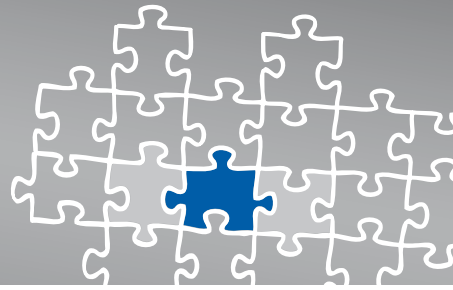


TechNote

Avaya Aura Session Manager 6.0

Stand: 9. Dezember 2010





Zusammenfassung

Dieses Dokument unterstützt sie bei der Integration der XCAPI 3.3.161 in ein bestehendes Umfeld des Avaya Aura Session Manager. Um eine optimale Zusammenarbeit beider Komponenten unter Verwendung des SIP-Protokolls zu gewährleisten, werden nachfolgend die nötigen Konfigurationsschritte erläutert.

Es wird vorausgesetzt, dass die eingesetzte Hardware betriebsbereit und die Software, insbesondere die der verwendeten CAPI-Applikation, installiert und für die Verwendung mit der XCAPI konfiguriert ist.

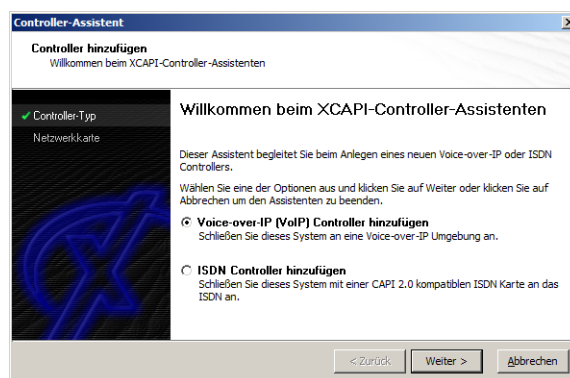
Bei technischen Fragen zur Installation und Konfiguration der Produkte anderer Hersteller konsultieren sie bitte die dafür vorgesehenen Dokumentationen.

Für eine Unterstützung der XCAPI-Installation steht das XCAPI-Handbuch auf unserer Website <http://www.xcapi.de> zur Verfügung.

XCAPI-Konfiguration

Starten sie die XCAPI-Konfiguration, um einen neuen Controller einzurichten. Sollte der XCAPI-Konfiguration noch kein Controller bekannt sein, werden sie direkt nach dem Start von dem XCAPI-Controller-Assistenten bei der Einrichtung unterstützt. Sollten bereits konfigurierte Controller vorhanden sein, können sie ebenfalls mit Hilfe des Assistenten einen neuen Controller anlegen. Wählen sie zunächst in der Übersicht der XCAPI unter dem Controller-Dialog den Punkt Klicken sie hier um einen neuen Controller zu konfigurieren aus.

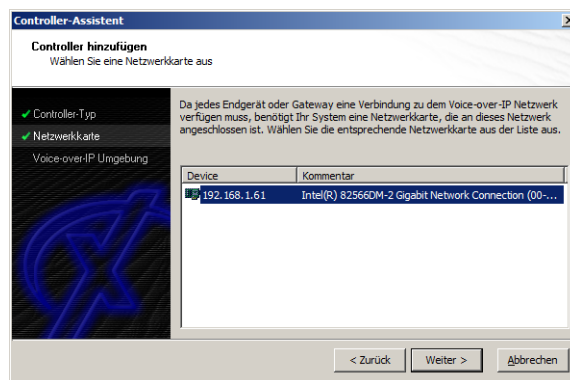
Anschließend, sofern nicht automatisch ausgewählt, im Controller hinzufügen-Dialog die Option Voice-over-IP (VoIP) Controller hinzufügen. Mit der Weiter-Schaltfläche gelangen sie zu dem nächsten Konfigurationsdialog.





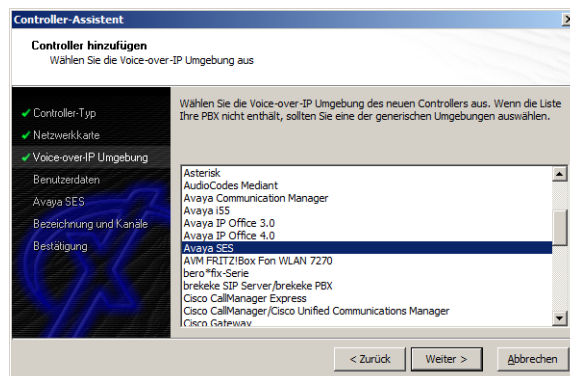
2.1 Auswahl der Netzwerkkarte

Wählen sie in diesem Dialog die Netzwerkkarte aus, die der Controller für die VoIP (Voice-over-IP) Kommunikation verwenden soll.



2.2 Voice-over-IP-Umgebung

Selektieren sie in dem Dialog Controller Hinzufügen den Eintrag Avaya SES (eine separate Auswahl für den Session Manager ist derzeit nicht verfügbar) aus. Dadurch wird die erfahrungsgemäß bestmögliche Vorauswahl der nötigen Konfigurationseinstellungen übernommen und ihnen eine manuelle Konfiguration erspart.





2.3 Benutzerdaten

Für die Einrichtung der XCAPI als vertrauenswürdigen Host sind keine Benutzerdaten notwendig.

Controller-Assistent

Controller hinzufügen
Geben Sie die SIP-Benutzerdaten ein

Das entfernte Gerät erfordert die Authentisierung eines Benutzers. Geben Sie entsprechende Benutzerdaten ein. Falsche Benutzerdaten können dazu führen, dass eine Kommunikation mit dem Gerät nicht möglich ist.

- ✓ Controller-Typ
- ✓ Netzwerkkarte
- ✓ Voice-over-IP Umgebung
- ✓ Benutzerdaten
- Avaya SES
- Bezeichnung und Kanäle
- Bestätigung

Benutzername (SIP-ID)

Passwort (SIP-PASSWORT)

Angezeigter Name

Organisation

< Zurück Weiter > Abbrechen

2.4 IP-Adresse des Avaya Aura Session Manager

In diesem Konfigurationsdialog geben sie die IP-Adresse der SM-100 Schnittstelle des Avaya Aura Session Manager ein.

Controller-Assistent

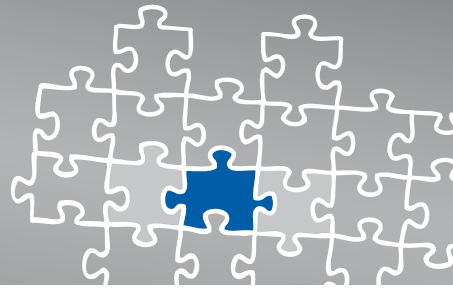
Controller hinzufügen
Geben Sie die Adresse des Avaya SES-Systems ein

Geben Sie die IP-Adresse des Avaya SES-Systems ein. Sollten sich mehrere Avaya SES-Systeme in Ihrem Netzwerk befinden, vergewissern Sie sich bitte, dass Sie den Hostnamen oder die IP-Adresse des korrekten Avaya SES-Systems eingeben.

- ✓ Controller-Typ
- ✓ Netzwerkkarte
- ✓ Voice-over-IP Umgebung
- ✓ Benutzerdaten
- ✓ Avaya SES
- Bezeichnung und Kanäle
- Bestätigung

Netzwerk-Adresse

< Zurück Weiter > Abbrechen



2.5 Controller-Bezeichnung und Anzahl der Leitungen

In dem vorletzten Konfigurationsdialog des XCAPI-Controller-Assistenten vergeben sie eine Bezeichnung für den neu angelegten Controller und tragen die Anzahl der verfügbaren Leitungen ein, die der XCAPI zur Verfügung stehen sollen.

Controller-Assistent

Controller hinzufügen
Geben Sie eine Beschreibung und die Anzahl der Leitungen ein

Geben Sie eine sinnvolle Bezeichnung für diesen Controller und die Anzahl der Leitungen ein. Bitte beachten Sie, dass die effektive Anzahl der Leitungen von der installierten Lizenz abhängt.

Bezeichnung:

Leitungen:

< Zurück Weiter > Abbrechen

2.6 Controller fertigstellen

Verwenden sie abschließend die Fertigstellen-Schaltfläche, um den neuen Controller anzulegen.

