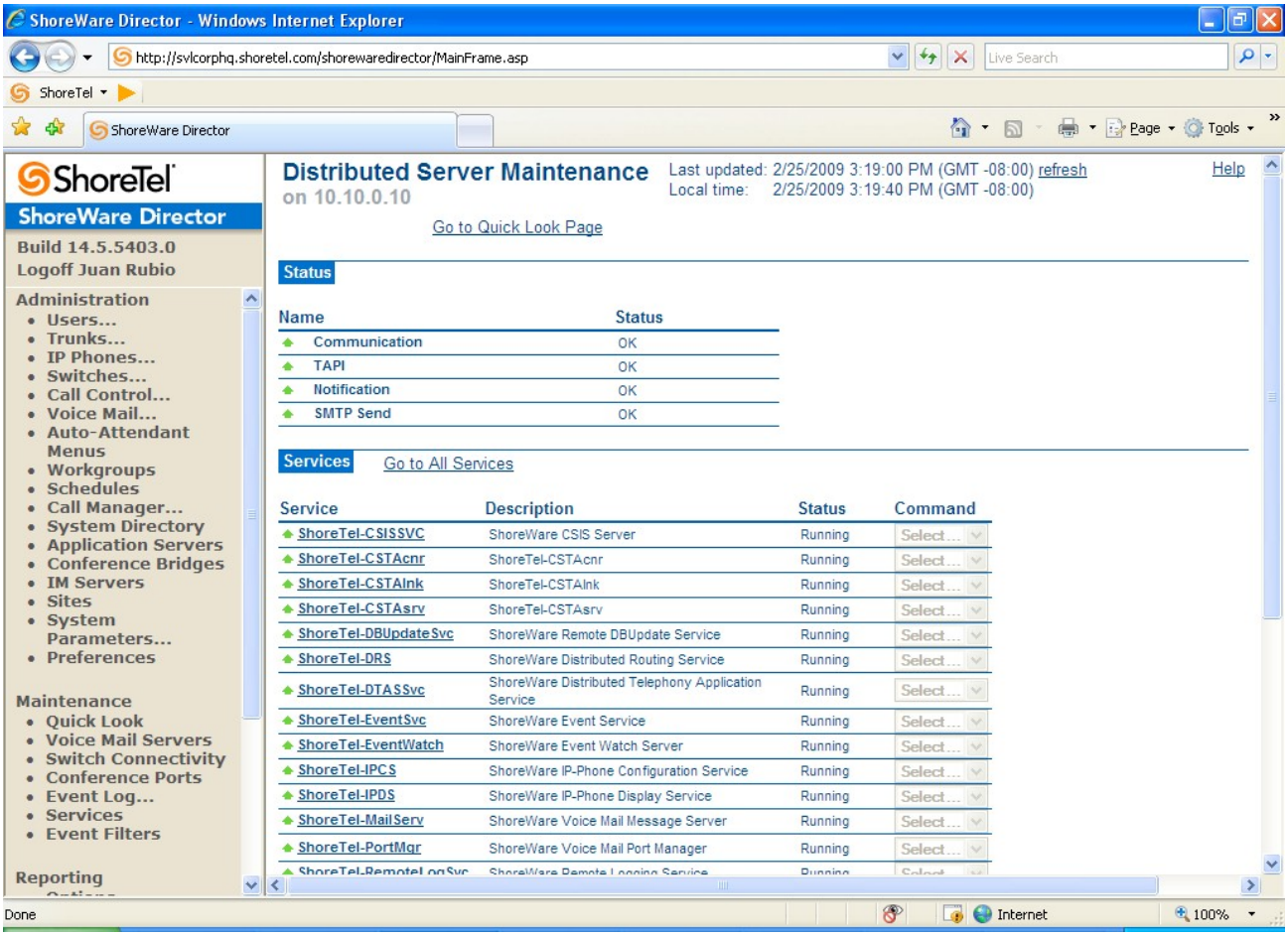
(connects to the CSTA Server)
(login to an STLI session)
(ends an STLI sessions)

Note: The Windows Telnet client has some restrictions:

- Special keys do not work, e.g. if you have a type a command you cannot use the backspace key for corrections (because the backspace character would become a part of the command).
- There is no initial prompt. You have to start your diagnostic session by blindly typing the appropriate command (**`STLI`** or **`SuperVisor`**)

5.2 CSTA Server Service(s) Not Running

The CSTA Server consists of three subcomponents which run as Windows System Services. These three services must be up and running. Use the Microsoft Windows Services Panel or the ShoreTel Director Quick Look Distributed Server Maintenance Page to check the status of these services.



ShoreTel Director Quick Look Distributed Server Maintenance Page

If these services must be manually restarted you should use the following sequence for start up:

1. TeamCall LinkTSP
2. TeamCall CA ShoreTel
3. TeamCall CSTA Server

This sequence is recommended but not strictly required since all of these services have built-in automatic synchronizing and recovery capabilities. The use of this sequence will decrease the time needed to synchronize between these components and the availability of the system is reached much faster.

5.3 Invalid Device Extension (Monitor)

Login via **STLI** session.

```
telnet localhost 26535          (connects to the CSTA Server)
STLI                            (login to an STLI session)
```

Assuming that you want to use the device 3000, than you could use the **`MonitorStart`** command,

```
MonitorStart 3000               (starts monitor on x3000)
```

If the MonitorStart command responds with an error indicating an `invalidMonitorObject` then you are using an extension number that does not exist or is invalid:

```
error_ind UniversalFailure operationalError
invalidMonitorObject
```

In the example above, an attempt is made to start a monitor on extension 3000 but the `invalidMonitorObject` reference in the response indicates that there is no extension 3000 that can be monitored on the PBX.

5.4 Wrong Listener Port Configuration

Using Telnet on the DVM host (that is the computer where the CSTA Server is running) enter the following (note that the characters **`SuperVisor`** that you type will not be echoed back on the screen—you'll be typing "blind"):

```
telnet localhost 26535          (connects to the CSTA Server)
SuperVisor                      (login to a SuperVisor session)
error_ind SUCCESS SuperVisor    (response indicates success)
BYE                             (disconnects from session)
```

If an error message such as `connection refused` or something similar appears, the port is probably not 26535. Please check the configuration. The login port may be manually configured via the setting **`loginPort`** inside the *Default.conf* configuration file.

5.5 Listener Port Already In Use by Another Process

Using Telnet on the DVS host (that is the computer where the CSTA Server is running)

Type the following (again, the word **SuperVisor** that you type will not be echoed back on the screen).

```
telnet localhost 26535
SuperVisor
```

If the response is neither `connection refused` nor `error_ind SUCCESS SuperVisor` then it is very likely that another process is listening on 26535. To confirm this, shutdown the ***TeamCall CSTA Server*** process and try this Telnet test again. If the same response is received, then you are sure that another process is using port 26535.

Solution: Either shut down the other process, or if this is not possible, choose a different listener port for the CSTA server via the **loginPort** setting inside the *Default.conf* file and restart the ***TeamCall CSTA Server*** process.

Note: We recommend that you use Netstat, a built-in Microsoft Windows Networking tool capable of displaying all listeners and their related program binaries:

```
C: netstat –a –b
```

This might help you to identify the other process which occupies the 26535 port. Be aware that the netstat command runs extremely slowly in conjunction with the **–b** parameter.

