TechNote

Avaya Aura Session Manager 6.0

December 9, 2010

XCAPI
voiceoverIP

TE-SYSTEMS
competence in e-communications.

Introduction

This document is intended to support you with the integration of the XCAPI Version 3.3.161 into an existing environment of the Avaya Aura Session Manager. Though being based on version 6.0 of the Avaya Aura environment it should be applicable to lower versions, given a few adjustments.

In the following sections we describe the essential steps of configuration to allow for optimal cooperation of the XCAPI and the Avaya Aura Session Manager by using the SIP protocol stack via TLS and SRTP for media encryption. This configuration example can be easily adapted to plain SIP trunking via TCP.

At this point we suppose that the Avaya Aura Session Manager and Avaya Communication Manager, the hardware the XCAPI is running on, and both the XCAPI and your CAPI applications are already installed properly. For some extended information on installation procedures please refer to the respective manuals. A short installation manual for the XCAPI is available at the XCAPI Website.
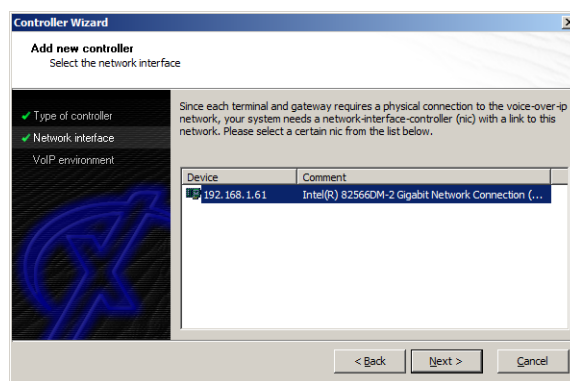
XCAPI Configuration

Please start up the XCAPI configuration to create a new controller assigned to the `Avaya Aura Session Manager`. If you've just installed the XCAPI and start the configuration tool for the first time, the `XCAPI Controller Wizard` will pop up automatically. This will also happen if there's no controller configured at all. To start up the `XCAPI Controller Wizard` on your own, just click the hyperlink labelled `Click here to add a controller` on the main page of the XCAPI configuration tool. On the first page of the Controller Wizard please select the `Add Voice-over-IP controller (VoIP)` option and continue by clicking on the Next button.
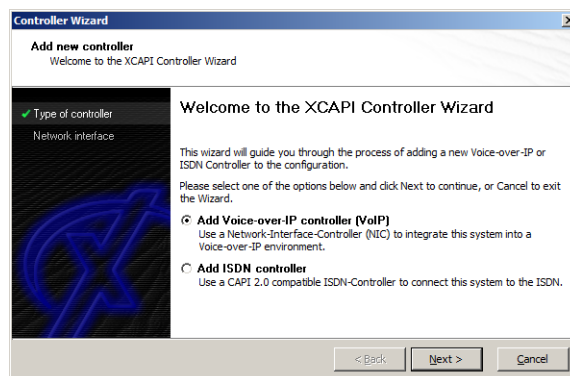
2.1 Network Interface

On this page of the XCAPI Controller Wizard you can select the network adapter you want to bind to the XCAPI controller.

2.2 Voice-over-IP Environment

The next dialog of the configuration tool shows a list of some common Voice-over-IP environments. Selecting one of those will configure the XCAPI with a selection of near-optimal presets for the kind of environment you have, sparing you quite a lot of manual configuration. Please select the `Avaya SES (Session Manager is not implemented yet)` option here.
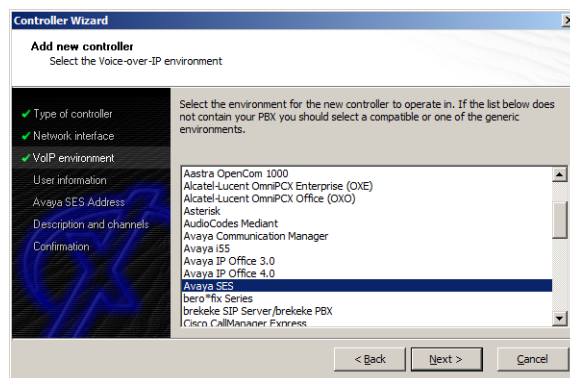
2.3   User Information

No user information is necessary for setting up the XCAPI as `Trusted Host` within the `Avaya Aura Session Manager` configuration.

2.4   IP Address of the Session Manager

In the dialog `Network Address` please provide the IP address of the SM-100 interface of your Avaya Aura Session Manager.
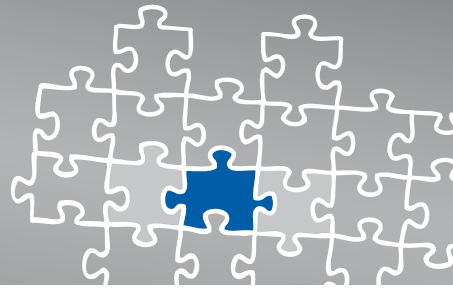
2.5 Description and Channels

Next, please enter how many simultaneous connections the XCAPI should handle when communicating with the Session Manager.

2.6 Confirmation

The final dialog of the Controller Wizard performs some checks on the configuration parameters you've made. If any errors are detected here, you can go back to the respective dialogs and correct the necessary input. If everything is correct please use the finish button in order to finally create the new controller.

The controller you've just created now will appear on the main page of the XCAPI configuration. As we're now finished with all XCAPI-related configuration tasks, please save the changes you've made and exit the configuration tool.
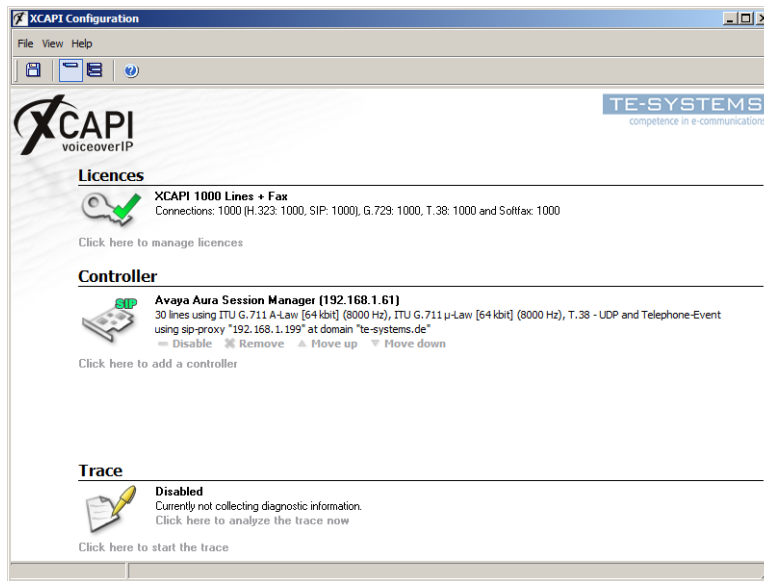
You need to restart the bound CAPI applications to take effect on any controller changes.

System Manager Configuration

In order to establish the communication between the XCAPI and the Avaya Aura Session Manager using the SIP protocol, you need to add the XCAPI as `SIP Entity` with all its according configurations.

