

Administration, upgrades and maintenances

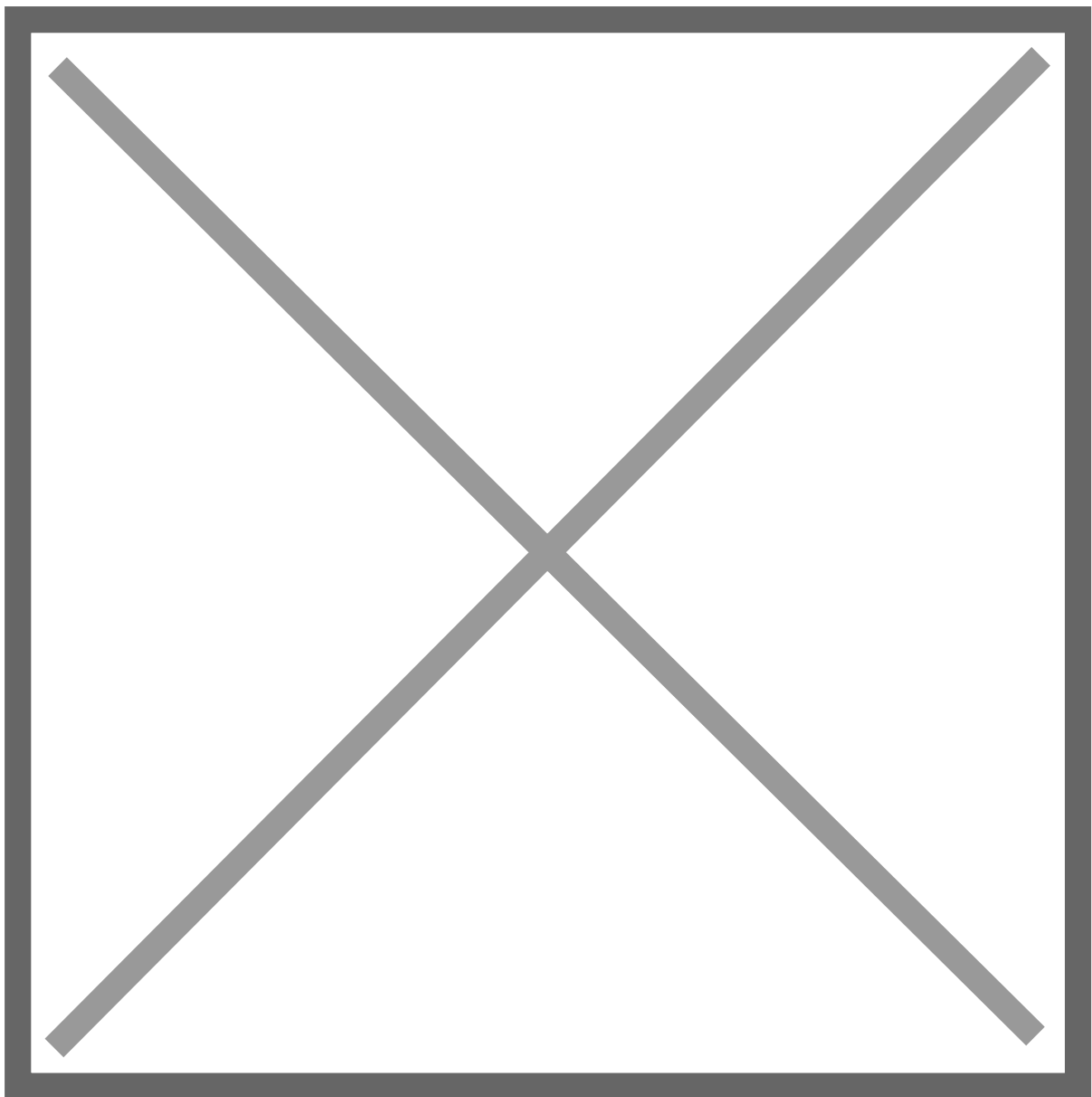
Everything related to Avaya AES Installations, upgrades and implementations

- [AES - Testing SMS Service](#)
- [AES - Update Process](#)
- [AES - TSAPI CTI link integration](#)
- [AES - Upgrade 8.0.1 to 8.1.3](#)
- [AES - Renew AES Cert using System Manager](#)

AES – Testing SMS Service

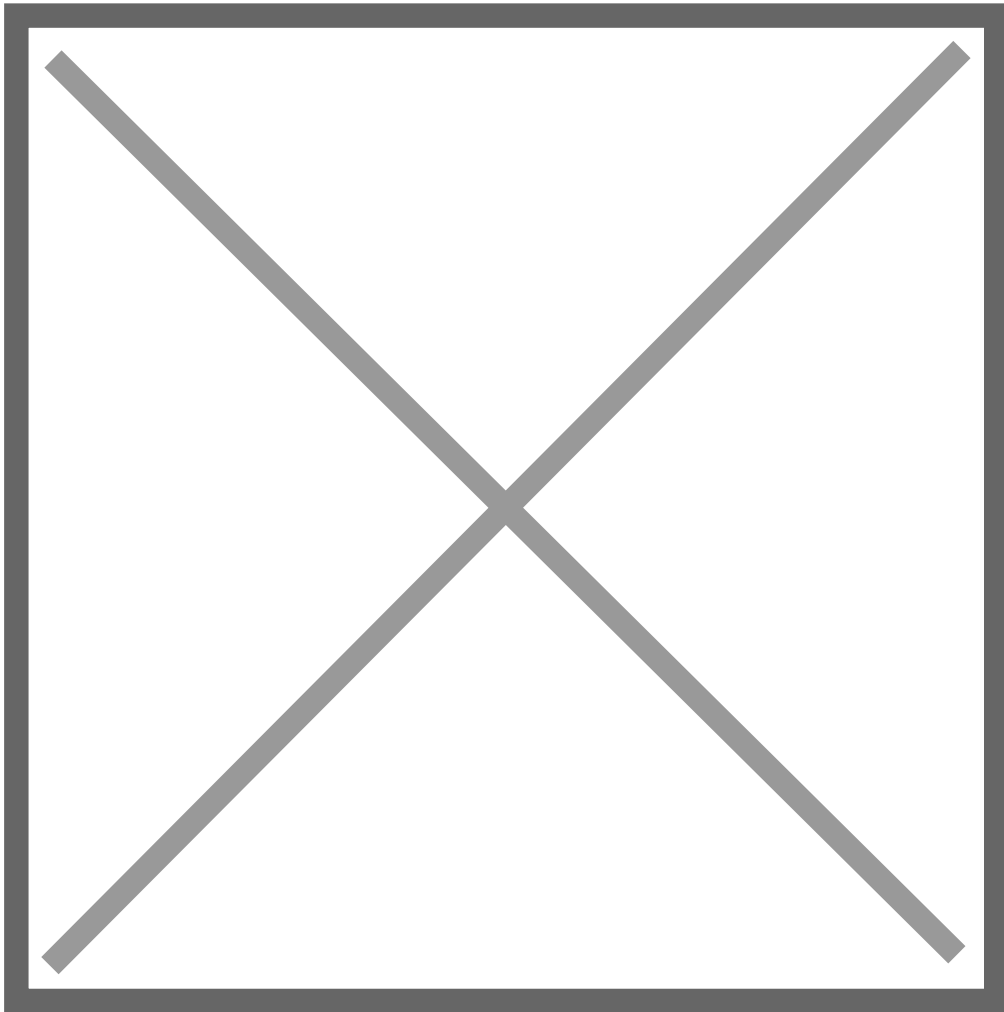
System Management Service (SMS) is an interesting service that all Application Enablement Servers run by default with no need for licensing, it exposes management features of Communication Manager. This service enables its clients to display, list, add, change and remove specific managed objects on Communication Manager.