5.6 Requests from the Lync FE are Blocked

Login to the Lync host (that is the computer where the Lync Server is running). Lets assume that the DVS host (that is where the CSTA Server is running) has the IP-Address 10.99.0.10.Type:

```
telnet 10.99.0.10 26535
SuperVisor
```

(Note that the word **SuperVisor** that you type will not be echoed back on the screen—you'll be typing "blind".) The SuperVisor login command should respond with the message:

```
error_ind SUCCESS SuperVisor
```

If you are seeing a connection refused error message or something similar, it is very likely that there is a network connectivity issue or a firewall preventing connections from the Lync front end to the DVS host for the specified port.

Solution: Ping end to end, then verify with your network administrator that there aren't any network rules or policies that prevent access. Change firewall rules to allow TCP connections from the Lync host to the DVM host for the specified port.

5.7 License expired

Use the **`License`** command of a SuperVisor Telnet session to check the license. This command responds with information about the installed license.

```
License
error_ind SUCCESS License
maxMonitors: 9
days left: 60
expired: no
```

If the license command indicates an expired license please contact your ilink sales representative to obtain a new license file. Install a valid license for the CSTA Server by copying and pasting it into the CSTA Server *Default.conf* file or by using the ***License Tool*** application.

5.8 Monitor Points Exceeded

To check how many monitor points are actually in use, utilize the **`ShowDeviceMonitors`** command after starting a SuperVisor session using Telnet. This command lists all the monitored devices (each of them consuming a single license)

```
ShowDeviceMonitors
error_ind SUCCESS ShowDeviceMonitors
1000 sticky:false active:true observers:1
1001 sticky:false active:true observers:2
1002 sticky:false active:true observers:1
1003 sticky:false active:true observers:1
1004 sticky:false active:true observers:5
1005 sticky:false active:true observers:1
1006 sticky:false active:true observers:1
1007 sticky:false active:true observers:1
```

When a device is already monitored and another monitoring request for the same device is received by the CSTA Server it does not consume a new license. The number of active monitors for a given extension is indicated by the `observers` value. In this example there are 8 used

monitors (1000-1007, requiring at least 8 licenses) however there are a total of 13 active monitors because there are 5 observers on extension 1004 and 2 observers on extension 1001.

If you suspect that the number of monitored devices allowed by your license has been exceeded you can directly attempt to start monitoring a device that is not yet being monitored using an STLI session. For example:

```
telnet localhost 26535
STLI
error_ind SUCCESS STLI
MonitorStart 1000
```

If the **`MonitorStart`** command responds with an error that references `LICENSEERROR MONITORINGPOINTSEXCEEDED`, it means that you do not have a license with permission for enough monitored devices.

```
error_ind LICENSEERROR MONITORINGPOINTSEXCEEDED
Monitor not set
```

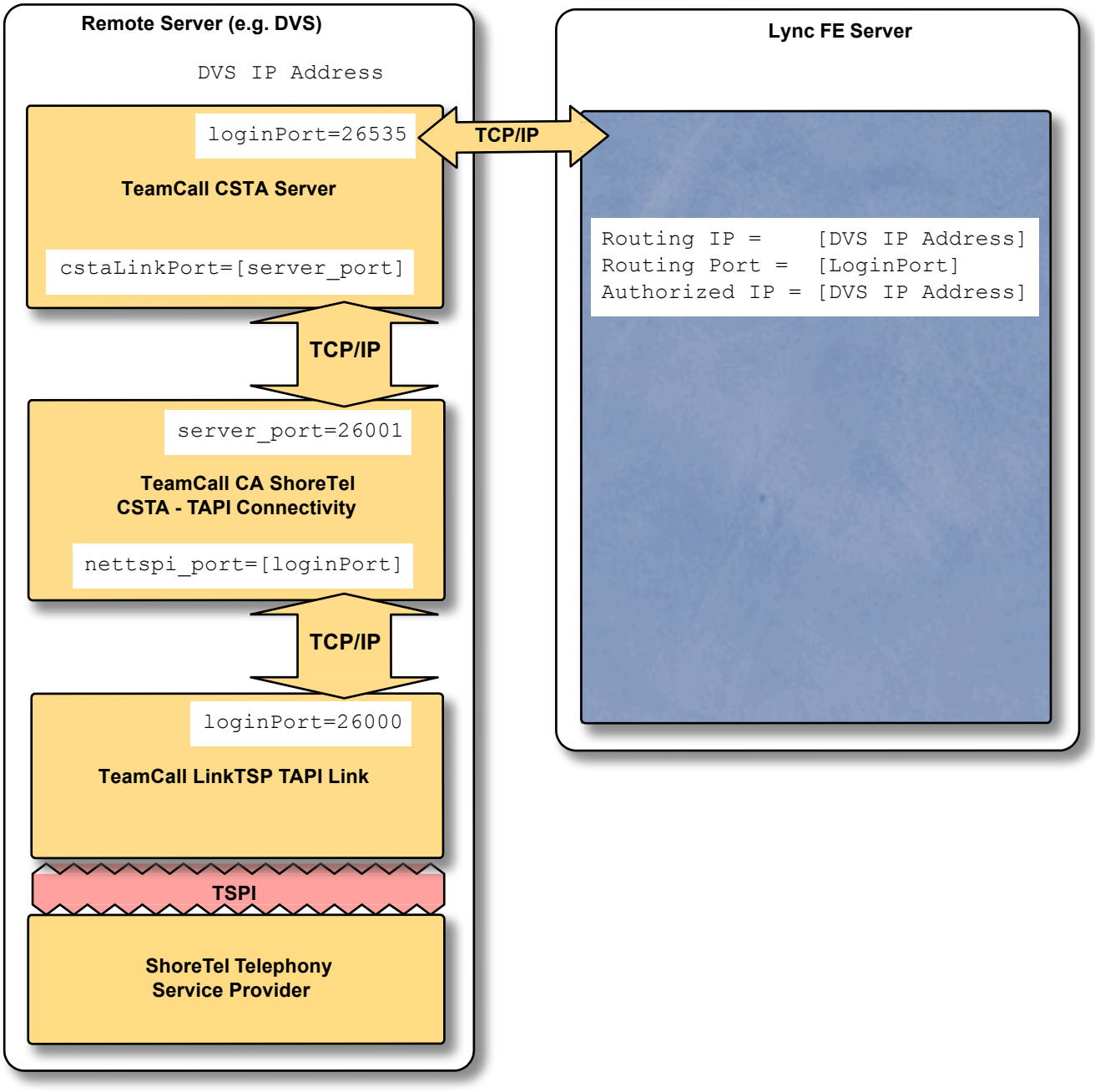
Solution: Obtain a new license file with a larger monitor limit. Replace the existing license with the larger license by copying and pasting it into the CSTA Server *Default.conf* file or by using the ***License Tool*** application.

5.9 Server Port Cascading Failure

ShoreTel CSTA server functionality is based on three separate subcomponents. These components are cascaded together via TCP/IP sockets.

Usually you do not have to change any of these ports. The installer chains up these ports correctly using the default values as shown in the diagram below.