Controller-Assistent

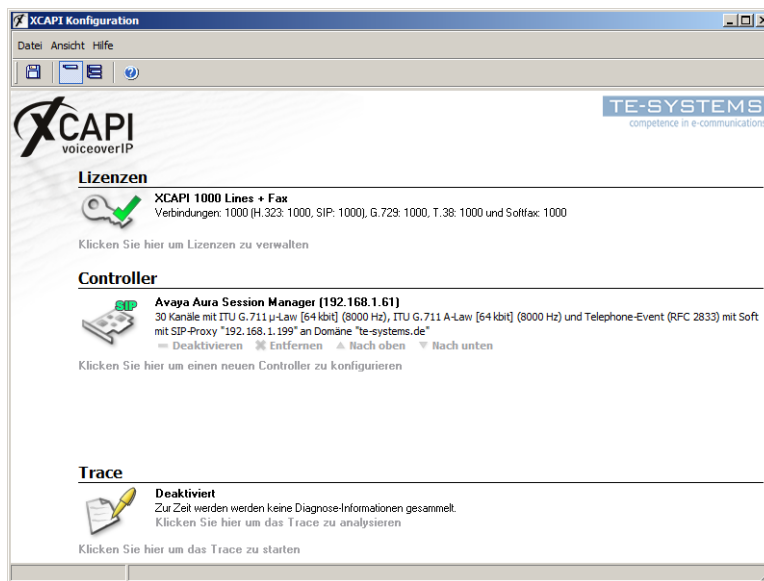
Controller hinzufügen
Bestätigen Sie die eingegebenen Informationen

Klicken Sie auf Fertigstellen um der Konfiguration den neuen Controller hinzu zu fügen.

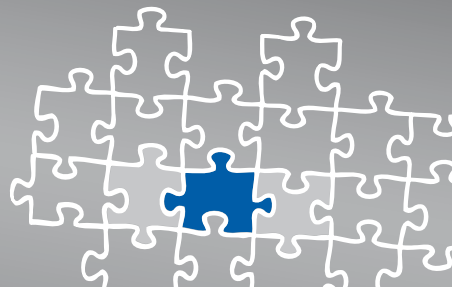
< Zurück **Fertigstellen** Abbrechen



Der angelegte SIP-Controller wird nun in der Übersicht der XCAPI-Konfiguration angezeigt. Speichern sie abschließend den neu konfigurierten XCAPI-Controller ab.



Beachten Sie, dass die vorgenommenen Änderungen des XCAPI-Controllers erst nach dem Speichern und anschließendem Neustart der angebundenen CAPI-Applikation wirksam werden.



Konfiguration des System Managers

Um eine Kommunikation zwischen der XCAPI und dem Avaya Aura Session Manager zu ermöglichen, muss die XCAPI als SIP Entity mit den dazugehörigen Konfigurationen eingerichtet werden.

Die dafür nötigen Konfigurationsschritte werden in den nachfolgenden Kapiteln erläutert.

3.1 Domains

In diesem VoIP-Umfeld wird für das Domänen-basierte Routing die SIP-Domäne `te-systems.de` verwendet.

AVAYA Avaya Aura™ System Manager 6.0

Home / Routing / Domains

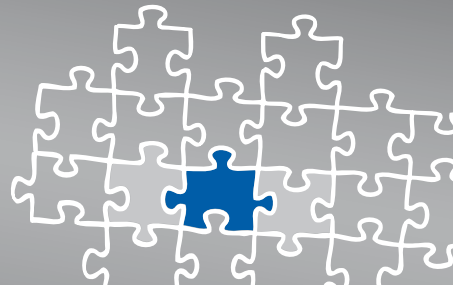
Domain Management

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	te-systems.de	sip	<input type="checkbox"/>	

Select : All, None



3.2 Locations

Die Location trägt in diesem Beispiel die Bezeichnung Laboratory Test Location.

Home / Routing / Locations

Location

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#)

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Laboratory Test Location	

Select : All, None

Für die Location werden die Default-Einstellungen verwendet.

Home / Routing / Locations / Location Details

Location Details

General

* Name:

Notes:

Managed Bandwidth: Kbit/sec

* Average Bandwidth per Call: Kbit/sec

Location Pattern

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

* Input Required



3.3 Adaptations

Die Adaptions werden wie folgt verwendet.

Home / Routing / Adaptations

- ▶ 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

Adaptations

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) ▼

2 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	ACMG450	DigitConversionAdapter_te-systems.de		
<input type="checkbox"/>	XSSA	XSSAAadapter_te-systems.de		

Select : All, None

Als Digit Conversion für ein- und ausgehende Rufe zwischen dem Session Manager und dem Communication Manager wird der ACM-Client-bezogene Matching Pattern 1 verwendet und der Matching Pattern 77 wird der Applikation zugeordnet.

Home / Routing / Adaptations / Adaptation Details

Adaptation Details [Commit](#) [Cancel](#)

General

* Adaptation name:

Module name: ▼

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*1	*3	*3	*0		both	

Select : All, None

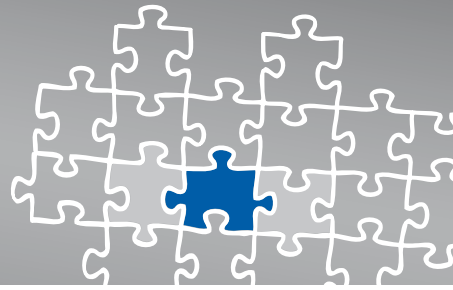
Digit Conversion for Outgoing Calls from SM

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*1	*3	*3	*0		both	

Select : All, None



Adaptation Details

Commit Cancel

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*77	3	3	0		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*77	3	3	0		both	

Select : All, None

3.4 SIP Entities

Die in diesem Konfigurationsbeispiel verwendeten SIP Entities (Communication Manager, Session Manager und XCAPI/XSSA) werden folgendermaßen verwendet.

- ▶ 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

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ACMG450	192.168.1.126	CM	
<input type="checkbox"/>	ASM	192.168.1.199	Session Manager	
<input type="checkbox"/>	XSSA	192.168.1.61	Other	

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

Help

Help for SIP Entity Details fields
 Help for Committing configuration changes

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM	TLS	* 5061	ACMG450	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ASM	TLS	* 5061	XSSA	* 5061	<input checked="" type="checkbox"/>

Select : All, None

Port Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5061	TLS	te-systems.de	<input type="text"/>

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

Help

Help for SIP Entity Details fields
 Help for Committing configuration changes

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM	TLS	* 5061	ACMG450	* 5061	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel



Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

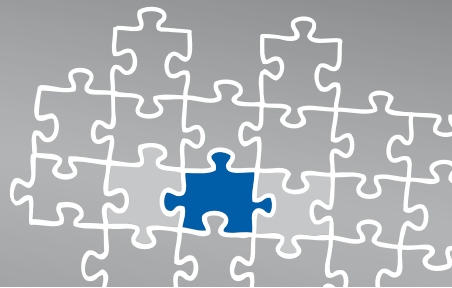
Add Remove

1 Item Refresh Filter: Enable						
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM	TLS	*5061	XSSA	*5061	<input checked="" type="checkbox"/>

Select : All, None



Bei reinen SIP-Trunk-Anbindungen via TCP muss der SIP-Protokoll-Stack mit dem Default-Port (5060) verwendet werden.



3.5 Entity Links

Die Entity Links für den Communication Manager und die XCAPI/XSSA werden mit dem TLS-Protokoll und dem Default-Port 5061 verwendet.

Home / Routing / Entity Links

Entity Links

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#)

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	ASM_ACMG450_5061_TLS	ASM	TLS	5061	ACMG450	5061	<input checked="" type="checkbox"/>	—
<input type="checkbox"/>	XSSA	ASM	TLS	5061	XSSA	5061	<input checked="" type="checkbox"/>	—

Select : All, None



Bei reinen SIP-Trunk-Anbindungen via TCP muss der SIP-Protokoll-Stack mit dem Default-Port (5060) verwendet werden.



3.6 Time Ranges

Die Einstellungen im Dialog Time Ranges werden mit den Default-Vorgaben verwendet.