This is a diagram representing the 3rd party software accessing the SMS web service multiple elements can be accessed via SMS but in this case we will focus in stations (ip softphones):



Basic administration needs to be set up in the AES (Communication Manager Interface -> Switch Connections) but this will not be covered in this entry.

To have SMS working properly Communication Manager IP address needs to be set up in AES SMS service (AE Services -> SMS):



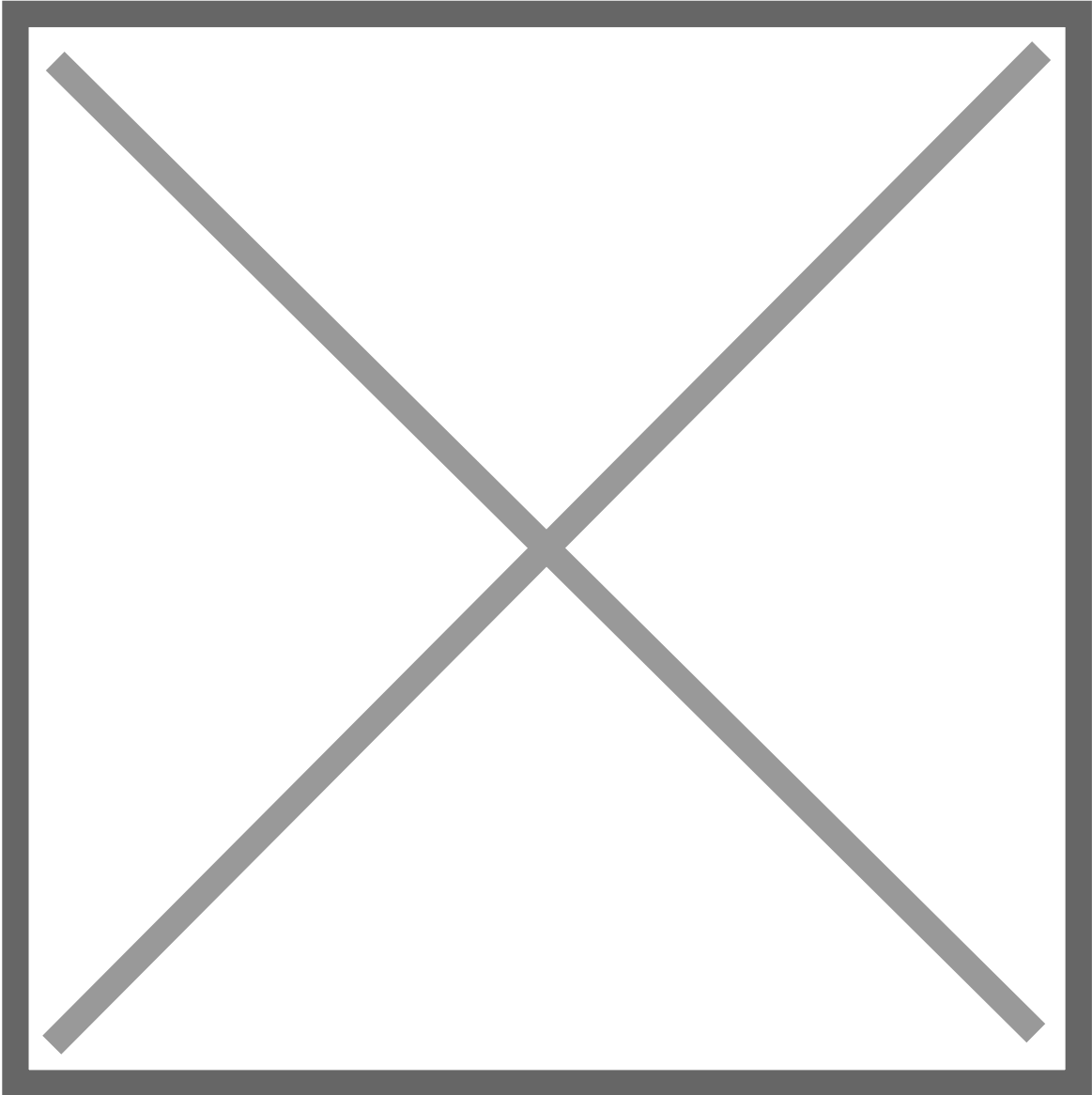
Normally, a specific user is created in Avaya Communication Manager for audit purposes, in my case SMSSrvc was created with profile 18.

Now its time to test the SMS service, here are some steps you can follow to busyout/release an specific station (SMS Service test web page provide information & documentation for WSDL and more):

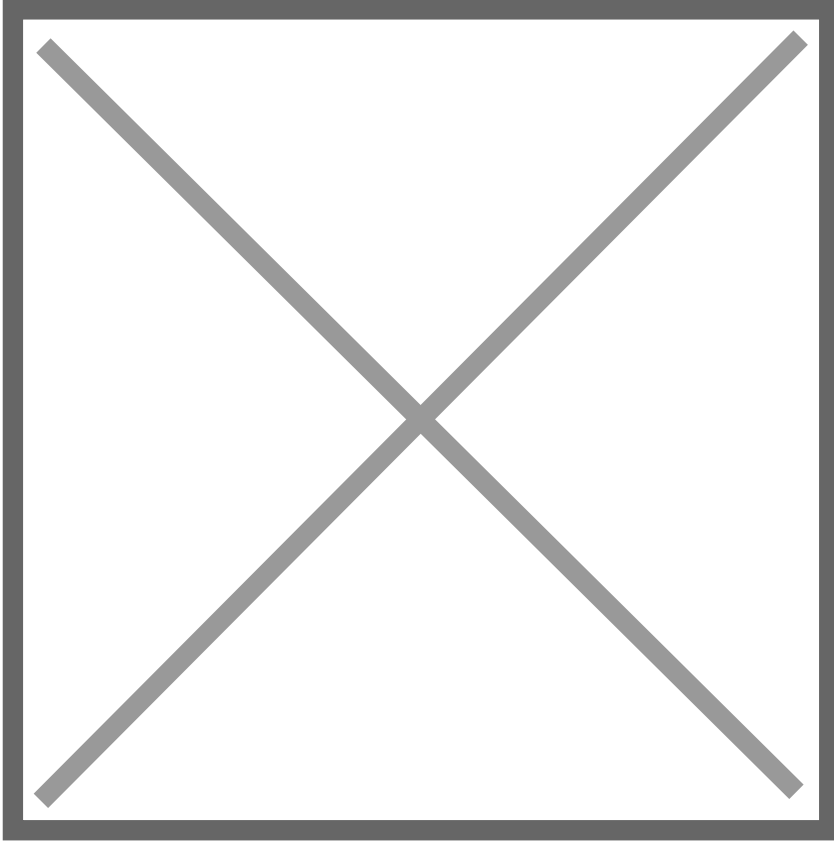
- 1) Access AES SMS web page using https://AES_IP/sms/sms_test.php
- 2) Fill out information to busyout:
 - a. CM Login ID/Password
 - b. Set Model to "Station"
 - c. Operation should be set to "busyout"
 - d. Set Qualifier to the extension number to be reset
- 3) Press "Submit Request" Button
- 4) Repeat step 2) but setting Operation to "release"
- 5) Press "Submit Request" Button

6) Press "Release" Button to disconnect session

Here is a screenshot for running the process described above:

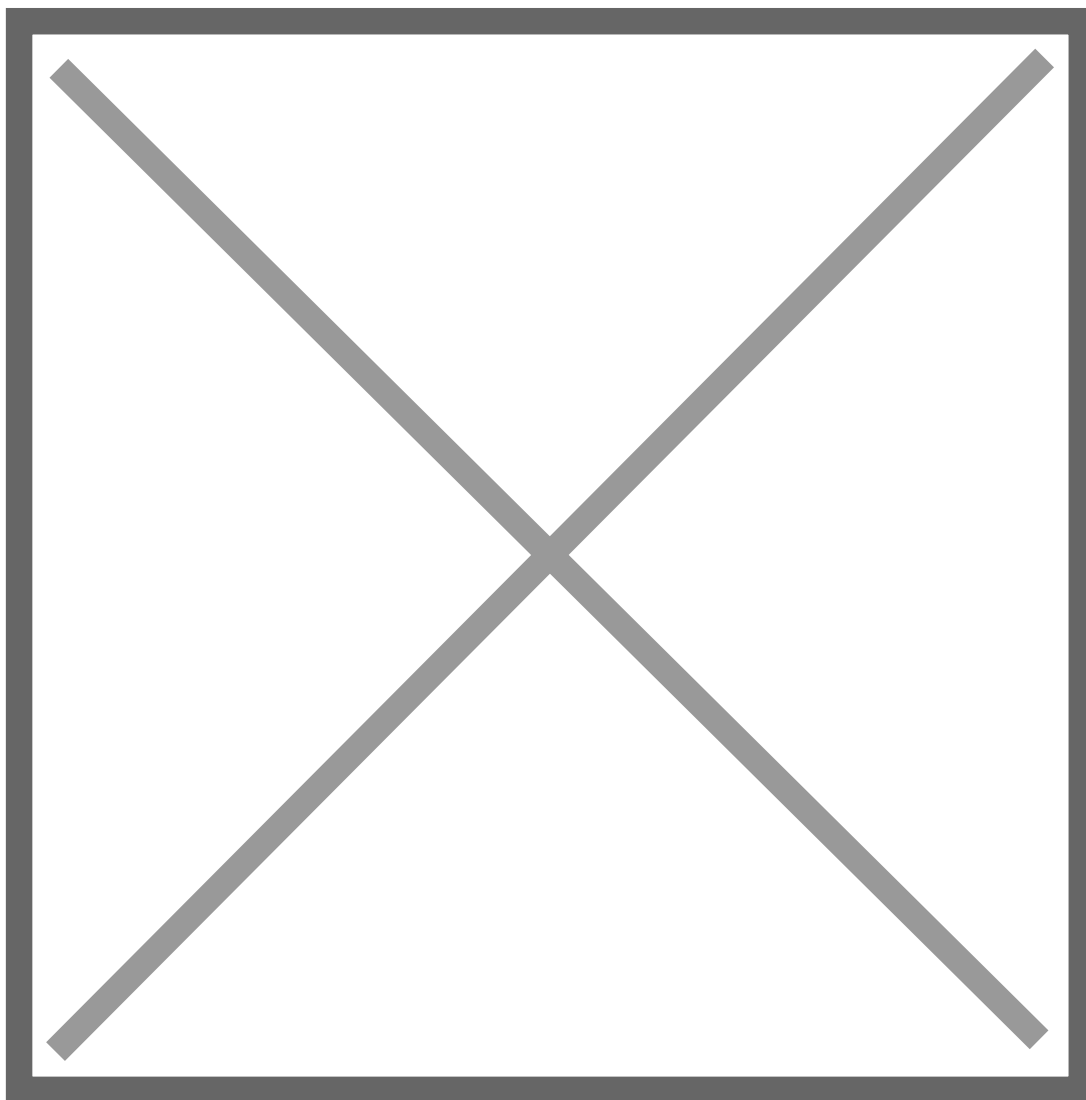


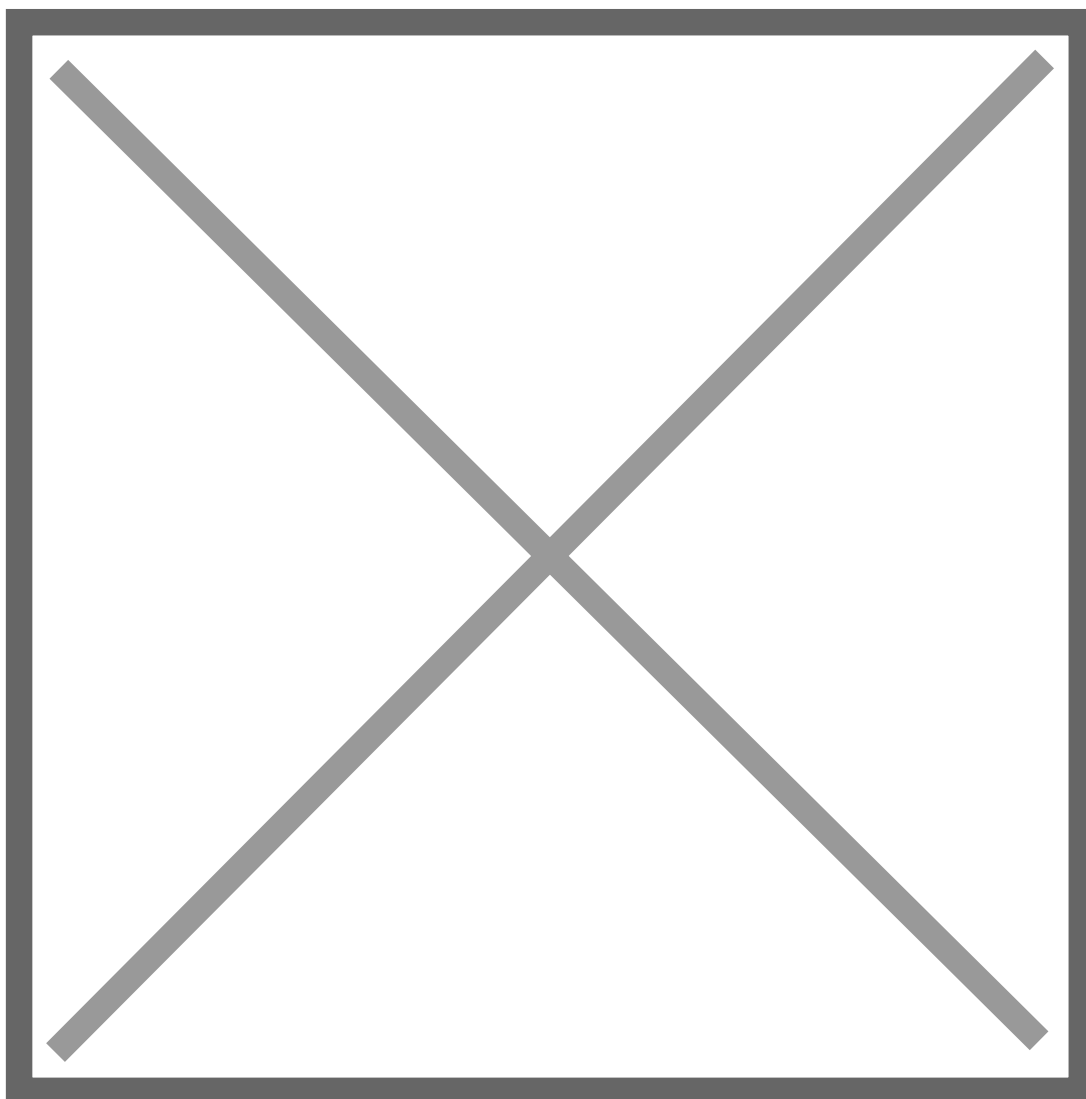
PBX commands after using the web page

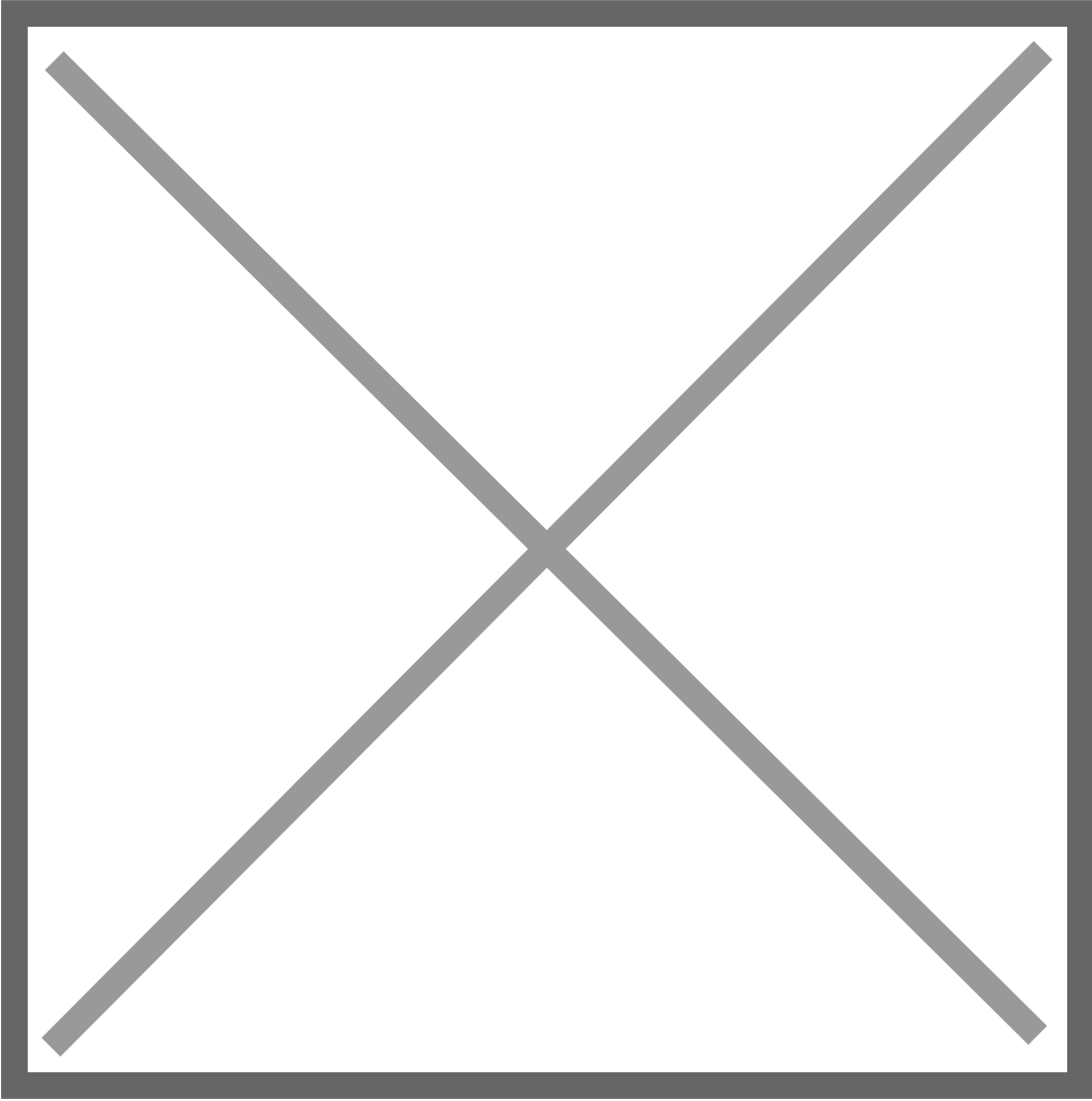


For more information visit Avaya devconnect program:

https://www.devconnectprogram.com/site/global/home/p_home.gsp







Source: <https://whereismyvoicepacket.com/aes-sms/>

AES - Update Process

In this entry we will document the process to apply updates in an Application Enablement Server, this what we will be applying:

812Plus_LSUPatch14.bin <- Linux Security Update Patch

aesvcs-8.1.3.4.0.2-servicepack.bin <- AES Service Pack 8.1.3.4

Here is the procedure

- Upload files to /tmp (you can use WinSCP)
- SSH the AES and move current directory to /tmp (**cd /tmp**)
- Verify the current version (**swversion**)

```
[root@denusvm-labaes1 cust]# swversion
*****
Application Enablement Services
*****
Version: 8.1.3.1.0.7-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
RTS Version:AES-8.1.3.1.0.7-0

*****
Operating System Version: Linux 3.10.0-1160.11.1.el7.x86_64

***** Patch Numbers Installed in this system are *****
LSU-8.1.2Plus-4
FP8.1.3.0.0.25 (AES 8.1.3)
FP8.1.3.1.0.7 (AES 8.1.3)
*****
```

- Change permissions on the files uploaded

```
chmod 750 812Plus_LSUPatch14.bin
chmod 750 aesvcs-8.1.3.4.0.2-servicepack.bin
```

- Execute the Linux update first (accept all terms), when done AES will restart (reconnect)

```
[root@denusvm-labaes1 tmp]# ./812Plus_LSUPatch14.bin
```

- Now lets apply AES SP 8.1.3.4 (accept all terms), when done AES will restart (reconnect)

```
[root@denusvm-labaes1 cust]# ./aesvcs-8.1.3.4.0.2-servicepack.bin
```

- Verify the new version after patches installed (**swversion**)