Section 5.10 shows the keyword entries in the configuration files for each component and the default values. Installations should reserve the default ports of 26000, 26001, and 26535 for the ShoreTel CSTA Server. Only if it is essential that another process use one of the default ports, should the default port settings in the configuration files be overridden.



Cascading TCP ports

5.10 Configuration Files

By default, the configuration files for the CSTA Server components are stored in the directory **%ProgramFiles%*ilink**ShoreTel CSTA Server**Config***

Note: You do not usually need to modify these files as the CSTA Server installer already properly configures them for a typical situation.

Note: As a best practice, you should always create a backup copy of a configuration file before modifying it.

TeamCall CSTA Server Settings

The configuration file of TeamCall CSTA Server is named *Default.conf*. It contains the following keys:

Key	Default	Comment
`loginPort`	`26535`	Listener Port. This port is to be used in the Lync routing settings
`license`		Default is empty: demo mode with 1 monitor, Otherwise: a hexdump on a single line with encrypted licensing data
`logFileMaxSize`	`100`	Maximum size of a log file in KB. This size is limited only by file system constraints. A recommended value is 10240 (= 10 MB).
`logFileMaxBackups`	`2`	Number of log files to keep during log rotation. This number is limited only by file system constraints. The recommended range is 0 to 30.
`debugLevel`	`0`	0 = debug logging switched off 9 = for logging during debug sessions
`cstaLogEnabled`	`0`	Write csta.log (0 or 1)
`interfaceLogEnabled`	`0`	Write Interface.log (0 or 1)
`cstaLinkAddress`	`127.0.0.1`	The IP address of the host where TeamCall CA ShoreTel service is running. By default this is the loopback address because it is on the same host as the TeamCall CSTA Server service.
`cstaLinkPort`	`26001`	The listener port of the TeamCall CA ShoreTel. **Note**: this port is explicitly set to `26001` during the installation
`onNetPrefixList`		List of prefixes used if ShoreTel On-Net Dialing feature is activated. All prefixes are listed on a single line separated by semicolons (";") By default this is empty. **Note**: Configuring the CSTA server for On-Net Dialing also requires making corresponding entries in the *Dialplan.conf* file (see below).
`maxExtensionLength`	`5`	Maximum number of digits in an extension number. Should be set to 3, 4, or 5.

rfc2806PrivateContext	enterprise	"Private Context" string used to construct RFC2806 telURIs for extension numbers that have no corresponding DID number. The DID Prefix entered during installation is unique to the PBX and is used for this purpose. The default value (enterprise) is used when extension numbers are used as Line URI numbers of the Lync users.
setsignalhandler	1	For debugging only in the case a crash occurs: 0 : don't create a coredump 1 : create a coredump

TeamCall CA ShoreTel Settings

The configuration file of TeamCall CA ShoreTel is named *ca_config.properties*. It contains the following keys:

Key	Default	Comment
server_port	26001	The listener port.
nettspi_hostname	127.0.0.1	The IP address of the host where the TeamCall LinkTSP service is running. By default this is the loopback address because it is on the same host as the TeamCall CA ShoreTel service.
nettspi_port	20000	The port of the TeamCall LinkTSP service.

TeamCall LinkTSP Settings

The configuration file of TeamCall LinkTSP is named *LINKTSP.INI.* It contains the following keys:

Key	Default	Comment
loginPort	20000	The listener port.
Driver	RpcTspX.tsp	The TAPI TSP driver DLL

TeamCall CA ShoreTel and TeamCall LinkTSP Logging Settings

The TeamCall CA ShoreTel and TeamCall LinkTSP share a common configuration file that controls logging behavior named *log4j-config.xml*. This is an XML file that contains key value pairs using XML tags.
The root logger at the top of the configuration file contains a "Level" key. To change the level of detail in the log files produced, change the value of this key.

Key	Default	Comment
Level	INFO	Logging level. The default, "INFO", will log general information, warnings, and errors. To capture all debugging information, change this value to "DEBUG". To stop all logging change the value to "OFF".

Dial Plan Settings for uaCSTA Clients

The ShoreTel CSTA Server provides a telephone number mapping function for clients using the uaCSTA protocol such as Microsoft Lync software. Mapping, or translation, of telephone numbers is controlled by the *DialPlan.conf* configuration file. (The *Default.conf* file provides extension length and On-Net Dialing prefix values.) *DialPlan.conf* contains two tables, each with two columns of values. The first columns of both tables start in the first character position and the second columns start after a run of tabs and/or spaces.

The first table is known as the “Extension Translation Table” and it starts after a line that reads:

```
--Extension Translation Table
```

The entries in this table tell the gateway how to map references to internal extensions between DID numbers and extension numbers that can be dialed by the PBX. The first column contains characters to match with an external number (including country code). The second column contains digits to substitute in order to form the corresponding extension number.

The second table is known as the “External Translation Table” and it starts after a line that reads:

```
--External Translation Table
```

The entries in this table tell the gateway how to map references to external numbers between DID numbers and digit sequences that can be dialed by the PBX. The first column contains characters to match with an external number (including country code). The second column contains digits to substitute in order to form the corresponding dialable sequence.

Note: All entries are evaluated in the order they appear in the *DialPlan.conf* file. For translation to occur correctly, make sure that every entry is in the correct order: from most specific to least specific.

Translating Numbers Received from uaCSTA Clients

Telephone numbers received from a uaCSTA client are first examined to determine if they are already dialable extension numbers (based on their length) or On-Net Dialing extensions (based on their prefix). If so, no translation is required.

Otherwise, these numbers are processed by matching the leading characters of the telephone number provided with an entry in the first column of the Extension Translation Table. If a match is found, the matching portion of the provided telephone number is replaced with the digits found in the corresponding entry in the second column.

The examples below illustrate the substitution process for mapping to extension numbers:

First Column	Second Column	Number Provided	Resulting Extension
+14085551	11	+14085551234	11234
+14085551	589	+14085551234	589234
+140828512	7	+14085551234	734
+14085551234	456	+14085551234	456

If no match is found in the Extension Translation Table, then the matching process is repeated using the External Translation Table. The leading characters of the provided telephone number are matched with an entry in the first column of the External Translation Table. If a match is found the matching portion of the provided telephone number is replaced with the digits found in the corresponding entry in the second column.

These examples illustrate the substitution process for mapping to a dialing sequence for an external number:

First Column	Second Column	Number Provided	Resulting External Dialing Sequence
+	9+	+14085551234	9+14085551234
+1	91	+14085551234	914085551234
+1408	9	+14085551234	95551234
+1212	81212	+12125551234	812125551234

Translating Numbers to be Delivered to uaCSTA Clients

Telephone numbers received from the PBX are first examined to determine if they are extension numbers (based on their length) or On-Net Dialing extensions (based on their prefix). If so, numbers are converted from extension numbers to numbers in “international format” by matching the leading digits of the extension number with an entry in the second column of the Extension Translation Table. If a match is found the matching portion of the extension number is replaced with the digits found in the corresponding entry in the first column. If no match is found no translation is performed. If all the digits in the second column match the number in question, then all the digits are replaced with the entry found in the corresponding first column.