Home / Routing / Time Ranges

- 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

Time Ranges

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

3.7 Routing Policies

Die Routing Policies werden wie folgt verwendet.

Home / Routing / Routing Policies

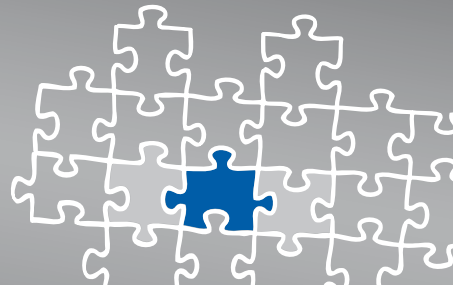
- Elements
- Events
- Groups & Roles
- Licenses
- ▾ Routing
 - Domains
 - Locations
 - Adaptations
 - SIP Entities
 - Entity Links
 - Time Ranges
 - Routing Policies
 - Dial Patterns
 - Regular Expressions
 - Defaults
- Security
- System Manager Data
- Users

Routing Policies

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To-ACMG450	<input type="checkbox"/>	ACMG450	
<input type="checkbox"/>	To-XSSA	<input type="checkbox"/>	XSSA	

Select : All, None



Routing Policy Details

[Commit](#) [Cancel](#)

General

* Name:

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

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

[Add](#) [Remove](#)

2 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	0	4	36	<input type="checkbox"/>	te-systems.de	Laboratory Test Location	PSTN Calls
<input type="checkbox"/>	1	3	3	<input type="checkbox"/>	te-systems.de	Laboratory Test Location	ACM Clients

Select : All, None

Regular Expressions

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------



Routing Policy Details

[Commit](#) [Cancel](#)

General

* Name:

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](#)

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	77	3	3	<input type="checkbox"/>	te-systems.de	Laboratory Test Location	XSSA via TLS/SRTP

Select : All, None

Regular Expressions

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------



3.8 Dial Patterns

Der Rufnummernplan (Dial Patterns) wird für dieses Konfigurationsbeispiel wie folgt verwendet. Der Dial Pattern 0, für Amtsverbindungen, und der Dial Pattern 1, für ACM-Clients, werden dem Communication Manager zugeordnet. Der Dial Pattern 77 wird für das Routing zur CAPI-Applikation (via XCAPI/XSSA) verwendet.

Home / Routing / Dial Patterns

- 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

Dial Patterns

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) ▾

4 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	0	4	36	<input type="checkbox"/>	te-systems.de	PSTN Calls
<input type="checkbox"/>	1	3	3	<input type="checkbox"/>	te-systems.de	ACM Clients
<input type="checkbox"/>	77	3	3	<input type="checkbox"/>	te-systems.de	XSSA via TLS/SRTP

Select : All, None

Home / Routing / Dial Patterns / Dial Pattern 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

Dial Pattern Details

[Commit](#) [Cancel](#)

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Laboratory Test Location		To-ACMG450	0	<input type="checkbox"/>	ACMG450	

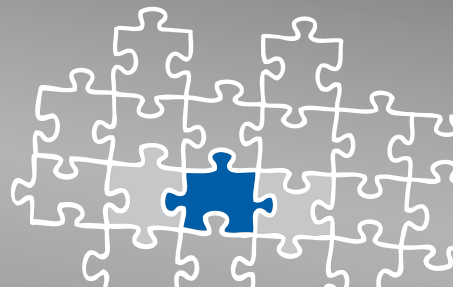
Select : All, None

Denied Originating Locations

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>		



Home / Routing / Dial Patterns / Dial Pattern 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

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Laboratory Test Location		To-ACMG450	0	<input type="checkbox"/>	ACMG450	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Home / Routing / Dial Patterns / Dial Pattern 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

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Laboratory Test Location		To-XSSA	0	<input type="checkbox"/>	XSSA	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------



Transport Layer Security

Ab der XC-API-Version 3.3.129 wird das TLS (Transport Layer Security)-Verfahren unterstützt. Die dafür nötigen Voraussetzungen und Vorgehensweisen werden anhand eines Konfigurationsbeispiels in den nachfolgenden Kapiteln erläutert.

4.1 XC-API SIP Security Additions

Um den Einsatz der XC-API SIP Security Additions zu ermöglichen, muss der XSSA-Installer (derzeit `xssa-1.2.10-r2438`) auf dem XC-API-Server installiert werden.

Bei Bedarf können mit Hilfe des XC-API SIP Security Additions (XSSA) eigene RSA-Schlüsselpaare, selbstsignierte Zertifikate und Certificate Signing Requests erstellt werden.

Beachten Sie, dass die über das XSSA erstellten Schlüssel bzw. Zertifikate in dem aktuellen Verzeichnis generiert werden, in dem das Kommandozeilen-Programm `xssa-ldr` aufgerufen wird.

RSA-Schlüssel

Mit Hilfe des XSSA-Loaders (`xssa-ldr`) wird für dieses Konfigurationsumfeld der benötigte RSA-Schlüssel via Kommandozeile mit einer Verschlüsselungsstärke von 2048 Bit erstellt.

Der private Schlüssel wird dabei in der Datei `192.168.1.61-private.pem` und der öffentliche Schlüssel in der Datei `192.168.1.61-public.pem` abgelegt.

Die Kommandozeile wird dafür wie nachfolgend aufgezeigt ausgeführt:

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

CA-signiertes Zertifikat

Bei Bedarf kann mit dem generierten privaten Schlüssel eine CSR (Certificate Signing Request)-Datei erstellt werden.

In dem nachfolgend aufgeführten Beispiel wird die Datei `192.168.1.61-csr.pem` mit den benötigten Parametern und Angaben erstellt, die für ein CA-signiertes Zertifikat benötigt wird. Die Parameter `cn` und `idn` müssen mit dem entsprechenden Hostnamen des XC-API-Servers verwendet werden.

```
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
```



4.2 Hinzufügen einer End Entity

In diesem Beispiel wird eine End Entity mit dem vordefinierten INBOUND_OUTBOUND_TLS-Profil und einem entsprechenden Namen/Kennwort hinzugefügt. Das Eingabefeld CN, Common Name muss mit der IP-Adresse des Applikationsservers (XCAPI/XSSA) übereinstimmen. Für das Certificate Profil muss das Profil ID_CLIENT_SERVER verwendet werden. Als Token muss der Eintrag PEM file selektiert werden.

Benutzername und Kennwort werden auch im nächsten Dialog Enroll For Server Certificate verwendet.

Home / Security / Certificates / Certificate Authority

CA Functions
Basic Functions
Edit Certificate Profiles
Edit Publishers
Edit Certificate Authorities
RA Functions
Edit User Data Sources
Edit End Entity Profiles
Add End Entity
List/Edit End Entities
Supervision Functions
Approve Actions
View Log
System Functions
System Configuration
Edit Services
Public Web

Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username	XSSA-TLS	<input checked="" type="checkbox"/>
Password	<input checked="" type="checkbox"/>
Confirm Password	
Email		<input type="checkbox"/>
Subject DN Fields		
CN, Common Name	192.168.1.61	<input checked="" type="checkbox"/>
CN, Common Name		<input type="checkbox"/>
OU, Organization Unit	SDP	<input type="checkbox"/>
O, Organization	AVAYA	<input type="checkbox"/>
C, Country (ISO 3166)	US	<input type="checkbox"/>
Certificate Profile	ID_CLIENT_SERVER	<input checked="" type="checkbox"/>
CA	tmdefaultca	<input checked="" type="checkbox"/>
Token	PEM file	<input checked="" type="checkbox"/>
<input type="button" value="Add End Entity"/> <input type="button" value="Reset"/>		



Erstellen Sie das XSSA-Server-Zertifikat mit dem entsprechenden Inhalt der generierten CSR-Datei, siehe Kapitel 4.1. CA-Signiertes Zertifikat.