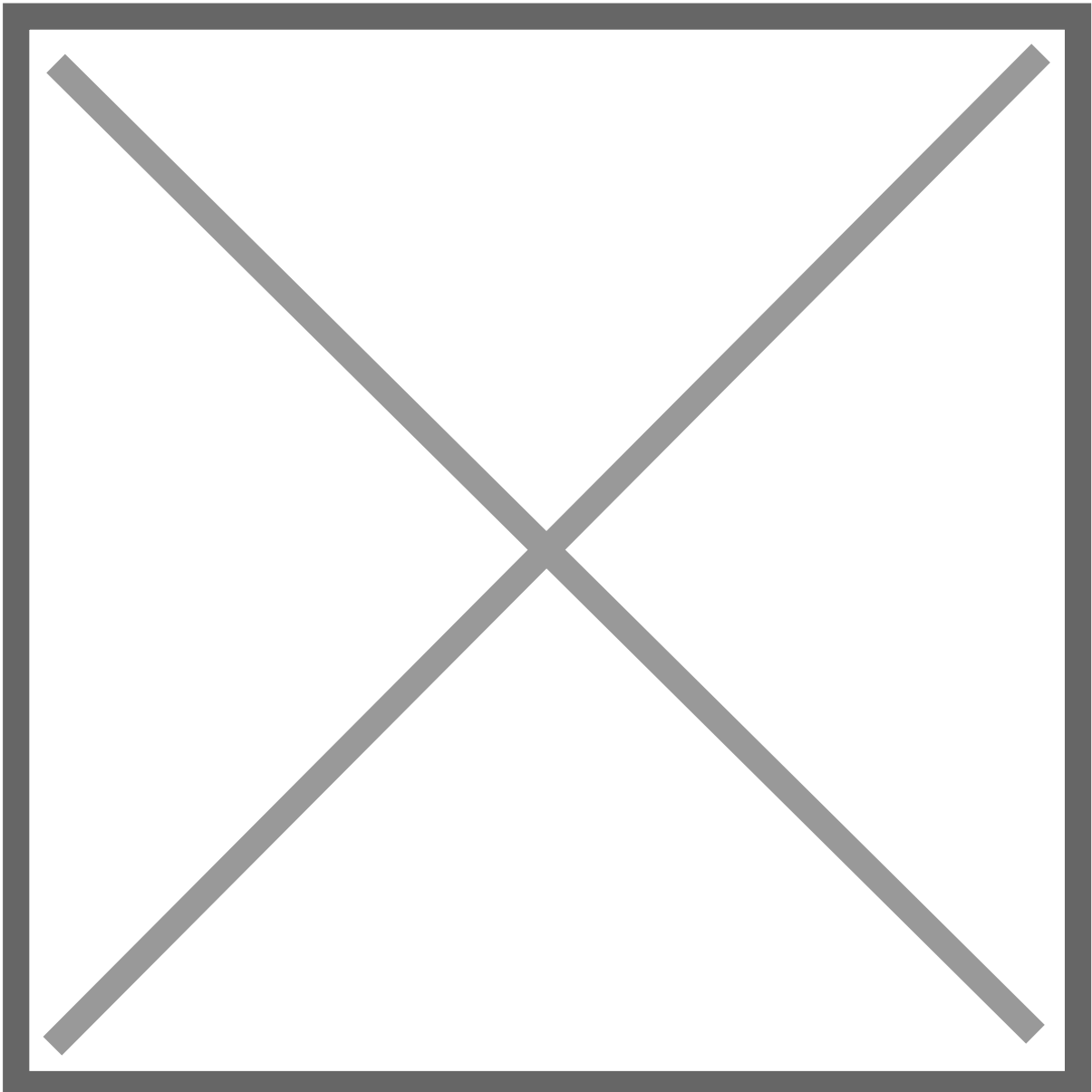
```
[root@denusvm-labaes1 tmp]# swversion
*****
Application Enablement Services
*****
Version: 8.1.3.4.0.2-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
RTS Version:AES-8.1.3.4.0.2-0

*****
Operating System Version: Linux 3.10.0-1160.53.1.el7.x86_64
***** Patch Numbers Installed in this system are *****
LSU-8.1.2Plus-4
FP8.1.3.0.0.25 (AES 8.1.3)
FP8.1.3.1.0.7 (AES 8.1.3)
LSU-8.1.2Plus-14
FP8.1.3.4.0.2 (AES 8.1.3)
```

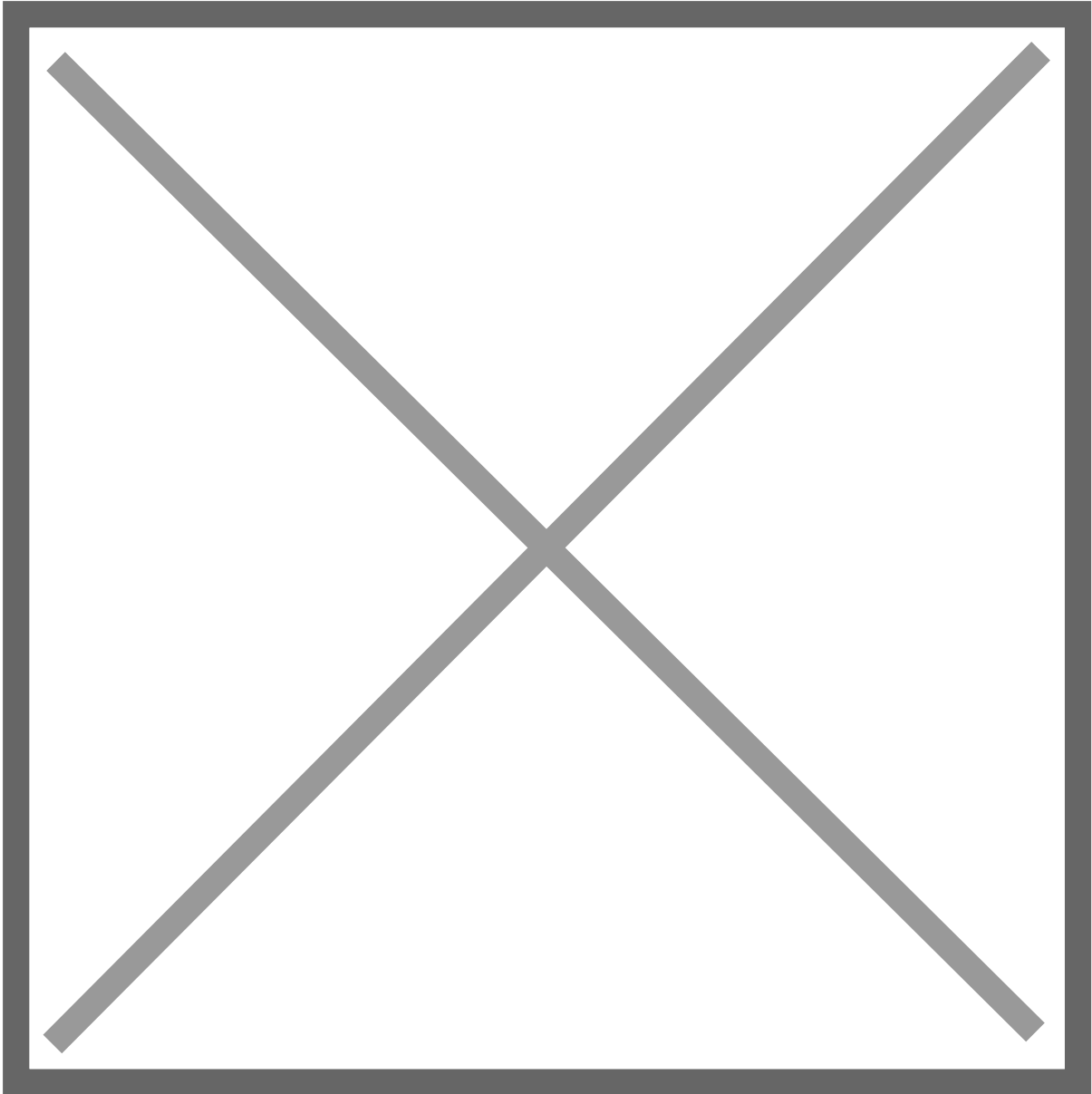
AES - TSAPI CTI link integration

In this entry let's work in integrating an Application Enablement Server to a Communication Manager and create TSAPI CTI link that we will be testing in the next entry. We will assume that the CM and AES servers are already deployed, connectivity is in place and the administrator have the credentials/permissions to perform changes/additions.