The configuration of this examples communication manager part is not described at all. We assume that the related trunk and routing configuration harmonize to your VoIP environment.

3.1 Domains

This Session Manager environment uses the SIP domain `te-systems.de` for allowing domain-based routings.
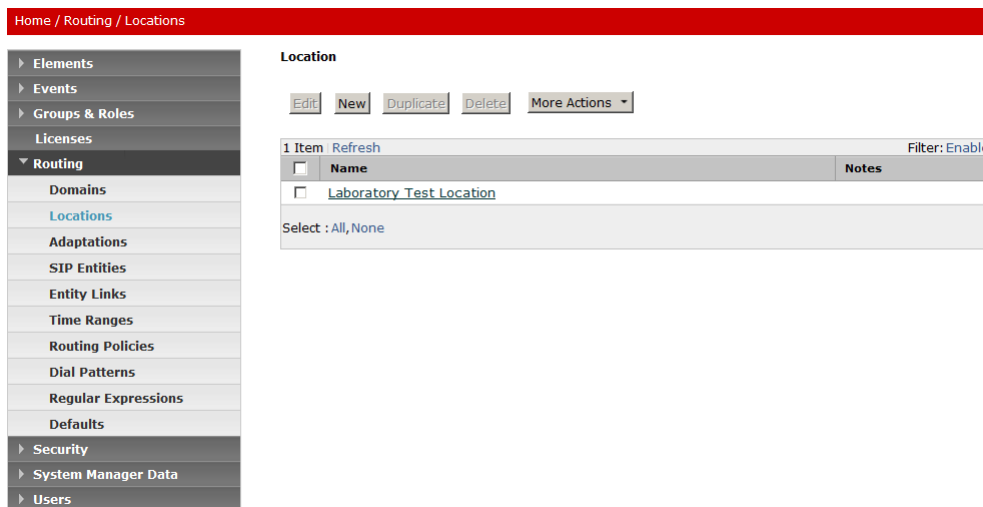
3.2 Locations

The location for this example is named `Laboratory Test Location`.
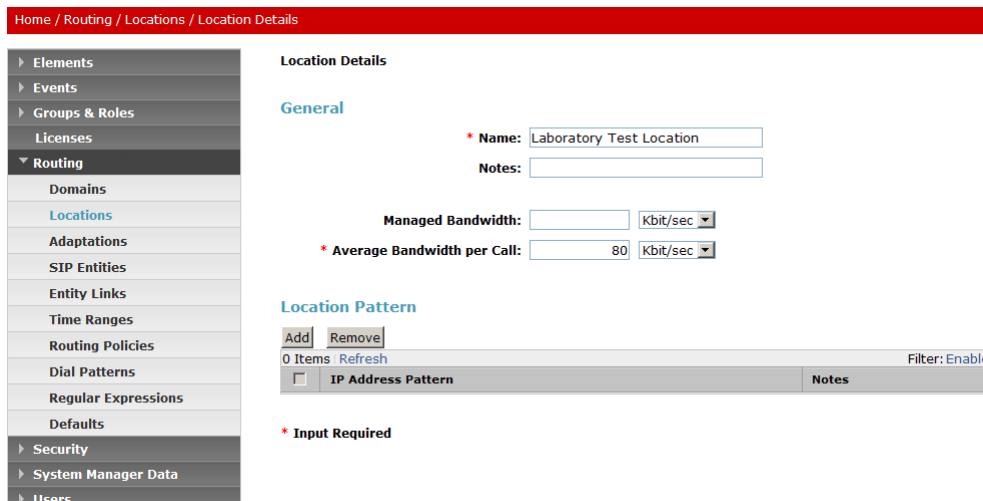
The location details are used with their default values.

3.3 Adaptations

The adaptations for these environment SIP entities are used as shown next.

Home / Routing / Adaptations				
Adaptations				

Edit New Duplicate Delete More Actions ▾

2 Items | Refresh   Filter: Enable

	Name	Module name	Egress URI Parameters	Notes
☐	ACMG450	DigitConversionAdapter_te-systems.de		
☐	XSSA	XSSAAdapter_te-systems.de		

Select : All, None

Elements / Events / Groups & Roles / Licenses / Routing / Domains / Locations / Adaptations / SIP Entities / Entity Links / Time Ranges / Routing Policies / Dial Patterns / Regular Expressions / Defaults / Security / System Manager Data / Users

The digit conversion for incoming and outgoing calls from/to the Session Manager is used as follows. The `Matching Pattern 1` is related to the clients of the communication manager whilst the `Matching Pattern 77` is used for matching the application.

Home / Routing / Adaptations / Adaptation Details	

Adaptation Details   Commit Cancel

General

* Adaptation name: ACMG450

Module name: DigitConversionAdapter_te-systems.de

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item | Refresh   Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 1	* 3	* 3	* 0		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item | Refresh   Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 1	* 3	* 3	* 0		both	

Select : All, None

Home / Routing / Adaptations / Adaptation Details

Adaptation Details

Commit Cancel

General

* Adaptation name: XSSA
Module name: XSSAAdapter_te-systems.de
Module parameter:
Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item | Refresh

Filter: Enable

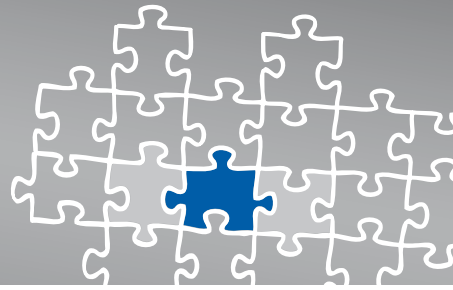|	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 77	* 3	* 3	* 0		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item | Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 77	* 3	* 3	* 0		both	

Select : All, None

3.4 SIP Entities

This example's SIP Entities (Communication Manager, Session Manager and the XCAPI/XSSA) are used as shown next.

Home / Routing / SIP Entities

- Elements
- Events
- Groups & Roles
- Licenses
- Routing
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- Security
- System Manager Data
- Users

SIP Entities

Edit New Duplicate Delete More Actions ▾

4 Items | Refresh

Filter: Enable

	Name	FQDN or IP Address	Type	Notes
☐	ACMG450	192.168.1.126	CM	
☐	ASM	192.168.1.199	Session Manager	
☐	XSSA	192.168.1.61	Other	

Select : All, None

Home / Routing / SIP Entities / SIP Entity Details

- ▶ Elements
- ▶ Events
- ▶ Groups & Roles
- Licenses
- ▼ Routing
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- ▶ Security
- ▶ System Manager Data
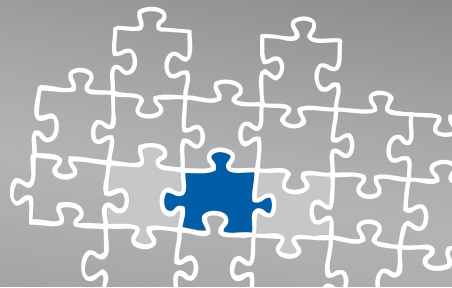- ▶ Users