These examples illustrate the substitution process:

First Column	Second	Extension	Resulting Number
+14085551	11	11987	+14085551987
+14085551	589	589123	+14085551123
+140828512	7	789	+14082851289
+14085551234	456	456	+14085551234

Telephone numbers received from the PBX that correspond to external numbers are converted to DID numbers by matching the leading digits of the external number with an entry in the second column of the External Translation Table. If a match is found the matching portion of the number is replaced with the digits found in the corresponding entry in the first column. If no match is found then no translation is performed. If all the digits in the second column match the external number, then all the digits are replaced with the entry found in the corresponding first column.

These examples illustrate the substitution process:

First Column	Second	External Number	Resulting Number
+1	1	14085551987	+14085551987
+1		4085551987	+14085551987

Configuring Dialplan for On-Net Dialing

If the On-Net Dialing feature is enabled additional entries in the Extension Translation Table are needed. As described above, the CSTA Server determines if a number is an extension number or an externalnumber based on its length. Telephone numbers too long to be extension numbers are considered external numbers unless they start with one of the On-Net Dialing prefixes configured in the
Default.conf configuration file (see above).

If On-Net Dialing is configured then the extension numbers used in the mapping process will consist of the On-Net Dialing prefix followed by an extension number of the standard length and the Extension Translation Table must contain appropriate entries.

For example, a PBX is configured to use 3 digit extensions and an On-Net Dialing prefix of 589. All extensions associated with that prefix are associated with the DID range (408)555-1xxx. In this case the On-Net Dialing prefix 589 would be added to the list of On-Net Dialing prefixes configured in the *Default.conf* file and there would be an entry in the Extension Translation Table of the Dialplan.conf fie with **`+14085551`** in the first column and **`589`** in the second column. This example is also illustrated in the second rows of each of the two sets of Extension Translation Table examples above.

Troubleshooting DialPlan.conf

To confirm an issue with the *DialPlan.conf* file

1. Prepare a list of valid extensions and their corresponding telURIs as entered into Lync settings
2. Open the DialPlan.conf file with a text editor
3. For each telURI, scan the first column in DialPlan.conf and find the **first** entry that matches the leading digits of the telURI then replace the matching digits with the digits in the second column and match the result against the correct extension.
4. For each telURI, scan the second column in DialPlan.conf and find the **first** entry that matches the leading digits of the extension then replace the matching digits with the digits in the first column and match the result against the correct telURI.

If any converted number doesn't match, confirm that the telURI entered into Lync was valid. If so, the DialPlan.conf file is the source of the problem.

Solution: Manually correct the DialPlan.conf file by reordering or correcting existing entries, deleting invalid entries and/or adding missing entries then restart the CSTA server components.

6. Lync Server Diagnostics

The majority of phone integration failures result from mistakes in Lync configuration. Always begin with a simple check of the following:

- Host Routing and authorization settings (which are global settings)
- IP address and port correct?
- Replace URI checkbox enabled?
- Matching routing table rule correct?
- User specific phone settings (which are – as the name implies – personal settings)
- Is the telURI entered correctly?

If this check does not lead to a solution than the usage of the Lync logging tool is to be considered.

Note: Lync logging has to be explicitly enabled. The examples in this illustration all refer to a Lync log file generated as documented in *Section 8.1 Lync Logging*, below.

6.1 Review the configured TCP route, Trusted Application Pool, and Trusted Application

Open the Lync Server Management Shell as an administrator and use the following commands to review your configuration (**enter each command on a single line**, even if printed here on multiple lines for formatting's sake).

Query the configured trusted applications:

```
get-CsTrustedApplication
```

Example output:

```
Identity                    : 10.40.1.3/urn:application:ShoreTelCSTA
ComputerGruus               : {10.40.1.3 sip:10.40.1.3@yourdomain.com;
gruu;opaque=srvr:ShoreTelCSTA:mKvuQmKrMFa9BhsMaf0mS44A}
ServiceGruu                 : sip:10.40.1.3@yourdomain.com;gruu;opaque=srvr:
ShoreTelCSTA:mKvuQmKrMFa9BhsMaf0mS44A
Protocol                    : Tcp
ApplicationId               : urn:application:ShoreTelCSTA
TrustedApplicationPoolFqdn : 10.40.1.3
Port                        : 26535
LegacyApplicationName       : ShoreTelCSTA
```

The list should contain such a block for the ShoreTel CSTA Server (possibly additional output blocks for other trusted applications as well). Check the IP addresses, host name, and port to make sure that all values are correct.

If you have a complex setup with multiple CSTA servers, you should see one entry for each CSTA server.

Query the configured trusted application pools:

```
get-CsTrustedApplicationPool
```

Example output:

```
Identity              : TrustedApplicationPool:10.40.1.3
Registrar             : Registrar:lync2013.yourdomain.com
FileStore             :
ThrottleAsServer      : True
TreatAsAuthenticated  : True
OutboundOnly          : False
RequiresReplication   : False
AudioPortStart        :
AudioPortCount        : 0
AppSharingPortStart   :
AppSharingPortCount   : 0
VideoPortStart        :
VideoPortCount        : 0
Applications          : {urn:application:ShoreTelCSTA, urn:application:other-
application}
DependentServiceList  : {}
ServiceId             : 1-ExternalServer-1
SiteId                : Site:Headquarters
PoolFqdn              : 10.40.1.3
Version               : 6
Role                  : TrustedApplicationPool
```

The list should contain such a block for the trusted application pool that you set up for ShoreTel CSTA Server (possibly additional blocks for other trusted application pools as well). Check that it contains the application name you've set for ShoreTel CSTA Server, also check the IP addresses and registrar name to make sure that all values are correct.

If you have a complex setup with multiple CSTA servers, you should see one entry for each CSTA server.

Query the static TCP routes:

```
get-CsStaticRoutingConfiguration
```

Example output:

```
Identity : Global
Route    : {MatchUri=shoreteldvs.yourdomain.com;MatchOnlyPhoneUri=False;
Enabled=True;ReplaceHostInRequestUri=True,

MatchUri=otherhost.yourdomain.com;MatchOnlyPhoneUri=False;Enabled=True;
ReplaceHostInRequestUri=True}
```

The list should contain one line for the static TCP route that you set up for ShoreTel CSTA Server (possibly additional lines for other TCP routes as well). Check that it contains the correct host name of the system where ShoreTel CSTA Server is installed.

If you have a complex setup with multiple CSTA servers, you should see one entry for each CSTA server.

6.2 Remove the configured TCP route, Trusted Application Pool, and Trusted Application

You need to remove these in the following order:

- Trusted Application
- Trusted Application Pool
- Static TCP Route

Open the Lync Server Management Shell as an administrator and use the following commands to review your configuration (**enter each command on a single line**, even if printed here on multiple lines for formatting's sake).

Remove the configured trusted application:

Query the list of configured trusted applications (for details see section 6.1 above):

```
get-CsTrustedApplication
```

To remove the application, look for the "`Identity`" value of CSTA servers' trusted application entry and use that value instead of `%Identity%` when entering the following command:

```
remove-CsTrustedApplication %Identity%
```

For example:

```
remove-CsTrustedApplication 10.40.1.3/urn:application:ShoreTelCSTA
```

Remove the configured trusted application pool:

Query the list of configured trusted application pools (for details see section 6.1 above):

```
get-CsTrustedApplicationPool
```

A trusted application pool can only be removed if there is no application associated with it. So if the pool still contains an application at this point, please remove it as well (if that's what you want) or skip the step of removing the application pool.