EJBCA

Enroll

- Create Browser Certificate
- Create Server Certificate
- Create Keystore

Retrieve

- Fetch CA & OCSP Certificates
- Fetch CA CRLs
- Fetch User's Latest Certificate

Miscellaneous

- List User's Certificates
- Check Certificate Status
- Administration

Enroll For Server Certificate

Please give your username and password, paste the PEM-formated PKCS10 certification request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded PKCS10 request starting with
 -----BEGIN CERTIFICATE REQUEST-----
 and ending with
 -----END CERTIFICATE REQUEST-----

Enroll

Username

Password

```
-----BEGIN CERTIFICATE REQUEST-----
MIICChCCANOCADAMRURwEwYDVQQDEwxxOTIuMTY4LjEuNjEwggE1MA0GC5qGSIB3
DQEBAQUAA4IBDwAwggEKAoIBAQDF92EuleWu7cmgz7tB/93yrkDvPtSIIuE1Kw8
E7hpSfyPryV4CZ61YK7/g0YbH9K2vwoIwUFCyYPAzvSmkM3dezi1khJC3LlgIt9
TkrKh/R3noARpDjJgSj85epypJYMExy0mSGIwpohY0hIHvuBG409oGw3xb4qxdl1d
6Lfk4CJ35F+j03vZFka+akZkqcyEpCbrfNBLo3YVN/99pRAo0ds/AA3A1JC0Z2qW
9oF1d8MdG4k0RxoPKOEwKRR77NLBwGYHkqyp66+R2c9/Swi tNFqXAUAA3wo8
5o2yAp19eJUjCaHs6MPpaxFmg08Kuorhktcofy0hKoLWwXxe7AgMBAAGgKjAoBgkq
hkiG9w0BCQ4xGzAZMbcGAlUdEQQMA6CDE5M14xNjguMS42MTANBgkqhkiG9w0B
AQUFAAOCAQEAI4d8Cobg3gUuZ5Ykfp8U8f4N/Odfa36JcM38FNGr-hhNTkEpap1F
rg0hQJbzjNk0z02EmOr0B8kfa4Dpon3EgsvGO88BgrxFIyPfe+eW+61CNMv6MsiJe
66Vj1AUI4jAh7Z1RNbjxoLc5I7YeWTFJcyX4BjJA4nvaKVRNOD1i8Ka3KGNMdr
t5k12JVHQ2b1cySzY1Qe5H2pj0WVLIWACKcT4uzk7Ivh51vqh1XvU2DiBiZzArSp
SOUrrgK4JmM6+eQ1PRFaJ2H0wRf59IghZah7bya6p09Yy2bhzZdFpLvUqjY17IRS
I+2OL8mmaDgNP5U2z2ee5gWBd2+04/19fg==
-----END CERTIFICATE REQUEST-----
```

Result type

www.te-systems.de

Telefon 05363 8195-0

freecall 0800 8379783

TE-SYSTEMS
competence in e-communications.



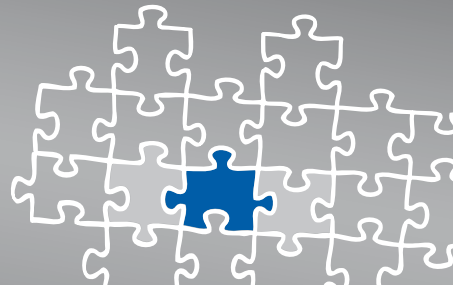
4.3 Vorbereitung des XSSA-CA-Certificate

Speichern Sie lokal das generierte XSSA-Zertifikat und öffnen Sie diese Datei mit einem Text-Editor. Markieren, kopieren und speichern Sie jeweils den private key- und certificate-Teil in separate .pem-Dateien.

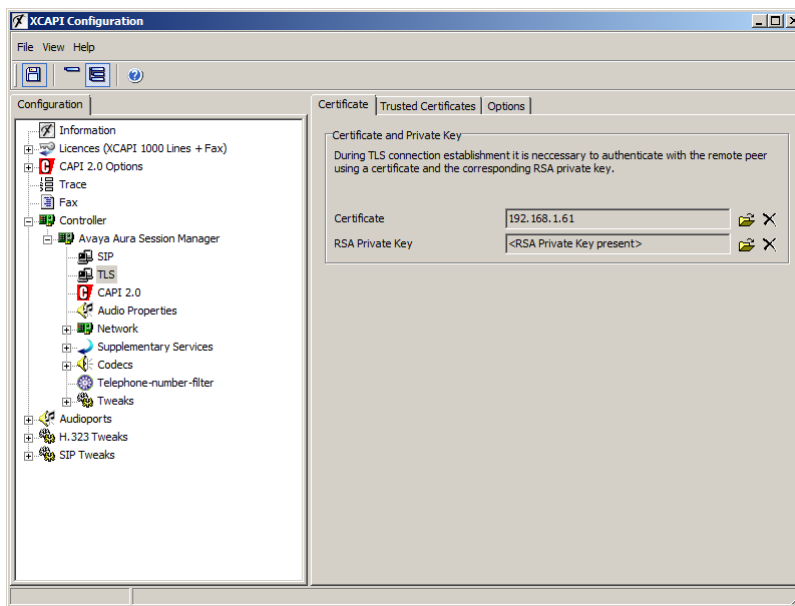
```
Bag Attributes
  friendlyName: 192.168.1.61
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAikGRk2GUU42vwMe
jL4tL7BAI+dA4VoJXTIMQ3kiZ6+GTF4kjV7e07tZvtgNNQTOH7QjocFzFydjh792
AR6EW/ogXi9r/iQtDqzlgRfbbPV3oU8Qpal6IgtvAX1PtoQNVoCBv7YB8TTF8wt
B2tzkgjXRmMrc5Gv7ggMryjyPLq5AgMBAACgYBBaMk/s4M58jurEQ5DMFHH+oH5
G8c6EVUitthus+rvsFH2NsES/LVeCFHRcHTNpaTiTK7b/mY+wry04BLif5zHSqZU
iSoDhWjyAti5H0gCuLJJIJdgqPa0YKM9JEko496xHsmVMPG1IM1IgaVGCku4pNnJ
8qc7oc9cbaXeorlQAQJBANnlU9RAOL/tTNwyT3/ld43Wg/mPlXFwN7HNVNkVRerx
m8Kf4l1qn7soHjRL6fVWA/Y+VhXD8/k8rzkgU0hmVMECQQCg/Gekg+Ze5t7/jfF8
LW2kxiUlaauJ5JUBij7YdTz2hYwUW2+ngiwPFPUseu2HqeEQQRiYx80B4mOzIV
Eav5AKA8tdzJgqtNLnz/zTFBwdo2tu9G1W76EF400Bwv9nFogLDR2WJW21Lh/qeL
wqgR8/7epbeukM5lXzcjGFQUPA8BAkAnUJzL0R6AjLdnB1onLQk1k8JfOag32f8
AiwXks/ee3vTOHQCD4s8/6wEgS6MYn4cj2Xg3As3/2Z3VbuMY0fZ2kEzK7EL6j0
S/vWwKRIU+ADETLuT71Bk949wFuv+qZwU1fpM5enhqfRdnUP4V4mn2f589HdXzu
kjh8P2MNsY2QOQ==
-----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-----
MIICQjCCAAfegAwIBAgIIBH2FQpt1duUwDQYJKoZIhvcNAQEFBQAwMTECAgA1UE
AwwHZGVmYXVsdENMAzGA1UECwwETUdNVDEOMAwGA1UECgwvFQV2BwUEwHhcNMTAx
MFAzMDkzNDIxWhcNMTIxMFAyMDkzNDIxWjBhMR0wGwYDVQDDBRzYXNjaG9udGut
c3lzZG90c3k2TEVMBGMA1UEAwMMTkyLjE2OC4xLjYxMgwwCgYDVQQLDANFRFAOB
DjAMBGNVBAc0MBUFWQV1BMQswCQYDVQGEWJUVUzCBnzANBghkqhkiG9w0BAQEFBQOB
jQAwGyKCyYEAiQyp7YZRTja/Ax6MvI0vEAj50DhwgldMqxDeQjPr42MXiSNKt7T
u1m+2A01BM4ftCOgIXMKJ2Oht3YAroRb+qZeL2v+JC00rOWBE9te9XehTxc1qKoi
h18BfU+2h11WgIG/tgEbxNMVLC0Ha308CNdHEytzka/uCAyvkPI8urkCAWEAAN/
MR0wHQYDVROBBYEFBNU4cR9qCvaGy87CLBo+TABdqmPMAwGA1UdEwEB/wQMAAw
HwYDVR0jBBgwFoAU9781Tnegzn2HFDstTR6+tTVX5ukwDgYDVR0PAQH/BAQDAGP4
MB0GA1UdJQQMwBQGCCGAUQFwMBBgggrBgEFBQcDAjANBgkqhkiG9w0BAQEFBQOB
gQA09zMXhX8jilMpzii8r8EJEg5obO+I8G2ximWcWu4CgDG7f92M9Hgn8L/iOqLo
c7FuKd85eTxVq7yUDQH+UCQkZ2rmpcv2zvIPi+Hr1AA3yepShHce+W7d05FkiTm
qMsB649tXv7WdKV4N9Pza2pIJaE8hafphCSXeTm0RoMxdQ==
-----END CERTIFICATE-----

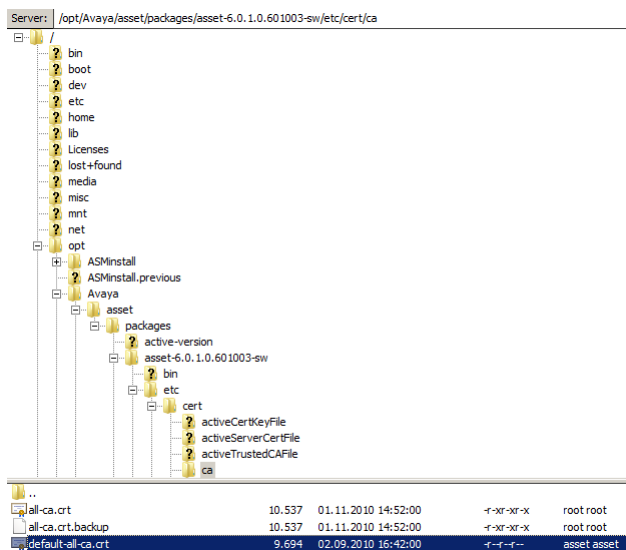
Bag Attributes
  friendlyName: default
subject=/CN=default/OU=MGMT/O=AVAYA
issuer=/CN=default/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIICQjCCAAugAwIBAgIIVNfMFz/WlrYwDQYJKoZIhvcNAQEFBQAwMTECAgA1UE
AwwHZGVmYXVsdENMAzGA1UECwwETUdNVDEOMAwGA1UECgwvFQV2BwUEwHhcNMTAx
MDI1MDgwNzQ2WhcNMTAxMDIyMDgwNzQ2WjAkmRAwDgYDVQDDAdkZWh2dWw0MQ0w
CwYDVQQLDARNR01UMQ4wDAhYDVQQKDAVBVkfZzQTCBnzANBghkqhkiG9w0BAQEFBQOB
jQAwGyKCyYEAuRgFv3HElyWL7M4EaG6NjLGFYGYWY2ph0UByZuUllPiaG1UYsLfn
RwSCeHlqfqb0RtPpMpNOBUiA7riLQw3SeOXCaacutWJbMpsBdq+WRQp7z6xqlQIv
X+2Vb5sM3fWR0GCFcdLqziCpl0g296FiJJzRkpeQdBhORw/FJ8NwkCAWEAANj
MGEWHwYDVR0BBYEFPe/JU53cM59h3w0rUyuvrU1v+bpMA8GA1UdEwEB/wQFMAMB
Af8WwYDVR0jBBgwFoAU9781Tnegzn2HFDstTR6+tTVX5ukwDgYDVR0PAQH/BAQD
AGGMA0GCCSgsIb3DQEBBQUAA4GBAIW980tj81EvztUKU7GeDXkpo91K884/rd0c
KBv/924awMtBiq27609cw158cX/x7wAXmLLyT7OqkxVCRjxh+PneM2/frB8/3Qf
WLJxjAdxLlry6KiHvVkmzjAjcu2bLdtPuanRw2t/eV3XysuE7rdVn+fCm2y516F
PlcUa/BE
-----END CERTIFICATE-----
```