Help

Help for SIP Entity Details fields

Help for Committing configuration changes

SIP Entity Details   Commit Cancel

General

* Name:	ASM
* FQDN or IP Address:	192.168.1.199
Type:	Session Manager
Notes:	
Location:	Laboratory Test Location
Outbound Proxy:	
Time Zone:	Europe/Berlin
Credential name:	

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

3 Items | Refresh   Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	ASM	TLS	* 5061	ACMG450	* 5061	☑
☐	ASM	TLS	* 5061	XSSA	* 5061	☑

Select : All, None

Port

Add Remove

2 Items | Refresh   Filter: Enable

	Port ▲	Protocol	Default Domain	Notes
☐	5061	TLS	te-systems.de	

Select : All, None

Home / Routing / SIP Entities / SIP Entity Details

- Elements
- Events
- Groups & Roles
- Licenses
- **Routing**
  - Domains
  - Locations
  - Adaptations
  - **SIP Entities**
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- Security
- System Manager Data
- Users

Help

Help for SIP Entity Details fields

Help for Committing configuration changes

SIP Entity Details   Commit | Cancel

General

* Name:	ACMG450
* FQDN or IP Address:	192.168.1.126
Type:	CM
Notes:	
Adaptation:	ACMG450
Location:	Laboratory Test Location
Time Zone:	Europe/Berlin
Override Port & Transport with DNS SRV:	☐
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	both

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration
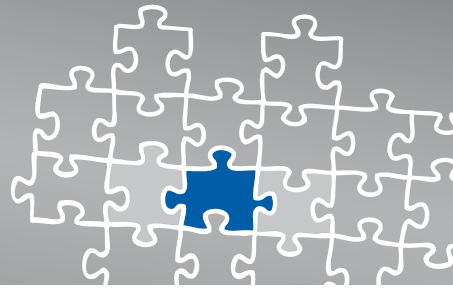
Entity Links

Add | Remove

1 Item Refresh   Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	ASM	TLS	* 5061	ACMG450	* 5061	☑

Select : All, None

* Input Required   Commit | Cancel

Home / Routing / SIP Entities / SIP Entity Details

- ▶ Elements
- ▶ Events
- ▶ Groups & Roles
- Licenses
- ▼ Routing
  - Domains
  - Locations
  - Adaptations
  - **SIP Entities**
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- ▶ Security
- ▶ System Manager Data
- ▶ Users

Help

Help for SIP Entity Details fields

Help for Committing configuration changes

SIP Entity Details

Commit Cancel

General

* Name:	XSSA
* FQDN or IP Address:	192.168.1.61
Type:	Other
Notes:	
Adaptation:	XCAPI
Location:	Laboratory Test Location
Time Zone:	Europe/Berlin
Override Port & Transport with DNS SRV:	☐
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item Refresh   Filter: Enable

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	ASM	TLS	* 5061	XSSA	* 5061	☑

Select : All, None

> For running plain SIP trunks via TCP, please use the SIP protocol stack with its default port (5060) for the `Entity Links`.

3.5 Entity Links

The `Entity Links`, one for the communication manager and the other for the XCAPI/XSSA, are related to the TLS protocol with its default port `5061`.

For running plain SIP trunks via TCP, please use the SIP protocol stack with its default port (5060) for the `Entity Links`.

3.6 Time Ranges

The `Time Ranges` are used with their default settings.

3.7 Routing Policies

The `Routing Policies` are used as shown next.

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details   Commit | Cancel

General

* **Name:** To-ACMG450

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACMG450	192.168.1.126	CM	

Time of Day

Add | Remove | View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add | Remove

2 Items | Refresh   Filter: Enable

	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	0	4	36	☐	te-systems.de	Laboratory Test Location	PSTN Calls
☐	1	3	3	☐	te-systems.de	Laboratory Test Location	ACM Clients

Select : All, None

Regular Expressions

Add | Remove

0 Items | Refresh   Filter: Enable

	Pattern	Rank Order	Deny	Notes

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details   Commit Cancel

General

* **Name:** To-XSSA

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
XSSA	192.168.1.61	Other	

Time of Day

Add   Remove   View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add   Remove

1 Item | Refresh   Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	77	3	3	☐	te-systems.de	Laboratory Test Location	XSSA via TLS/SRTP

Select : All, None

Regular Expressions

Add   Remove

0 Items | Refresh   Filter: Enable

	Pattern	Rank Order	Deny	Notes

3.8 Dial Patterns

The `Dial Patterns` for this environment are used as follows. Pattern 0 is used for allowing PSTN calls while pattern 1 is related to the communication manager clients. The dial pattern 77 is related to the XSSA/XCAPI. Ensure that the dial pattern configuration is consistent with the routing of the communication manager(s).

Home / Routing / Dial Patterns / Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

- **Elements**
- **Events**
- **Groups & Roles**
- Licenses
- **Routing**
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- **Security**
- **System Manager Data**
- **Users**

* Pattern: `1`

* Min: `3`

* Max: `3`

Emergency Call: ☐

SIP Domain: `te-systems.de ▼`

Notes: `ACM Clients`

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh   Filter: Enable

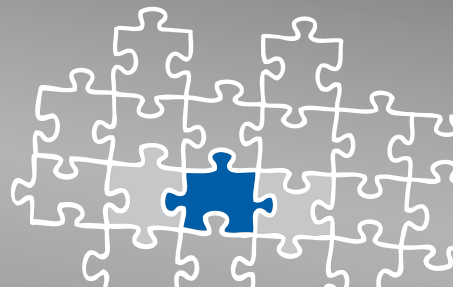|	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Laboratory Test Location		To-ACMG450	0	☐	ACMG450	

Select : All, None

Denied Originating Locations

Add Remove

0 Items | Refresh   Filter: Enable

	Originating Location	Notes
☐	Originating Location	Notes

Home / Routing / Dial Patterns / Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

- **Elements**
- **Events**
- **Groups & Roles**
- Licenses
- **Routing**
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
  - Defaults
- **Security**
- **System Manager Data**
- **Users**

* Pattern: `77`

* Min: `3`

* Max: `3`

Emergency Call: ☐

SIP Domain: `te-systems.de ▼`

Notes: `XSSA via TLS/SRTP`

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh   Filter: Enable

	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Laboratory Test Location		To-XSSA	0	☐	XSSA	

Select : All, None

Denied Originating Locations

Add Remove

0 Items | Refresh   Filter: Enable

	Originating Location	Notes
☐	Originating Location	Notes

Transport Layer Security

TLS (Transport Layer Security) is supported from XCAPI version 3.3.129. You can freely skip this chapter if run plain SIP trunk within your VoIP environment. The requirements and configuration procedure will be described in the next sections.

4.1 XCAPI SIP Security Additions

For using XCAPI SIP Security Additions (XSSA) it is necessary to run the XSSA installer, currently xssa-1.2.10-r2438, on the application/XCAPI server.

It is also possible to use the XCAPI SIP Security Additions (XSSA) application for generating RSA keys, self-signed certificates and certificate signing requests.

Please note that those RSA keys will be generated within the folder where the xssa-ldr executable is called.