To remove the pool, look for the "`Identity`" value of CSTA servers' trusted application pool entry and use that value instead of `%Identity%` when entering the following command:

```
remove-CsTrustedApplicationPool %Identity%
```

For example:

```
remove-CsTrustedApplicationPool TrustedApplicationPool:10.40.1.3
```

Remove the configured static TCP route:

Query the list of configured TCP routes (for details see section 6.1 above):

```
get-CsStaticRoutingConfiguration
```

To remove the route, look for the "`MatchUri`" value of CSTA servers' TCP route entry and use that

value instead of `%MatchUri%` when entering the following commands:

```
$delroute = Get-CsStaticRoutingConfiguration -identity global | Select-Object
-ExpandProperty Route | Where-Object {$_.MatchUri -eq "%MatchUri%"}


Set-CsStaticRoutingConfiguration -identity global -Route @{Remove=$delroute}
```

For example:

```
$delroute = Get-CsStaticRoutingConfiguration -identity global | Select-Object
-ExpandProperty Route | Where-Object {$_.MatchUri -eq
"shoreteldvs.yourdomain.com"}


Set-CsStaticRoutingConfiguration -identity global -Route @{Remove=$delroute}
```

See the ShoreTel CSTA Server Configuration Guide for information on how to configure new settings for TCP route, Trusted Application Pool, and Trusted Application.

6.3 No Matching Routing Table Rule

Symptom: The message flow in the log file is similar to:

```
Text: Non-trusted source sent an FQDN/IP that doesn't match a
routing table rule

Result-Code: 0xc3e93c5e SIPPROXY_E_ROUTING

SIP-Start-Line: INVITE sip:callcontrol@dvm1.csta.yourcompany.com
SIP/2.0

SIP-Call-ID: 19c4aacda45340a3b58eb9d602b2c073

SIP-CSeq: 1 INVITE

Data: user="johns@dvm1.csta.yourcompany.com"
```

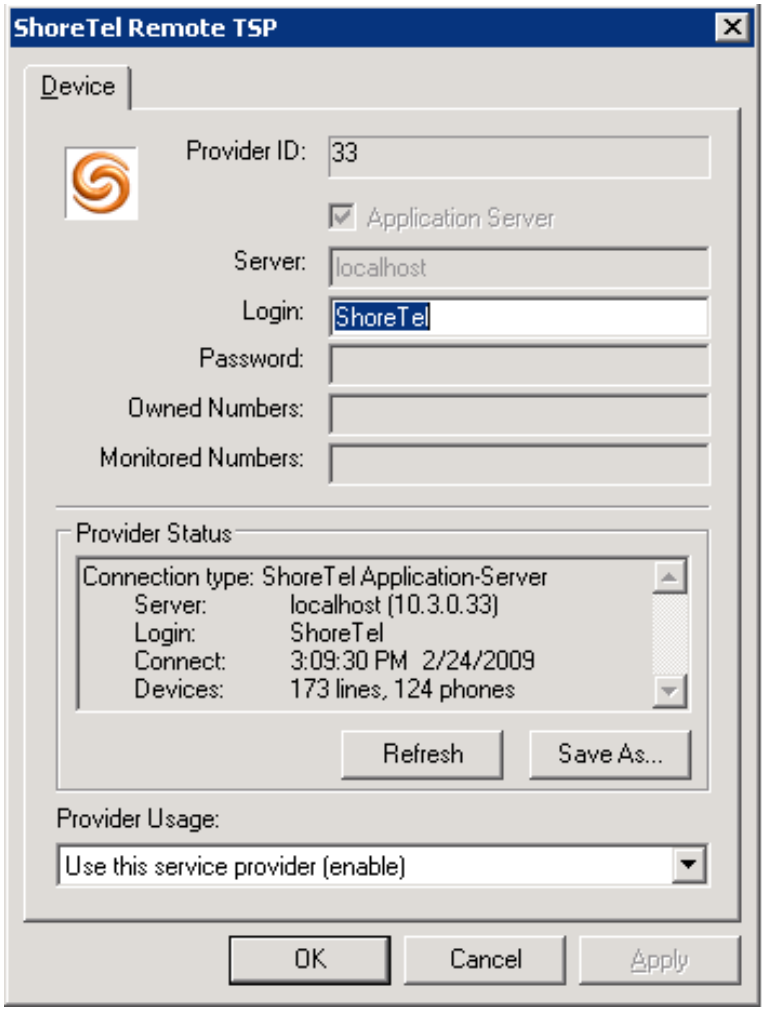
Solution: Change the static routing rule or change the SIP URI for the user (in this example there was no routing rule for `dvm1.csta.yourcompany.com`).

7. TAPI Diagnostics

The ShoreTel CSTA Server takes advantage of ShoreTel PBX support for Microsoft Telephony Application Programming Interface (TAPI) to exchange call control service requests and events.The TeamCall LinkTSP service connects to the ShoreTel TAPI service provider using the TAPI Service Provider Interface (TSPI).

The Telephony Management Service (TMS) application service (which runs on every ShoreTel server) connects the ShoreTel TAPI service provider to the rest of the ShoreTel distributed PBX. When TMS starts up, it creates a TAPI line device for each endpoint in the ShoreTel system. Access to these TAPI lines is provided through ShoreTel Remote TAPI Service Providers (RpcTsp.tsp and RpcTspX.tsp). The ShoreTel CSTA Server has access to these TAPI lines and receives new calls, call state information, and line device information from TMS via RpcTspX.tsp, thus allowing it to monitor all of the ShoreTel extensions.

To view the properties of the ShoreTel Remote TAPI Service Provider, open the ***Phone and Modem Options*** tab in the Windows Control Panel, then from the ***Advanced*** tab select ***ShoreTel Remote TAPI Service Provider*** and click on the ***Configure*** button.

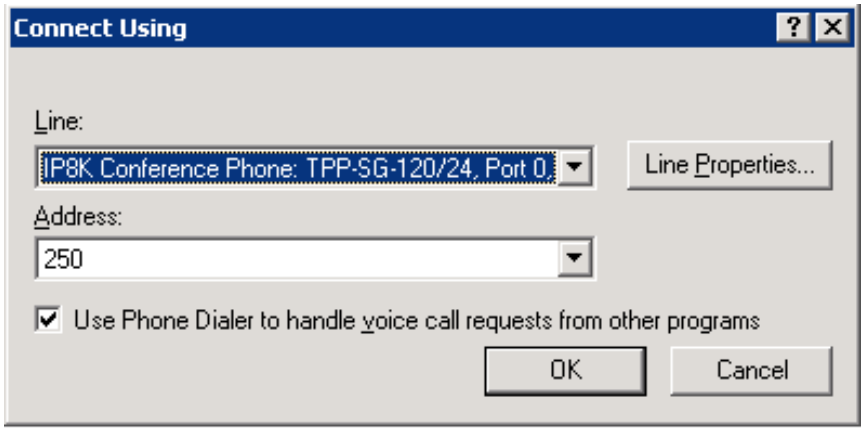


ShoreTel Remote TSP Properties

On a properly installed ShoreTel DVS, the ShoreTel Remote TAPI Service Provider status should appear as shown above. The ***Application Server*** and ***Server*** parameters are grayed out. The ***Login*** will be ShoreTel and no other parameters are defined. The ***Provider Status*** will display the server's localhost IP address - verify that this is the correct IP address. In addition, verify that the ***Devices*** status shows the appropriate number of lines and phones and that the ***Provider Usage*** is set to ***enable***.