Importieren Sie in der XCAPI-Konfiguration das System Manager CA-signierte Zertifikat und den privaten Schlüssel.

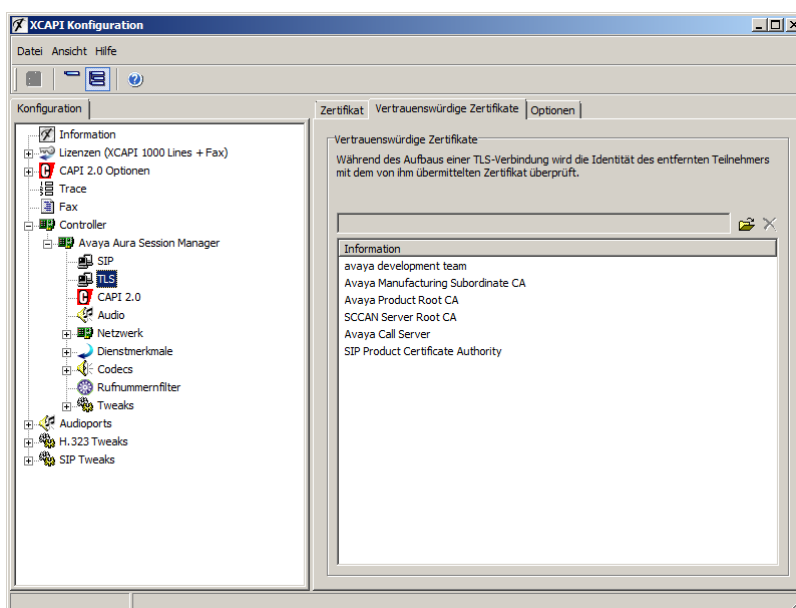


Speichern Sie lokal das benötigte Avaya Aura Session Manager CA-Zertifikat aus dem Verzeichnis /opt/Avaya/asset/packages/active-version/etc/cert/ca.

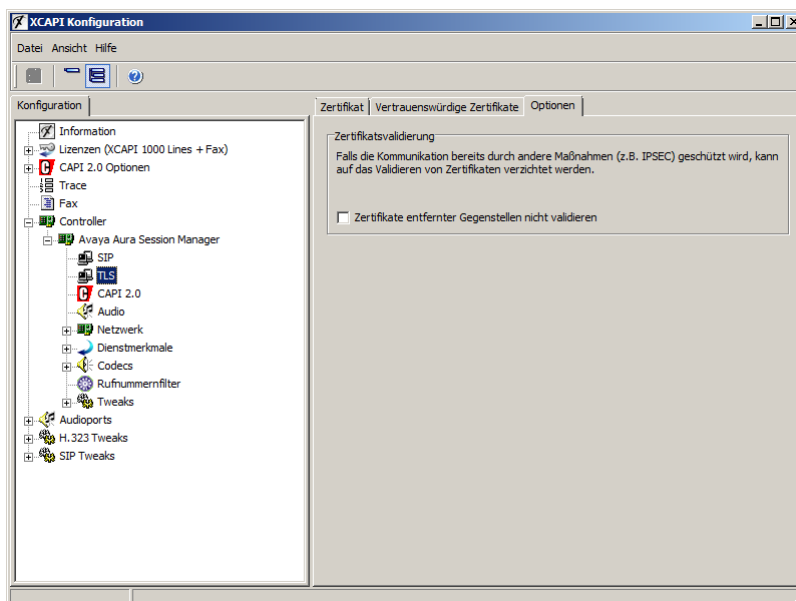


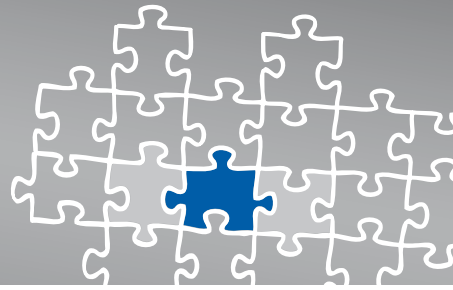


Erstellen Sie ein Backup dieser Datei, benennen sie diese entsprechend um (z.B. session-manager-ca.pem) und ändern sie den Dateityp auf .pem, um diese als vertrauenswürdiges Zertifikat im XCAPI-Controller zu importieren.



Beachten Sie, dass der Parameter Zertifikat der entfernten Gegenstellen nicht validieren NICHT aktiviert ist.