RSA Keys

For this example the XSSA-loader (xssa-ldr) is used to generate a 2048 bit RSA key via the command line interface. The private key is stored as 192.168.1.61-private.pem whilst the 192.168.1.61-public.pem filename is used for the public key.

The command line for this is used as follows:

```
C:\>xssa-ldr crytool generate rsa --bits=2048 --private=192.168.1.61-private.pem
--public=192.168.1.61-public.pem
```

CA-Signed Certificate

The private key can also be used to generate a CSR (Certificate Signing Request) file for requesting a CA-signed certificate. Please set the values for the parameters cn and idn to the IP address of your XCAPI server.

The next example shows how to create the 192.168.1.61-csr.pem file which is used for requesting a CA-signed certificate.

```
C:\>xssa-ldr crytool generate csr --private=192.168.1.61-private.pem --cn=192.168.1.61--idn=192.168.1.61
--csr=192.168.1.61-csr.pem
```

TE-SYSTEMS
competence in e-communications.

4.2 Add End Entity

Add a new `End Entity` using the predefined `INBOUND_OUTBOUND_TLS` profile and define a new username and password. The `CN, Common Name` field has to match the IP address of the XCAPI server. The value `Certificate Profile` has to be set to `ID_CLIENT_SERVER`. Select `PEM file` as value for the `Token` field and click `Add End Entity` to create the new user profile.

The username and password values will be used in the next step, enrolling a server certificate for the XSSA.

Enroll the server certificate for the XSSA with the content from the CSR file generated in step
4.1, CA-signed Certificate.

4.3 Preparing the XSSA CA Certificate

Save the file with the generated XSSA certificate to your local system and open the file with a text editor. Copy and paste the part of the `private key` and `certificate` and store them to separate `.pem` files.

```
Bag Attributes
    friendlyName: 192.168.1.61
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAIkGKe2GUU42vwMe
jL4tL7BAI+dA4VoJXTIMQ3kIz6+GTF4kjV7e07tZvtgNNQTOH7QjoCFzFydjh792
AK6EW/oGXi9r/iQtDqzlgRPbbPV3oU8Qpal6IgIvAX1PtoQNVoCBv7YBG8TTFSwt
B2tzkgjXRxMrc5Gv7ggMryjyPLq5AgMBAAECgYBbaMk/s4M58jurEQ5DMFHH+oH5
G8c6EVUithus+rvSFH2NsES/LVeCfHRcHTNpaTitK7b/mY+wry04BLifs5zHSgZU
iSoDhWJyAti5H0gCuLJJIdgqPa0YKM9JEkO496xHsmVYMPGlIMlIgaVGCku4pNnJ
Sqc7oz9cbaXeorlQAQJBANnlU9RAOL/tTNwyT3/ld43Wg/mPlXFwN7HNVNkVRerx
m8Kf4Ilqn7soHjRL6fvWA/Y+VhXD8/k8rzkGU0hmVMECQQCg/Gckg+Ze5t7/jFfS
LWZkxiU1aauJ5JUBij7YdTz2hYwUW2+ngiwPFPUsmeu2HqeEOQuRiYrSOB4mOzIV
EAv5AkA8tdzJgqtNLnz/zTTBWdoZtu9GlW76EF40OBWv9nFoqLDRZWJW21Lh/qeL
wqsK8/JepbeukM5lXzcjGFQUFA8BAkAnUJzL0R6AjLdnB1onLQk1kSJfOag328f8
AUwJxs/ee3vTOHQCD4s8/6xEgS6MYn4cj2Xg3As3/Zz3VbuMY0fZAkEAzK7EL6j0
S/vWWkKIU+ADETLuT71Bk949wTuv+q2WU1fpM5enhqfRdnUP4V4mn2Nf589HdXZu
kJh8PZMNsy2Q0Q==
-----END PRIVATE KEY-----
Bag Attributes
    friendlyName: 192.168.1.61
subject=/CN=sascha.te-systems.de/CN=
192.168.1.61/OU=SDP/O=AVAYA/C=US
issuer=/CN=default/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIICjjCCAfegAwIBAgIIBH2FOptlduUwDQYJKoZIhvcNAQEFBQAwMTEQMA4GA1UE
AwwHZGVmYXVsdDENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTAx
MTAzMDkzNDIxWhcNMTIxMTAyMDkzNDIxWjBhMR0wGwYDVQQDDBRzYXNjaGEudGUt
c3lzdGVtcy5k2TEVMBMGA1UEAwwMMTkyLjE2OC4xLjYxMQwwCgYDVQQLDANTRFAx
DjAMBgNVBAoMBUFWQVlBMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAiQYp7Y2RTja/Ax6Mvi0vsEAj50DhWgldMgxDeQjPr42MXiSNXt7T
u1m+2A01BM4ftCOgIXMXJ2OHv3YAroRb+gZeL2v+JC0OrOWBE9ts9XehTxClqXoi
Ai8BfU+2hA1WgIG/tgEbxNMVLC0Ha3OSCNdHEytzka/uCAyvKPI8urkCAwEAAaN/
MH0wHQYDVR0OBBYEFBnU4cR9qCvaGy87CLBo+TABdqmPMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU9781Tnegzn2HfDStTK6+tTVX5ukwDgYDVR0PAQH/BAQDAgP4
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQUFAAOB
gQAO9zMXhX8jilMpzii8r8EJEg5obO+I8G2ximWcWu4CgDG7f92M9HGn8L/iOqLo
cJFuKd85eTxVq7yUDQH+UCQkZZrmptcv2zvIPi+Hr1AA3ycpShHce+W7dO5rkitm
gMsB649tXv7WdKV4N9Pza2pIJaE8hafphCSXeTm0RoMxdQ==
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: default
subject=/CN=default/OU=MGMT/O=AVAYA
issuer=/CN=default/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIICQjCCAaugAwIBAgIIVNfMFz/W1rYwDQYJKoZIhvcNAQEFBQAwMTEQMA4GA1UE
AwwHZGVmYXVsdDENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTAx
MDI1MDgwNzQ2WhcNMjAxMDIyMDgwNzQ2WjAxMRAwDgYDVQQDDAdkZWZhdWx0MQ0w
CwYDVQQLDARNR01UMQ4wDAYDVQQKDAVBVkFZQTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAmuRGfV3HELyWL7M4EaG6NJLGfGYGWYZphUQBYzUllPiaG1UYsLfn
RwSCEhIqfqb0RtPpMpNOBUIa7riLQw3SeOXCaacutWJbmPsBdq+WRQp7r6xqlQIv
X+ZVB5sMSfPWR0GCFCdLqziCpl0g296PiJJJzKppeQdBhORw/FJ8NwkCAwEAAaNj
MGEwHQYDVR0OBBYEFPe/JU53oM59h3w0rUyuvrU1V+bpMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU9781Tnegzn2HfDStTK6+tTVX5ukwDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBBQUAA4GBAIw980tjSlEvztUKU7GeDXkpo91K884/rd0c
KBv/924awMtBiq276O9cwl58cX/x7wAXmLLyT7OQkxBVCRjxh+PneMZ/frB8/3Qf
WLJxjAdxlLry6KiHVvKmzjAjcu2bLdtpUAnRw2t/eV3XysuE7frdVn+fCm2y516F
P1cUa/BE
-----END CERTIFICATE-----
```
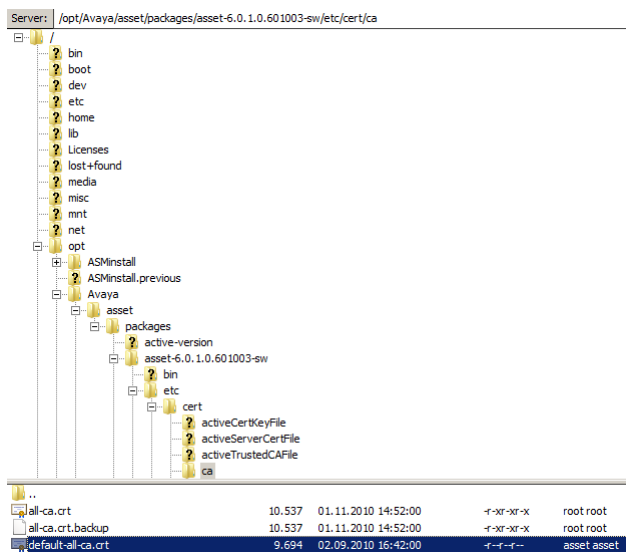
Import the certificate that has been signed by the System Manager CA and its private key into the XCAPI configuration.
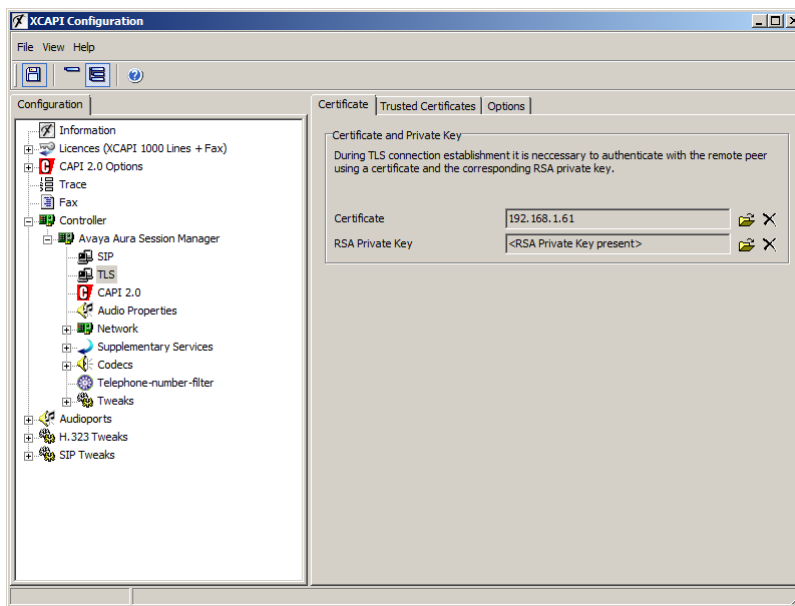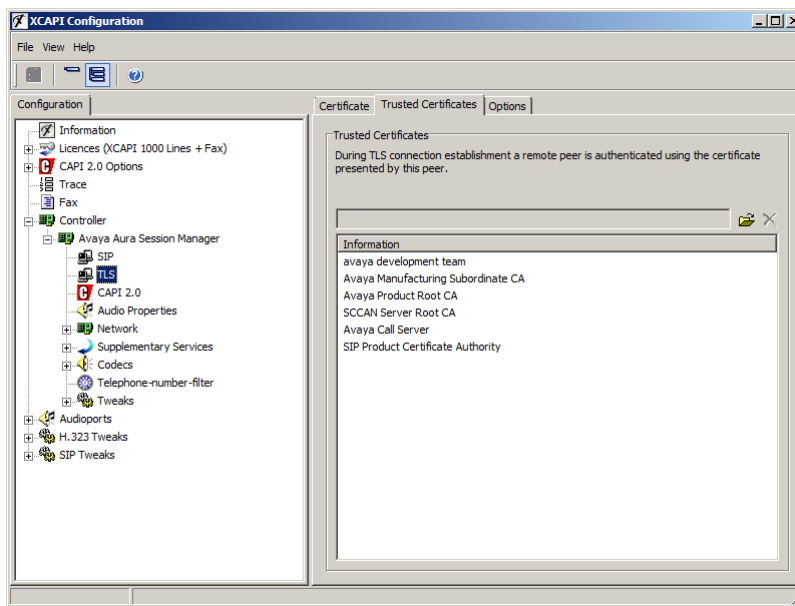