Several diagnostic steps involve observing the exchange of instructions and events between the PBX and the system running the ShoreTel CSTA Server through this TAPI service provider. Diagnostics are done on the same host where the CSTA Server is running.

Use Microsoft's ***Dialer.exe*** application (usually installed by default on Windows), to place a test call using one of the ShoreTel extensions. If it has never been used before the first step is to configure a TAPI line:

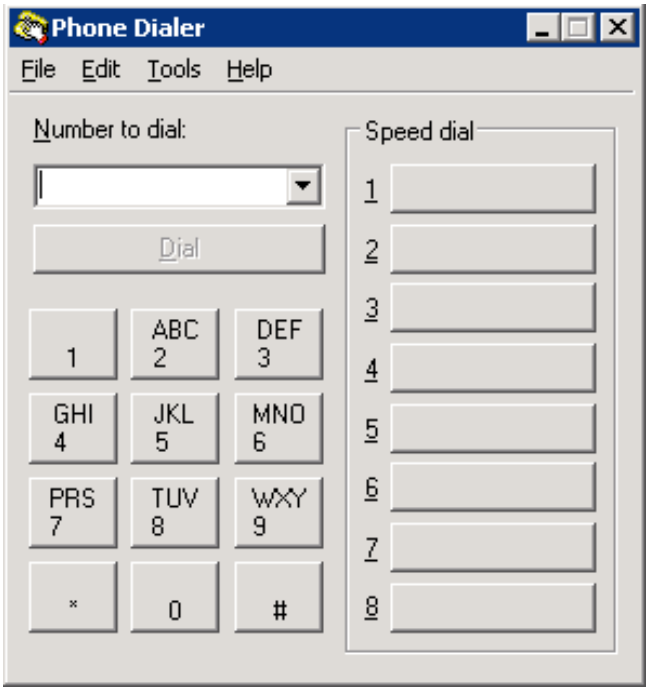


Configuring Dialer.exe

The ***Line*** is the name of a ShoreTel extension, along with the ShoreGear switch that is managing it and port number. The ***Address*** is the actual extension number. Select an appropriate Line and click on "OK". If the dialer application was utilized before and the ***Connect Using*** window is not displayed select ***Tools*** then ***Connect Using….***

Note: If you cannot select the desired Line Address then there is probably something wrong with the ShoreTel system, TAPI, or a communication problem. Please refer to the appropriate ShoreTel Maintenance Guide or contact your service provider or ShoreTel's Technical Assistance Center.

Once you have configured the appropriate line, the ***Phone Dialer*** application will be active:

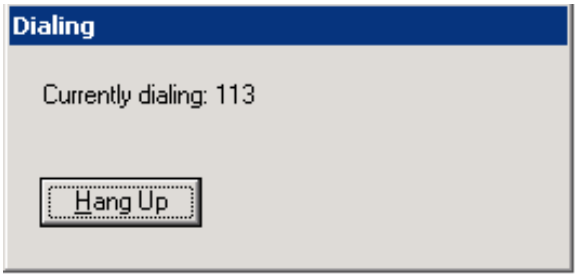


To test dialing functionality:

1. To place a call to another extension enter a valid extension in the ***Number to dial*** field
2. Press the ***Dial*** button and you will see the Dialing window displayed below.

Note: If you wish to place a call to an external number you must use an appropriate trunk access code followed by the full number (including country code). You cannot use a a number like “+14085551212” here.

Note: If the TAPI phone dialer does not respond to the ***Dial*** command or shows an error then there is probably something wrong with the ShoreTel system, TAPI, or a communication problem. Please refer to the appropriate ShoreTel Maintenance Guide or contact your service provider or ShoreTel’s Technical Assistance Center.



Dialing window

3. Press the ***Hangup*** button to end the call and close the Phone Dialer application by closing the application window or by selecting ***Exit*** from the ***File*** menu.

8. Logging

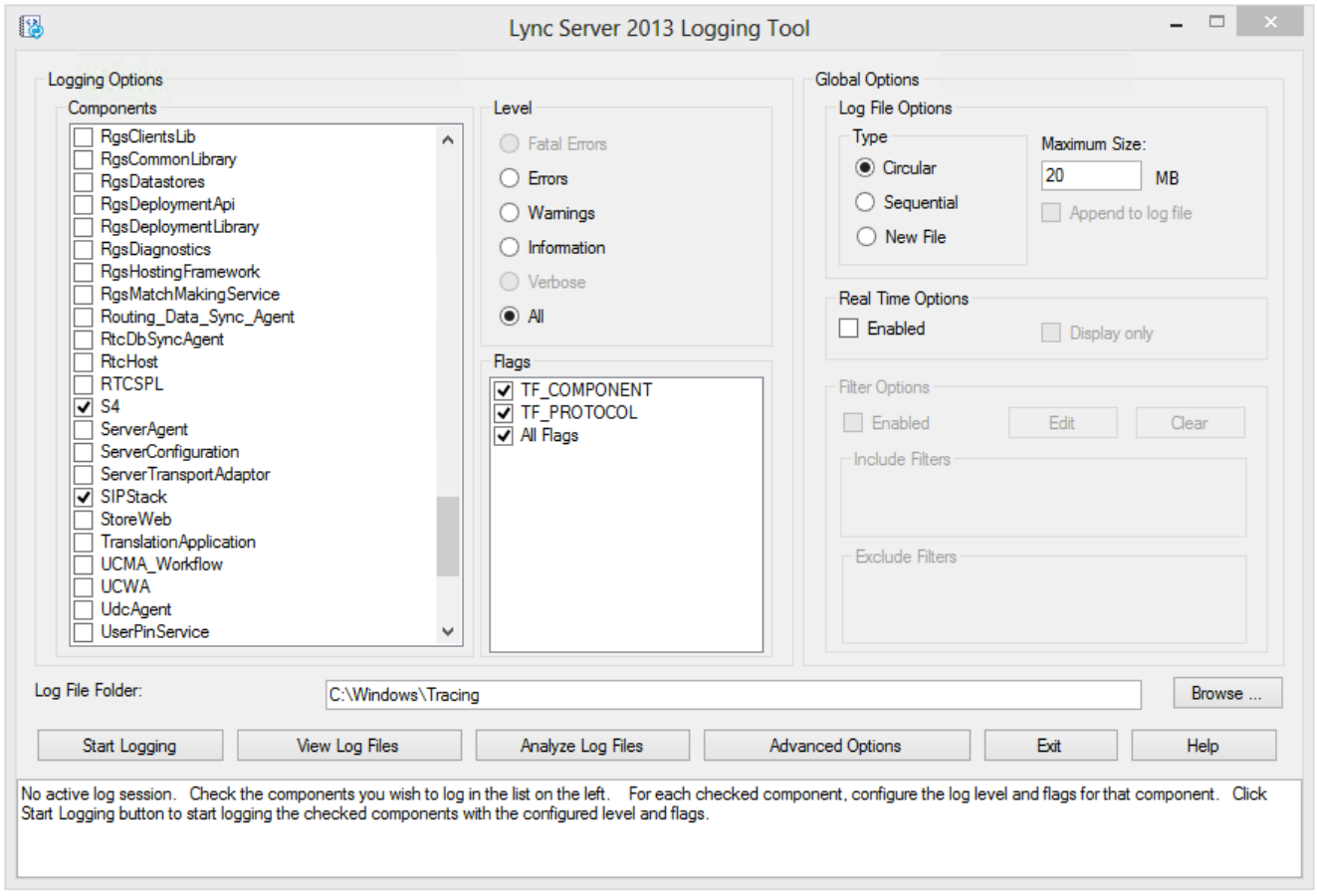
The Lync Server, the Lync client and the ShoreTel CSTA Server generate log files that can provide useful troubleshooting information.