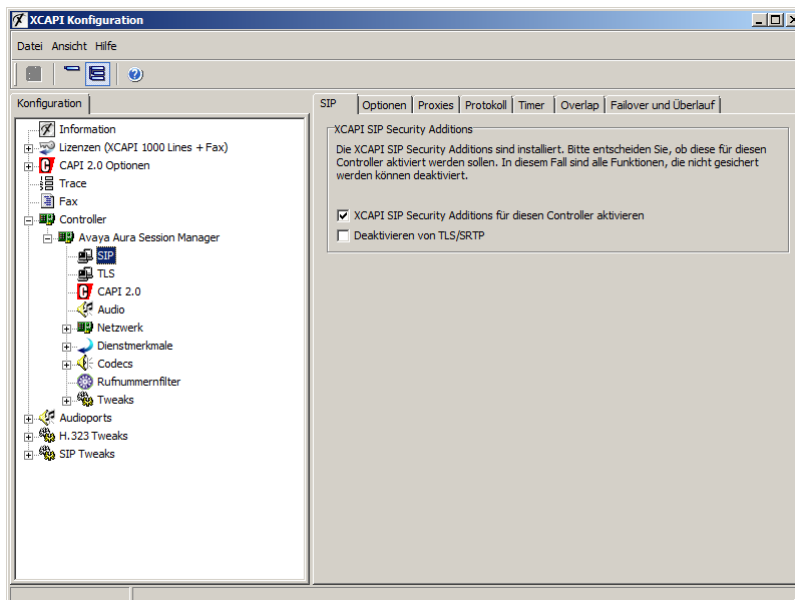




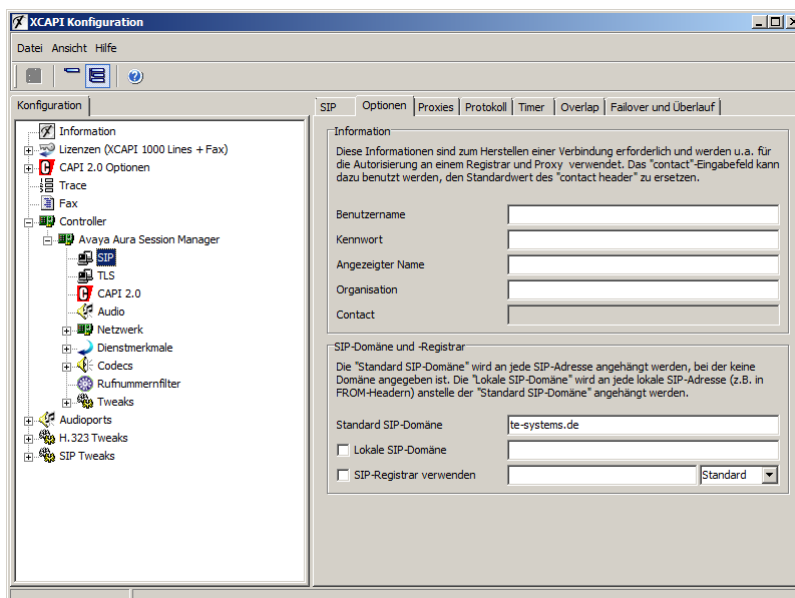
4.4 XCAPI-Controller - TLS/SRTP-Unterstützung

Überprüfen Sie die TLS/SRTP-bezogenen XCAPI-Controller-Einstellungen.

Die XCAPI SIP Security Additions für diesen Controller aktivieren-Einstellung muss für TLS/SRTP-Verbindungen entsprechend aktiviert werden.

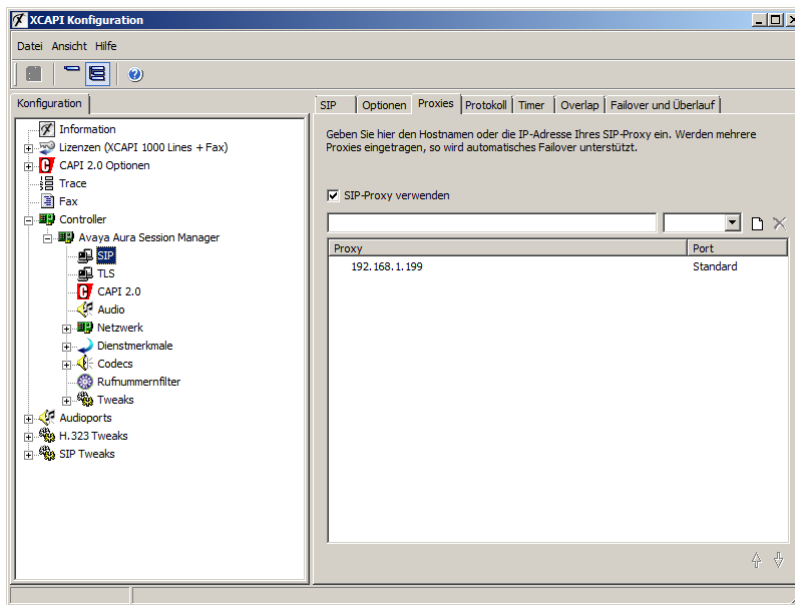


Die Standard SIP Domäne muss entsprechend der VoIP-Umgebung gesetzt werden. In diesem Beispiel wird die Domäne `te-systems.de`, siehe Kapitel Domains ab [Seite 7](#), verwendet.

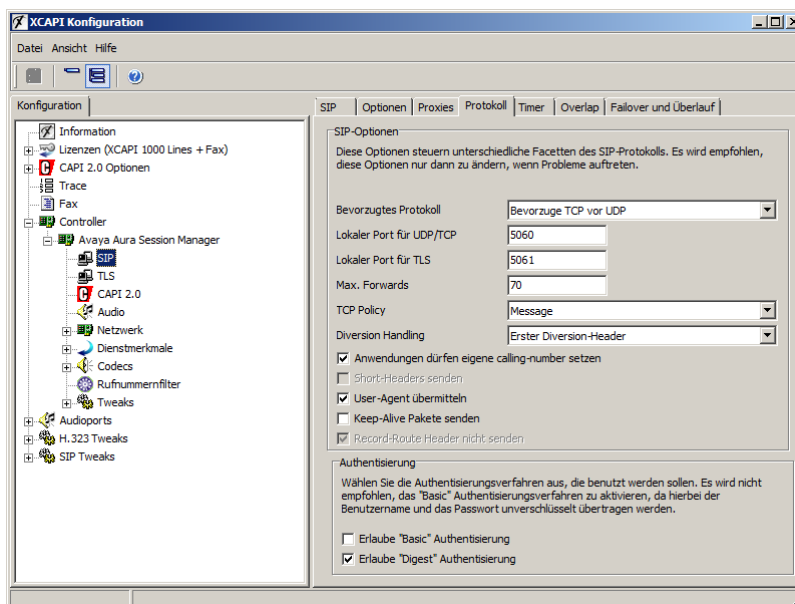




Der SIP-Proxy bezieht sich auf das Avaya Aura Session Manager SM-100-Interface.

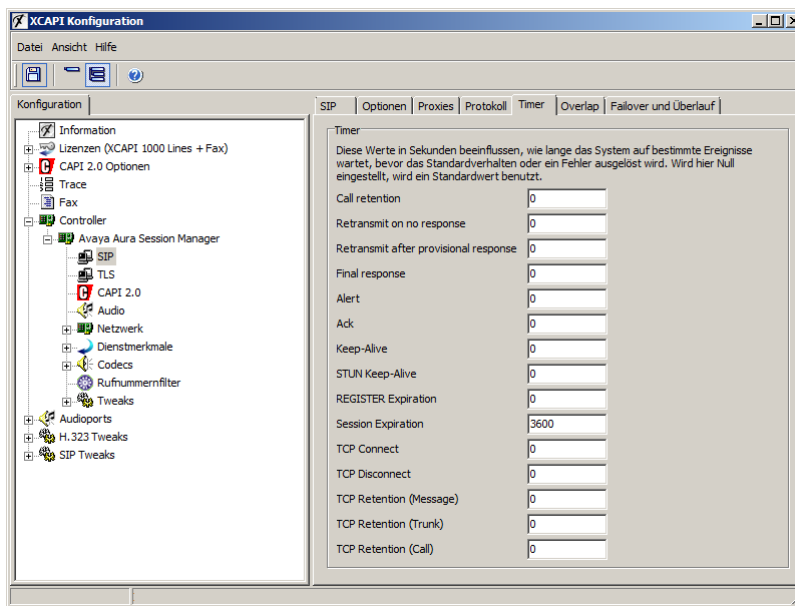


Die Protokoll-Einstellungen sollten mit den Default-Vorgaben verwendet werden.