Download the required Avaya Aura Session Manager CA certificate from /opt/Avaya/asset/packages/active-version/etc/cert/ca.
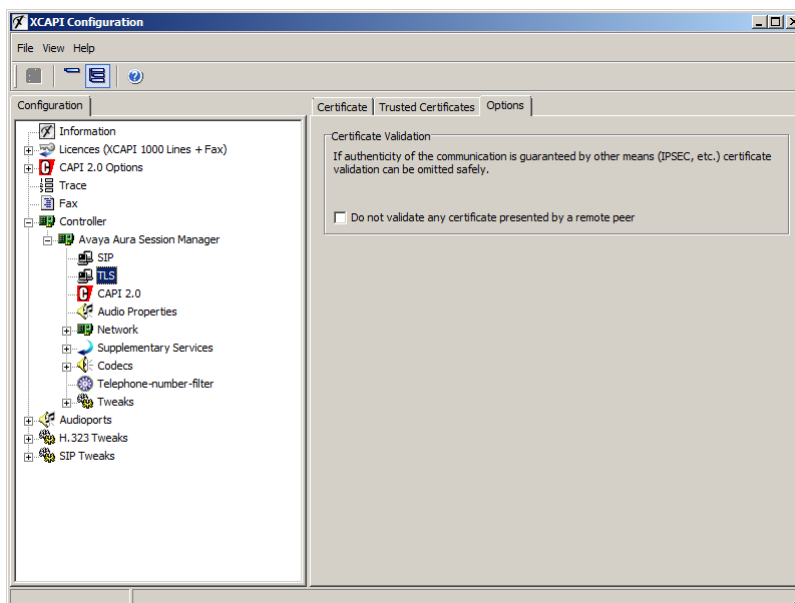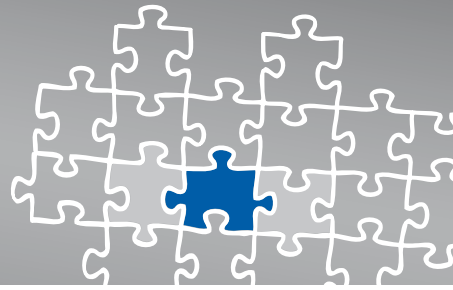
Make a backup of this file, rename it by your needs (session-manager-ca.pem) and change the file type to `.pem` for importing the file as trusted certificate into the XCAPI controller.