8.1 Lync Server Logging

8.1.1 Lync Server 2013 Logging

The Lync Server 2013 logging function is enabled using the Microsoft Lync Server 2013 Debugging Tools that can be downloaded from Microsoft at:
http://www.microsoft.com/en-us/download/details.aspx?id=35453

After installation, the tools can be found in **%ProgramFiles%\Microsoft Lync Server 2013\Debugging Tools.** Start OCSLogger:



Check the following components in order to troubleshoot Lync 2013 telephony integration:

- Inbound Routing
- Outbound Routing
- S4
- SIPStack

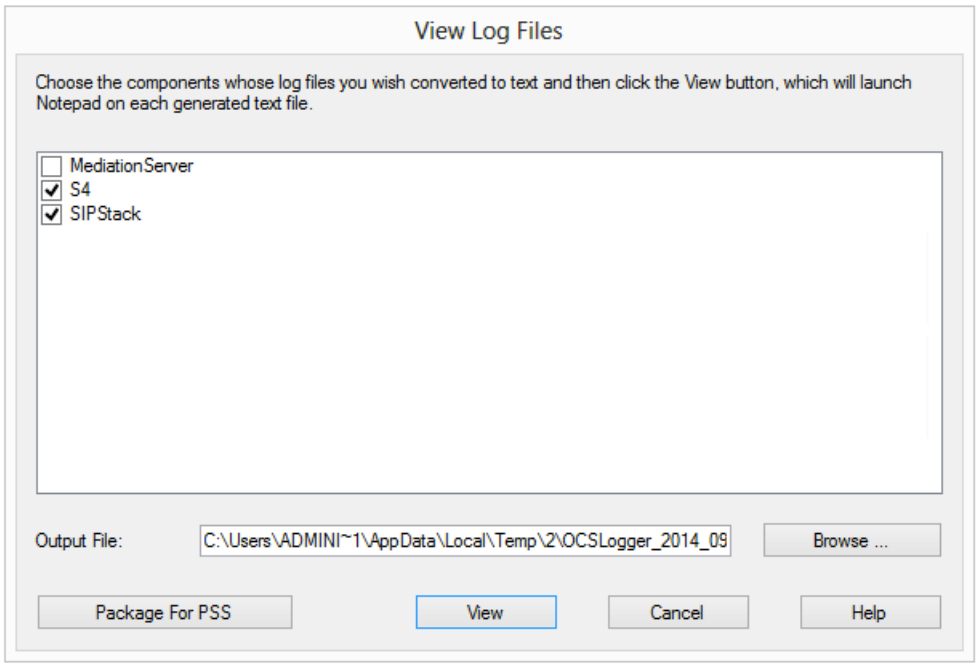
Click ***Start Logging*** to start the server logging.

Now sign-out/sign-in using the Lync client where the issue appears.

Reproduce the failing scenario and then click ***Stop Logging*** in the Lync Server 2013 Logging Tool.

The logs will be generated as binary .etl files to *%WinDir%\Tracing*.

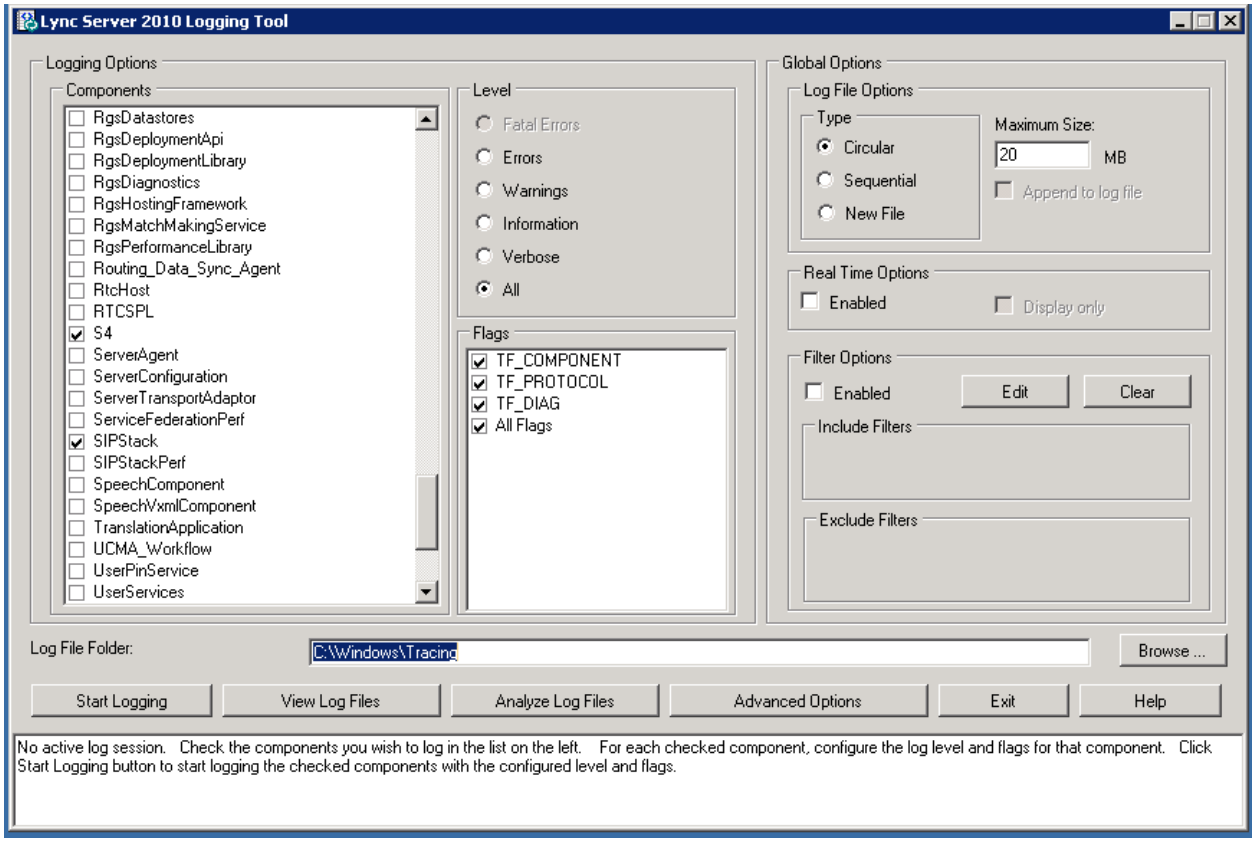
To view the contents of these log files, click ***View Log Files*** in the Lync Server 2013 Logging Tool. This will open the ***View Log Files*** window:



Use the checkboxes to indicate which logging information you want to view, specify a filename, and click ***View***. This will convert the binary .etl files into a readable text file.