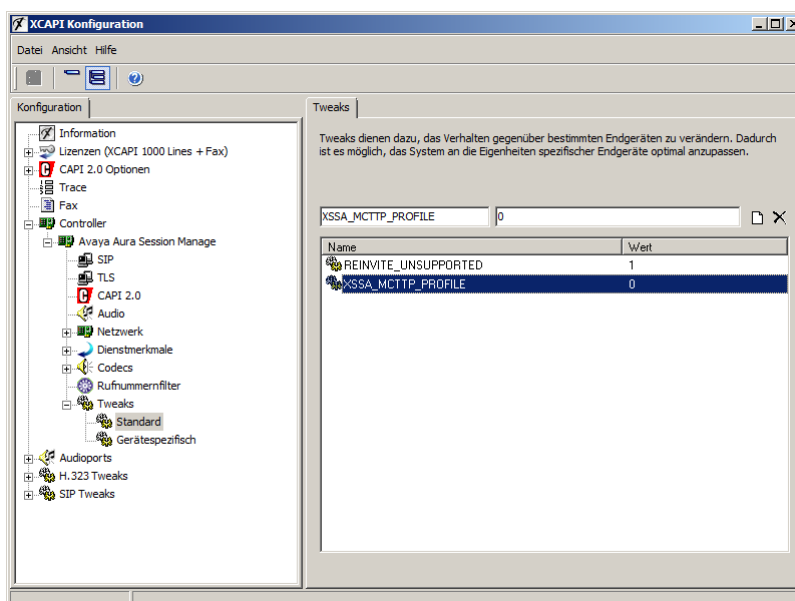


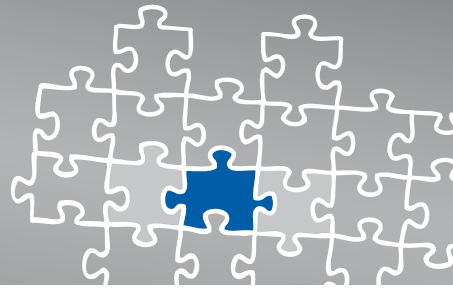


Der Session Expiration-Timer sollte equivalent zu den Einstellungen des Communication Managers sein.



Beachten Sie, dass der XCAPI-Controller-Tweak `XSSA_MCTTP_Profile` mit dem Wert 0 gesetzt ist, um die nötige TLS-/SRTP-Interoperabilität zwischen dem XSSA und dem Avaya Aura Session Manager herzustellen.





Secure Real-Time Transport Protocol

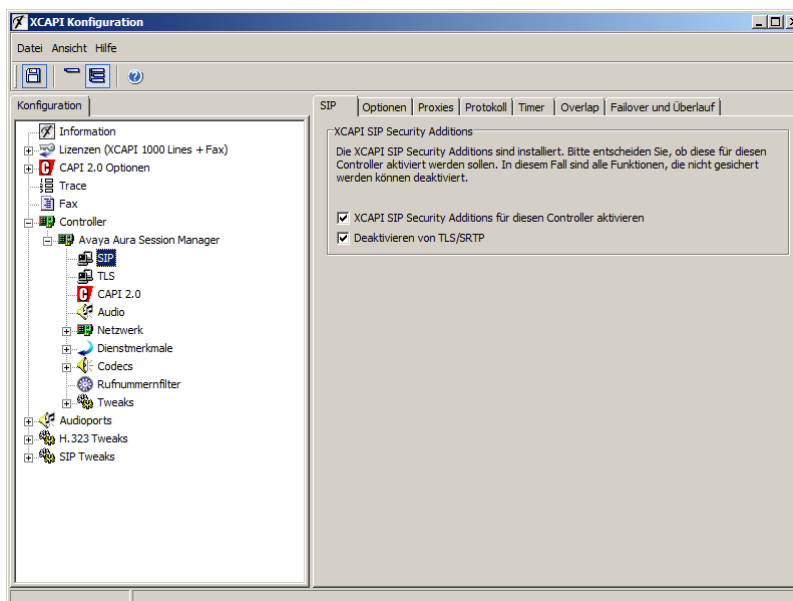
Beachten Sie, dass für SRTP-Verbindungen unter Verwendung des XSSA-Proxy mit aktiviertem TLS, die SIP-Entities, SIP-Clients und Media-Gateways die korrekten Media Encryption-Einstellungen verwenden. Neben den IP-Codec-Sets des Communication Managers, muss auch die equivalente Media Encryption für die SIP-Clients in der 46xxsettings.txt-Konfigurationsdatei verwendet werden.



Für XSSA/TLS/SRTP Interoperabilität muss als Media Encryption die Einstellung `1-srtp-aescm128-hmac80` verwendet werden. Für Standard-SIP-Trunking via TCP müssen alle Media Encryptions mit der Einstellung `none` verwendet werden.

SIP-Trunking ohne TLS/SRTP

Für Standard-SIP-Trunking via TCP-Protokoll zwischen dem Communication Manager, dem Session Manager und der XCAPI/XSSA müssen die Protokoll-Einstellungen der SIP-Entities, SIP-Clients und, bei Bedarf, der Signalling Group des Communication Managers mit der SIP/TCP-Transport-Methode und dem Default-Port 5060 verwendet werden. Sämtliche Media Encryption-bezogenen Einstellungen müssen innerhalb der IP-Codec-Sets und für die SIP-Clients deaktiviert werden. Beachten Sie, dass für den XCAPI-SIP-Controller der Parameter Deaktivieren von TLS/SRTP gesetzt ist.





Fax-Dienste

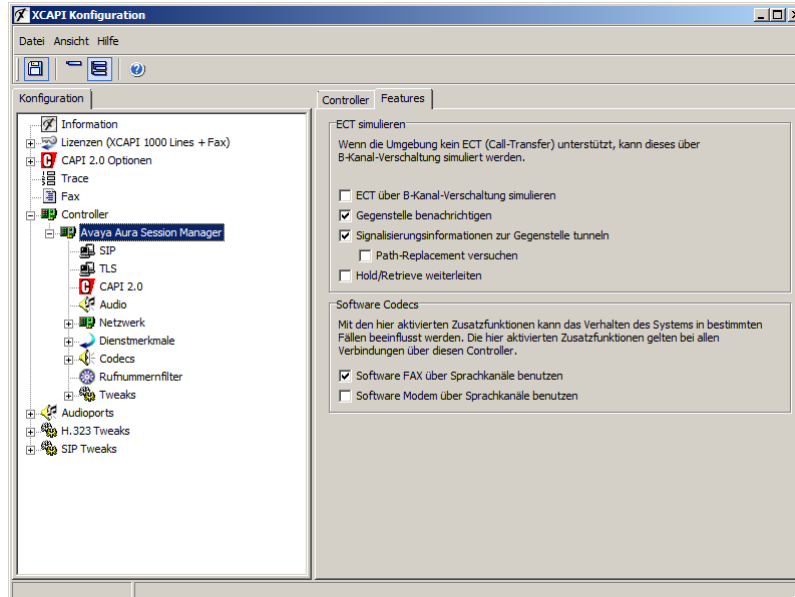
In den folgenden Abschnitten erläutern wir die Vorgehensweise für eine Konfiguration der Fax-Dienste T.38 und Software-Fax.

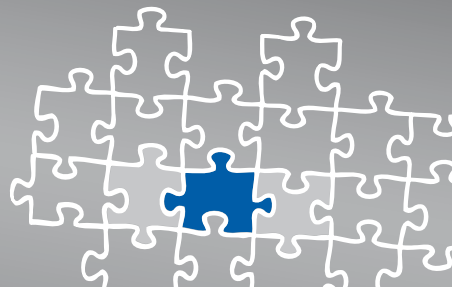
7.1 Software-Fax

In diesem Modus verhält sich die XCAPI durch die Übertragung von modulierten Faxsignalen wie ein herkömmliches analoges Faxgerät.