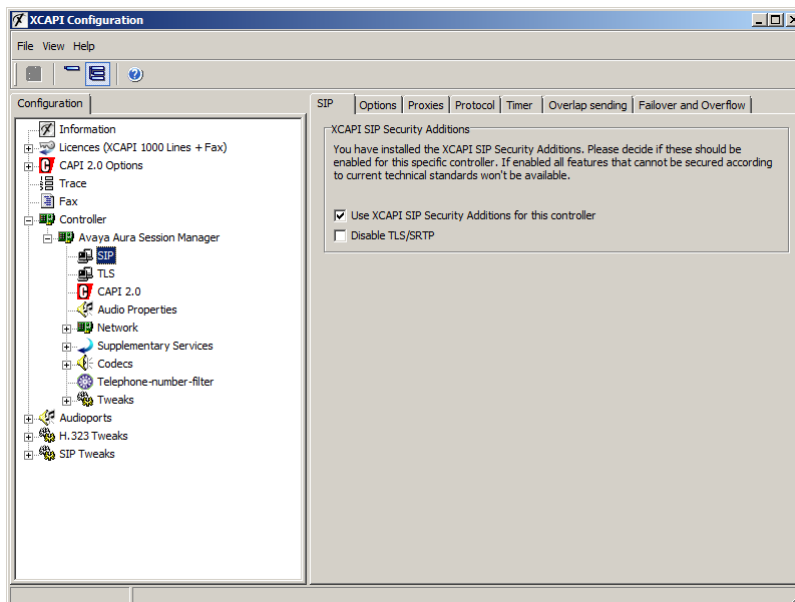The `Do not validate any certificate presented by a remote peer` should `NOT` be enabled.

4.4 XCAPI Controller - Configuring TLS/SRTP

Review the XCAPI controller settings for enabling TLS/SRTP capabilities.

The setting `Use XCAPI SIP Security Additions for this controller` must be enabled for using TLS and SRTP.
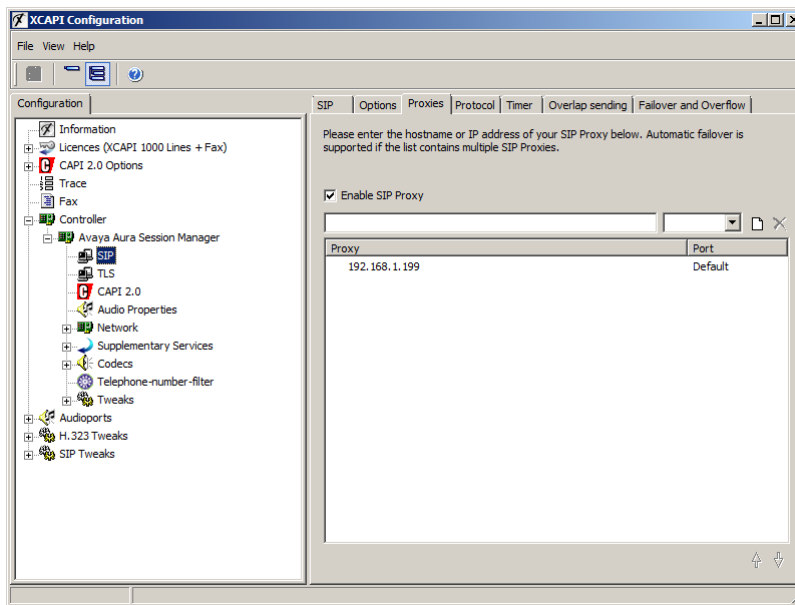

The `Default SIP Domain` must be equivalent to your environment. For this example the SIP domain is used as shown in the chapter `Domains` on page 7.
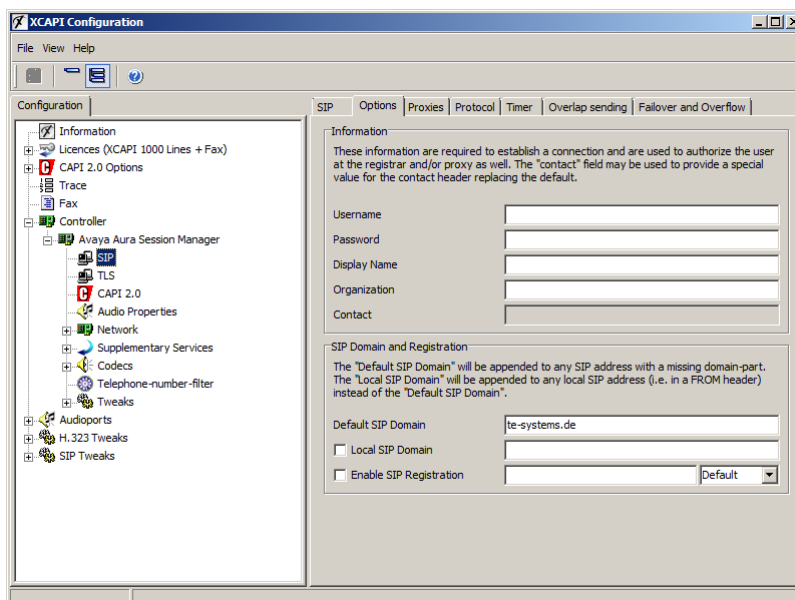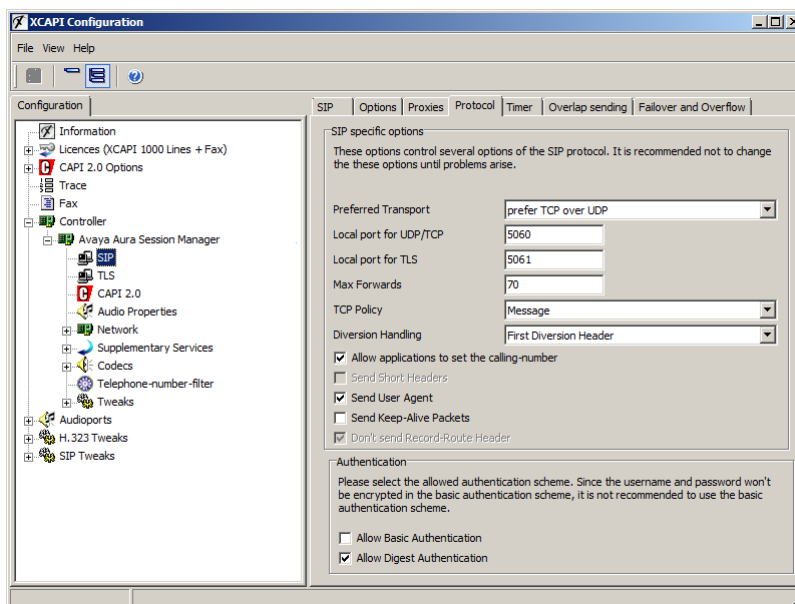
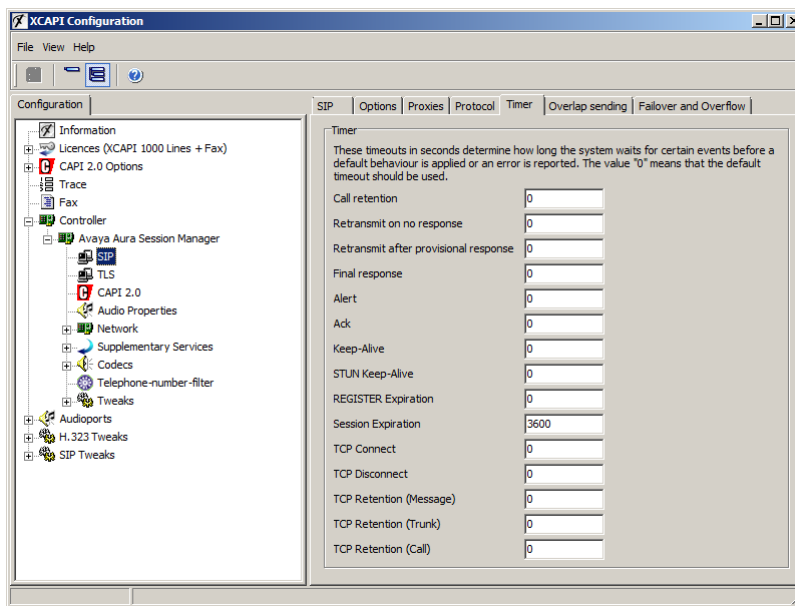The proxy is related to the Avaya Aura Session Manager's SM-100 interface.