8.1.2 Lync Server 2010 Logging

The Lync Server 2010 logging function is enabled from the console of the Lync Server 2010 host. Click Start > Microsoft Lync Server 2010 > Lync Server Logging Tool to launch the logging application:



Check the following components in order to troubleshoot Lync 2010 telephony integration:

- Inbound Routing
- Outbound Routing
- S4
- SIPStack

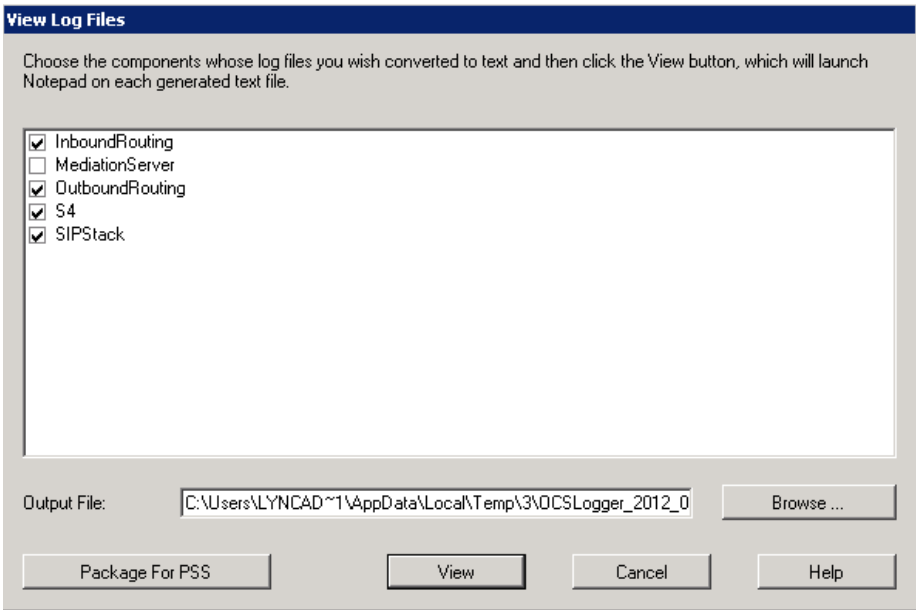
Click ***Start Logging*** to start the server logging.

Now sign-out/sign-in using the Lync client where the issue appears.

Reproduce the failing scenario and then click ***Stop Logging*** in the Lync Server 2010 Logging Tool.

The logs will be generated as binary .etl files to *%WinDir%\Tracing*.

To view the contents of these log files, click ***View Log Files*** in the Lync Server 2013 Logging Tool. This will open the ***View Log Files*** window:



Use the checkboxes to indicate which logging information you want to view, specify a filename, and click ***View***. This will convert the binary .etl files into a readable text file.

8.2 Lync Client Logging

Lync Client logging needs to be explicitly enabled as follows:

1. Sign in to Lync, click the Tools dropdown in the upper right hand, then choose *Options.*
2. Select the ***General*** tab.
3. **In Lync 2013:** Look for the Logging in Lync menu and set it to Full.
   In Lync 2010: Check the box to enable logging.
   With both clients you do not need to activate Windows event logging.
4. Save changes, then sign out of Lync and sign back in to activate the logging.

A log file will now be generated.

In **Lync 2013** the log file is located at:

%userprofile%\AppData\Local\Microsoft\Office\15.0\Lync\Tracing

File name: *Lync-UccApi-0.UccApilog*
(or a different file name with the *.UccApilog* file name extension).

In **Lync 2010** the log file is located at:

%userprofile%\Tracing

File name: *Communicator-uccp-0.uccplog*
(or a different file name with the *.uccplog* file name extension).

Example content of the log file:

```
08/01/2012|13:55:14.156 2BC:940 INFO   :: SIP/2.0 504 Server time-out

Authentication-Info: Kerberos
rspauth="602306092A864886F71201020201011100FFFFFFFF6D7B7A0E04D10F53B
A62891944F98297", srand="BB548579", snum="10", opaque="0FDE32B5",
qop="auth", targetname="sip/Lync.yourcompany.com", realm="SIP
Communications Service"

From: <sip:Admin@yourcompany.com>;tag=f94e507772;epid=0d60acc870

To:
<sip:callcontrol@dvm1.csta.yourcompany.com>;tag=399A3A01D09653F93535
7E3180DFD0EB


Call-ID: 82fbde0b79474e5a9b6f09414d333191


CSeq: 1 INVITE
[…]
```

This example illustrates a scenario where the remote CSTA server cannot be reached for one of the following reasons:

- Wrong static route; verify from Lync powershell command *Get-CsStaticRoutingConfiguration*
- Network connectivity or firewall problem between Lync FE and CSTA host
- CSTA Server is not up and running
- CSTA Server is configured with a wrong port number

Note: The Call-ID and the CSeq fields are very useful for tracing the flow of the SIP messages within other log files from the Lync Server because these attributes are used to correlate requests and responses.

8.3 CSTA Logging

The log files of the CSTA Server and its associated components are used primarily by ilink to narrow down internal CSTA server issues.

However, ilink TAC might request that CSTA server logging be enabled to help diagnose a problem. Logging is enabled and configured via the CSTA server's configuration file *Default.conf* which is located in **%ProgramFiles%*ilink**ShoreTel CSTA Server**Config***

This file contains key value pairs. The keys that control logging are as follows (showing the default values):

```
cstaLogEnabled = 0          # 0 -> off, 1 -> on
interfaceLogEnabled = 0     # 0 -> off, 1 -> on
debugLevel = 0              # 0 -> off, 9 -> max

logFileMaxSize= 10000       # log file will be rotated at this size (kB)
logFileMaxBackups = 5       # number of rotated log file to preserve
```

The log files generated by CSTA Server and its associated components are found in **%ProgramFiles%*ilink**ShoreTel CSTA Server**Logs***. The following log files are generated:

Filename	Component	Content	Format
Sys.log	TeamCall CSTA Server	Startup/Shutdown/licensing	text
Error.log	TeamCall CSTA Server	Internal processing	text
CSTA.log	TeamCall CSTA Server	Messages exchanged between TeamCall CSTA Server and TeamCall CA ShoreTel *(not activated by default)*	hexdump
Interface.log	TeamCall CSTA Server	Incoming messages and outgoing messages correlated to the used protocol interfaces *(not activated by default)*	hexdump
CAShoreTel.log	TeamCall CA ShoreTel	Internal processing	text
LinkTSP.log	TeamCall LinkTSP	Internal processing	text
CA-CSIS\ CSIS_CAxx.log	ilink CSIS Connector	Internal processing	text