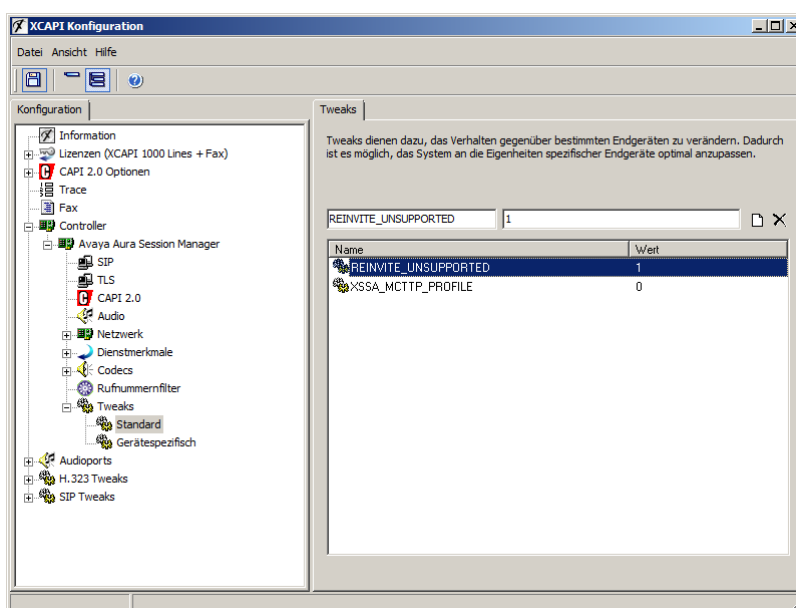
Öffnen Sie das XCAPI-Konfigurationstool, um den Software-Fax-Modus zu aktivieren. Wechseln Sie die Ansicht in den Expertenmodus mit der Funktionstaste F8, oder wählen Sie über das Auswahlménü Ansicht die Option Expertenmodus. Selektieren Sie in der Konfigurationsliste unter dem **Controller**-Dialog den entsprechenden **SIP-Controller** aus.

Wechseln Sie in die Ansicht des Feature-Reiters und aktivieren dort die Option Software FAX über Sprachkanäle benutzen.

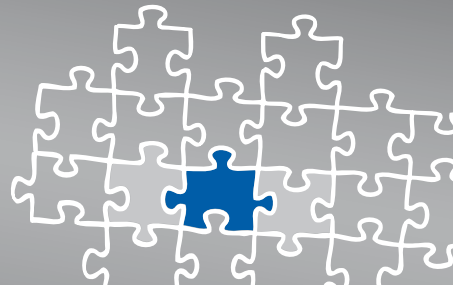




Beachten Sie, dass unter den XCAPI-Controller-Tweaks der Eintrag `REINVITE_UNSUPPORTED` mit dem Wert 1 aus Interoperabilitätsgründen aktiviert sein muss. Dieser Tweak unterdrückt sämtliche `RE-Invites`, auch solche die sich auf den Session Timer beziehen, einer bestehenden Verbindung.

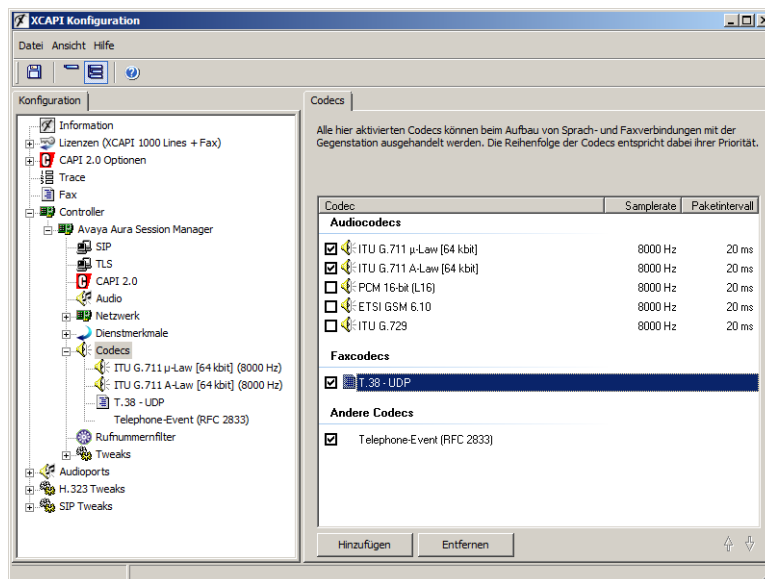


Bei einer TLS/SRTP-Anbindung muss zwingend die Software-Fax-Methode verwendet werden. Beachten Sie, dass alle T.38-bezogenen Einstellungen der relevanten IP-Codec-Sets deaktiviert sind.



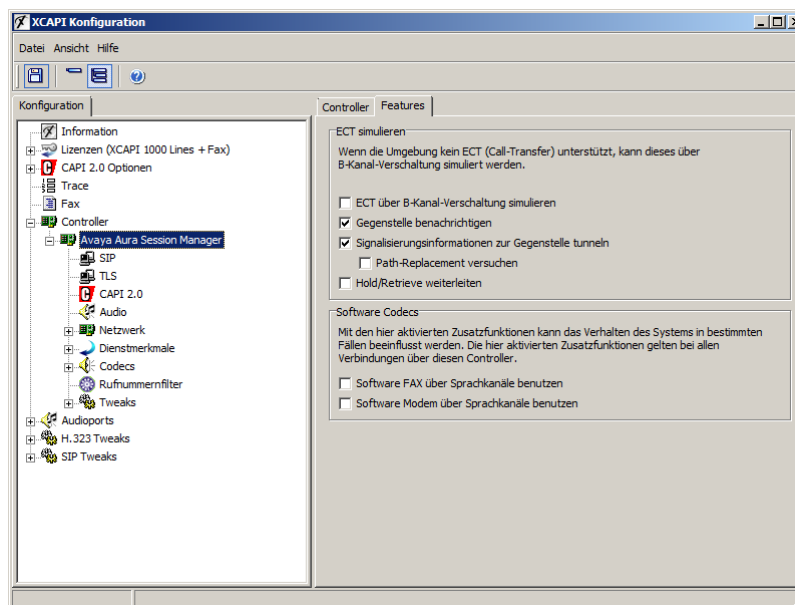
7.2 T.38-Fax

Beachten Sie, dass T.38 seitens der einbezogenen Media-Gateways und im XCAPI-Controller der T.38 - UDP-Codec verfügbar und eingerichtet sind.





Die Option Software Fax über Sprachkanäle benutzen, siehe Features-Einstellungen des XCAPI-Controllers, muss deaktiviert werden.



Beachten Sie, dass T.38 nicht in TLS/SRTP-Umgebungen verfügbar ist.



Haftungsausschluss

Copyright © 2010 TE-SYSTEMS GmbH

Alle Rechte vorbehalten

Kein Teil dieses Dokuments oder das Dokument als Ganzes dürfen ohne vorherige schriftliche Genehmigung von TE-SYSTEMS GmbH in irgendeiner Form reproduziert werden.

Die in diesem Dokument gemachten Angaben entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Die TE-SYSTEMS GmbH behält sich das Recht vor, Veränderungen ohne vorherige Ankündigung vorzunehmen.

Bei der Zusammenstellung von Texten und Abbildungen sowie bei der Erstellung der Software wurde mit größter Sorgfalt vorgegangen. Dennoch kann für die Richtigkeit, Aktualität und Vollständigkeit des Inhalts, eine Wirtschaftlichkeit oder die fehlerfreie Funktion von Software für einen bestimmten Zweck keinerlei Gewähr übernommen werden. Die TE-SYSTEMS GmbH schließt daher jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokuments entstehen.

Marken

Alle verwendeten Namen von Produkten und Dienstleistungen sind Marken oder eingetragene Marken (auch ohne gesonderte Kennzeichnung) der jeweiligen privaten oder juristischen Personen und unterliegen als solche den gesetzlichen Bestimmungen.

Drittrechte

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 (ey@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.

TE-SYSTEMS GmbH

Geschäftsführer Andreas Geiger
Oliver Körber

Anschrift Max-von-Laue-Weg 19
38448 Wolfsburg

Telefon 05363 8195-0
Fax 05363 8195-999
freecall 0800 8379783

E-Mail info@te-systems.de
Internet www.te-systems.de
www.xcapi.de