The protocol settings should be used with their default values.
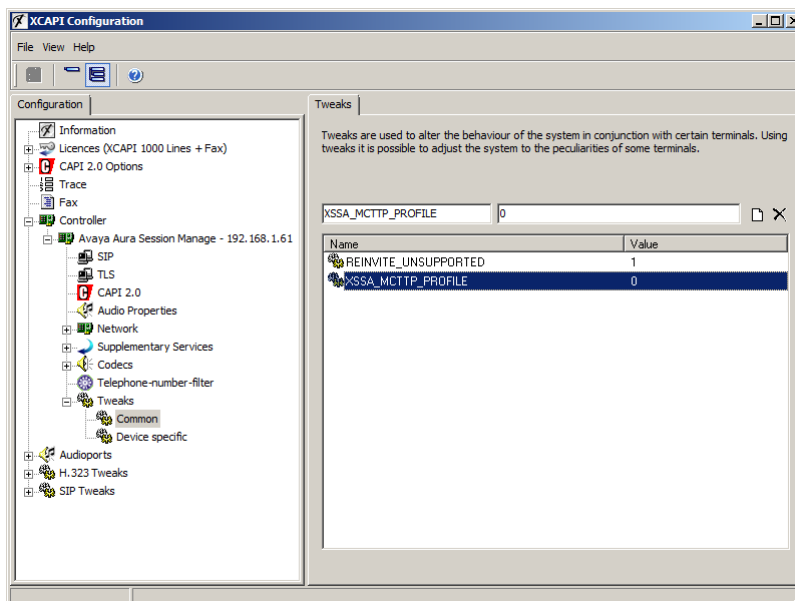
The Session Expiration timer must be equivalent with the values of the session and communication manager.

Please ensure that the XCAPI controller tweak XSSA_MCTTP_Profile is valued with 0 for enabling TLS/SRTP interoperability between the XSSA and the Avaya Aura Session Manager.

Secure Real-Time Transport Protocol

For running SRTP, which is necessary when using XSSA proxy with enabled transport layer security, you have to ensure that the SIP entities, SIP clients and media gateways are using the correct media encryption values.

Beside of the communication managers IP codec set(s), it is also important to enable the according media encryption for all involved session manager SIP clients within the `46xxsettings.txt` configuration file.

> For XSSA/TLS/SRTP interoperability, the media encryption value must be used with `1-srtp-aescm128-hmac80`. For plain SIP trunking via TCP, please set the media encryption values to `none`.

SIP Trunking without TLS/SRTP

If using the SIP via TCP protocol method between the communication manager, the session manager and the XCAPI/XSSA you have to ensure that the according protocol settings for the `SIP Entities`, `SIP Links` and, if needed, the communication managers `Signaling Group` is related to the SIP/TCP transport method and the default port value `5060`. Further, any media encryption has to be disabled for the communication manager(s) IP codec set(s) and the session manager(s) SIP clients.

Ensure that the XCAPI SIP controller option `Disable TLS/SRTP` is active.
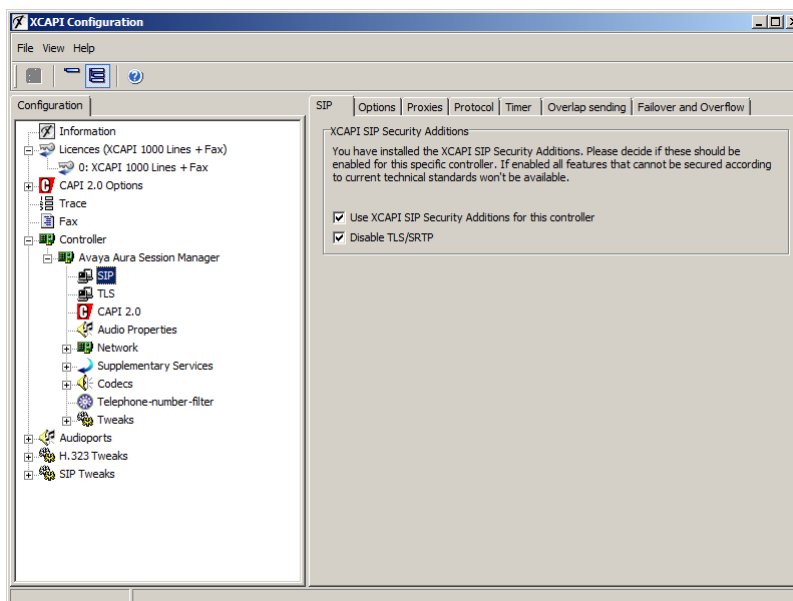
Fax Services

In this chapter, we are going to describe the necessary configuration for using Fax services in meaning of T.38 and `Softfax`.
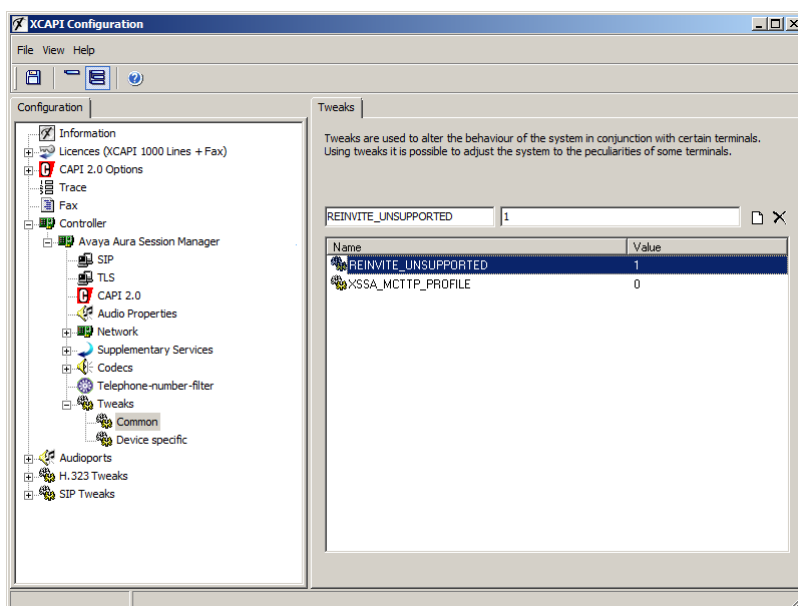
7.1 Software Fax

With the software fax mode, the XCAPI simulates an analogue Fax device by transmitting modulated Fax-signals modem-like over the established audio channels. To configure the software fax mode, please open the XCAPI configuration utility and select in the advanced configuration mode the SIP controller assigned to the gateway.

Open the configuration tab labeled `Features`. Enable the `Softfax` mode by setting the `Always use software fax over audio channels option` and save the changes to the XCAPI controller configuration.
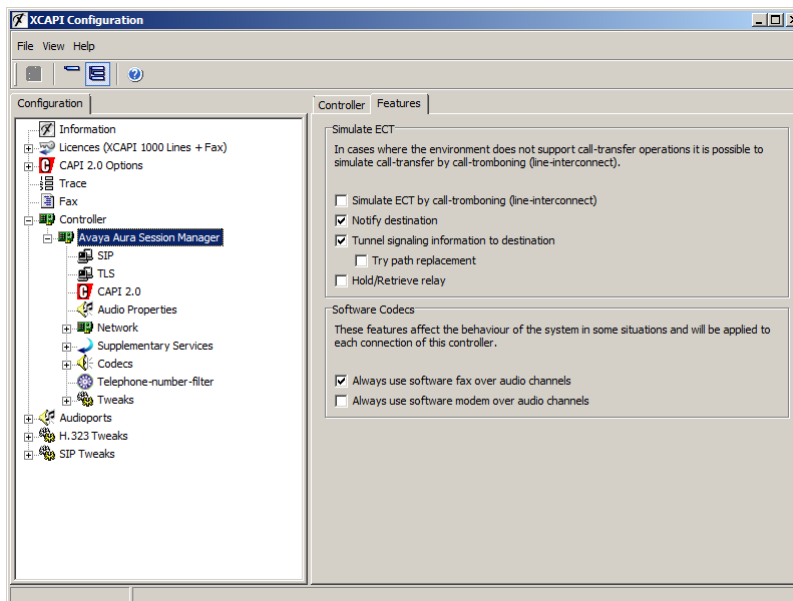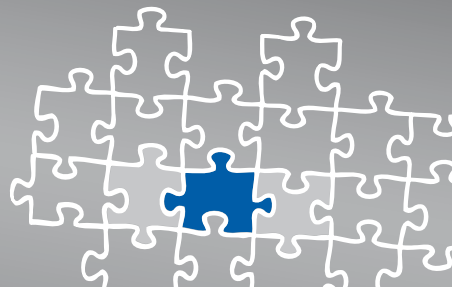
Please review the XCAPI controller tweaks and ensure that the REINVITE_UNSUPPORTED tweak is enabled (valued by 1) for interoperability reasons. This tweak will suppress any further SIP invites for refreshing the current SIP session.
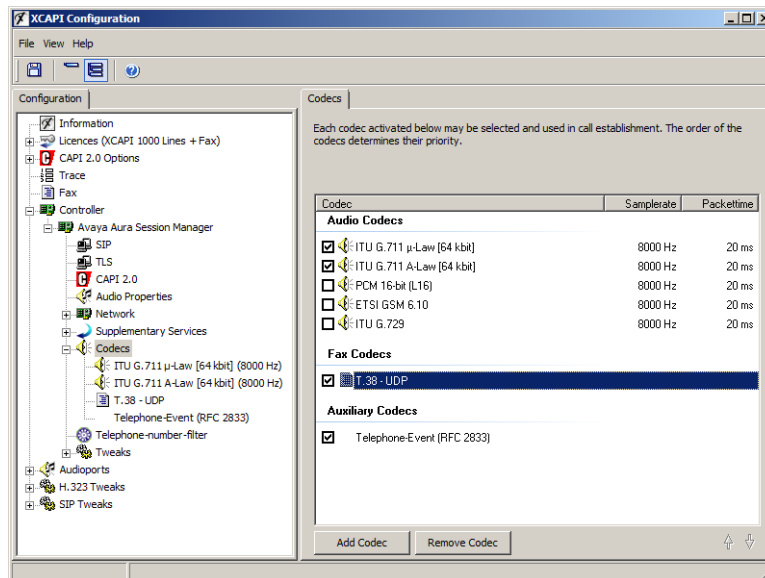

You have to use Software Fax for facsimile interoperability within TLS/SRTP environments. Ensure that all T.38-related settings within the IP codec set(s) are disabled.
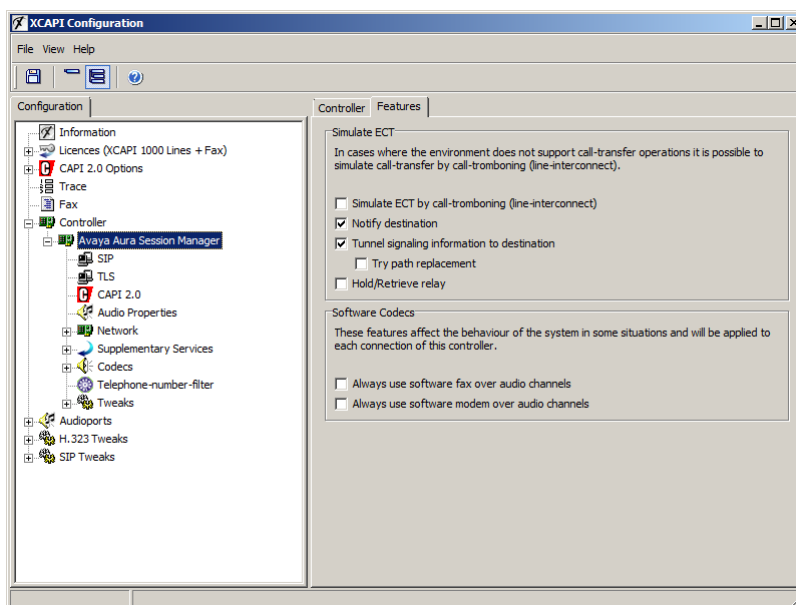
7.2 T.38 Fax

Please ensure that T.38 is enabled and capable for the involved media gateway(s).

When using T.38 it is mandatory that `T.38 - UDP` Codec is enabled within the XCAPI controller configuration.

The option `Always use software fax over audio channels` has to be disabled within the XCAPI controller's `Features` tab configuration.

Please note that `T.38` is not supported within TLS/SRTP environments.

Exclusion of Liability

Copyright © 2010 TE-SYSTEMS GmbH

Trademarks

All names of products or services used are trademarks or registered trademarks (also without specified indication) of the respective private or legal persons and are therefore subject to legal regulations.

Third Party Disclaimer and Limitations

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes source code derived from the RSA Data Security, Inc. MD2, MD4 and MD5 Message Digest Algorithms.

This product includes source code derived from the RFC 4634 Secure Hash Algorithm software.