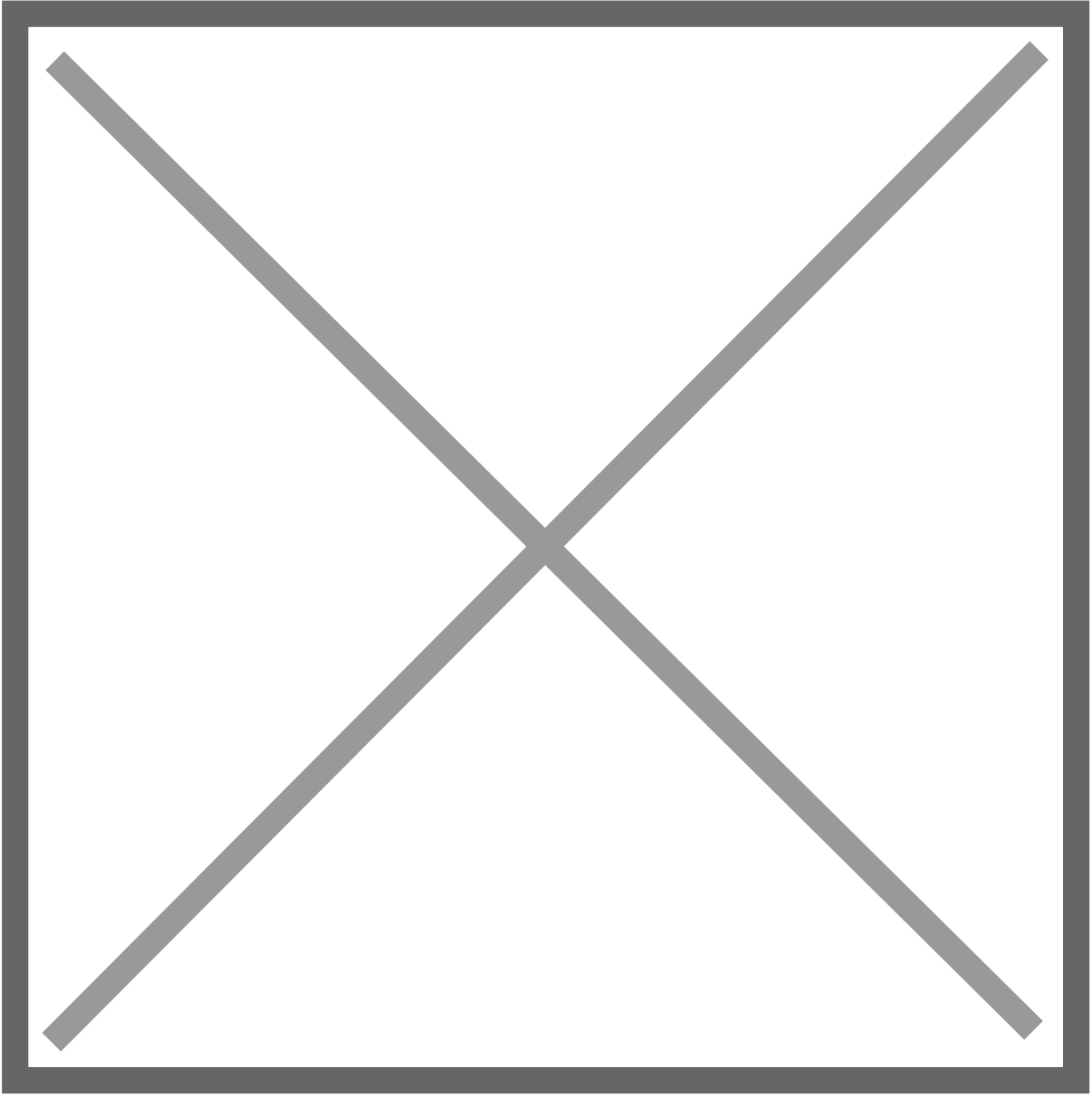
Let's begin with ***change ip-services*** Set up in the first page enabling AESVCS running on port 8765 on Communication Manager:

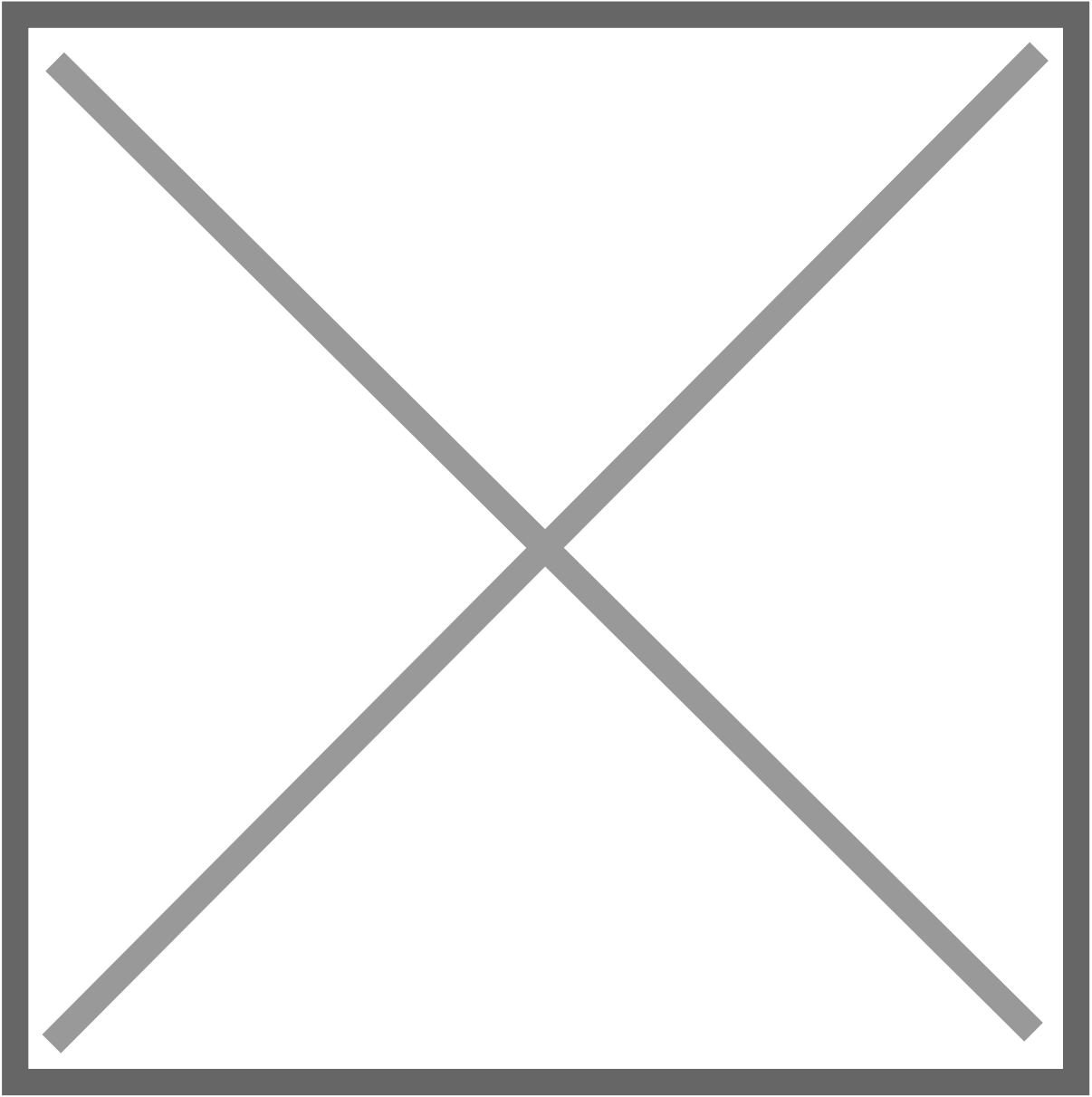


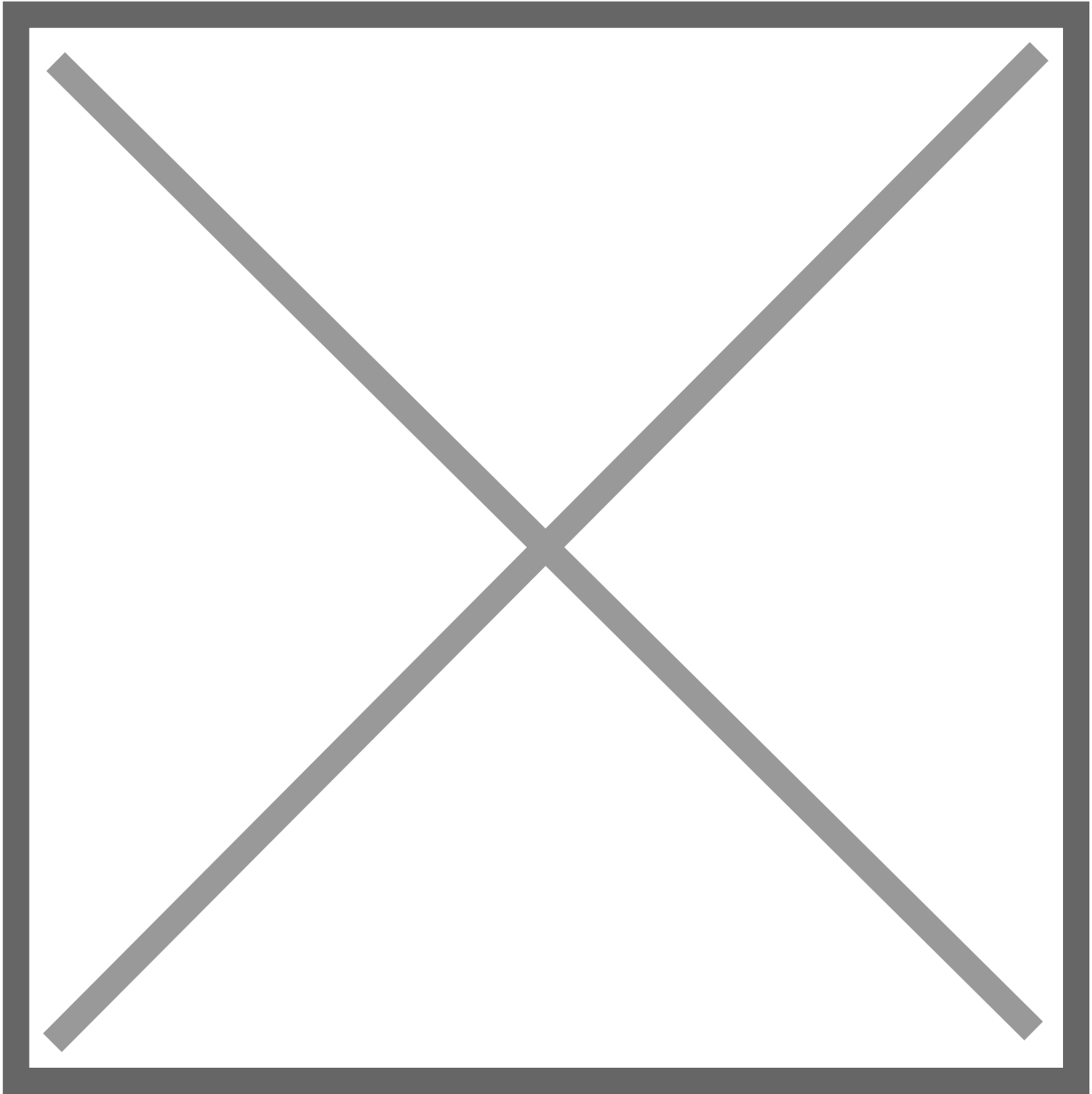
On the third page set up the hostname of the AE Server and password:



Second step is adding the CTI link with ***add cti 1:***

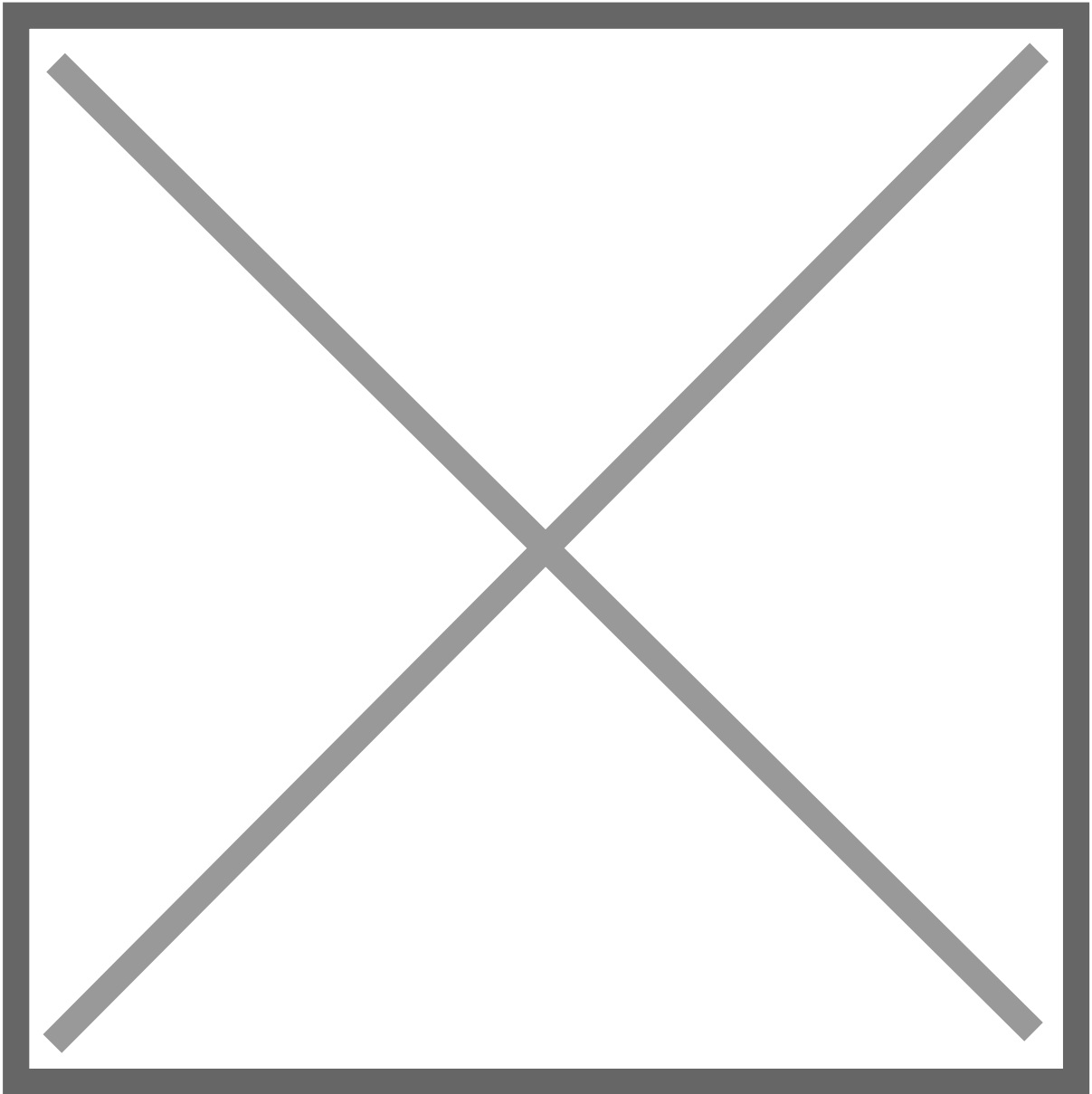




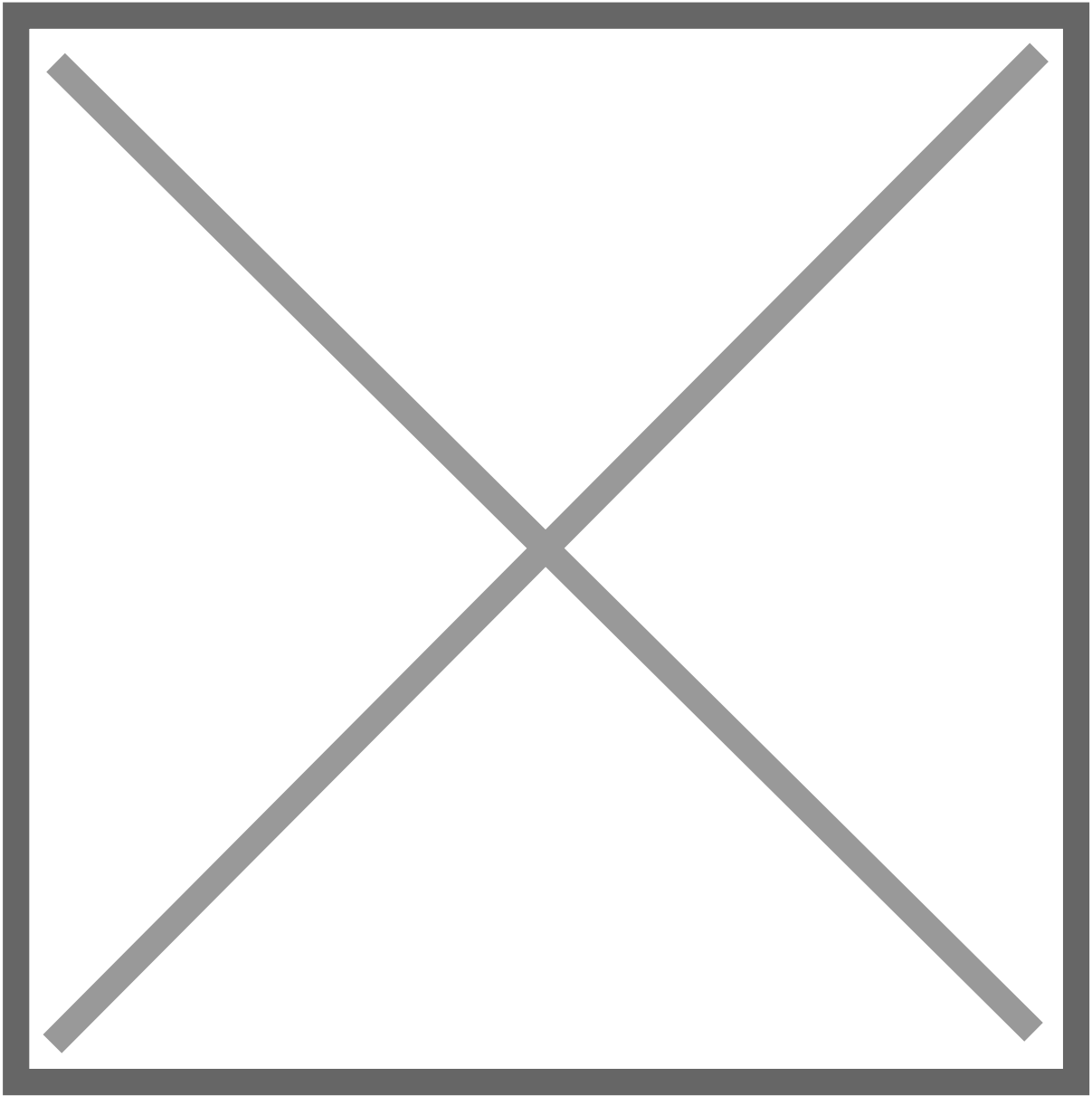


Now it's time to make the changes in the AE Server:

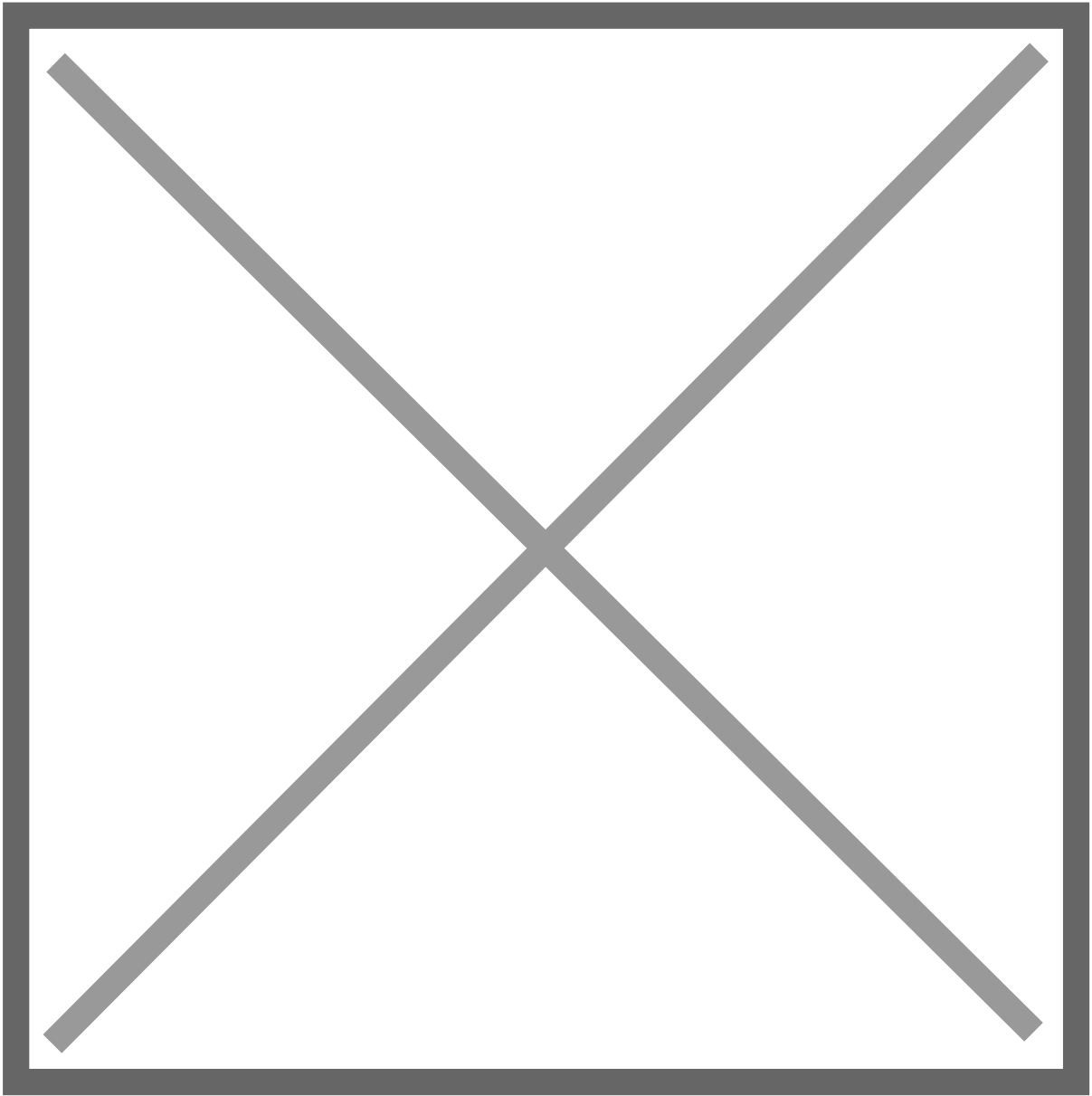
First, log in into the AES using the web portal and navigate to **Communication Manager Interface -> Switch Connections -> Add Connection:**



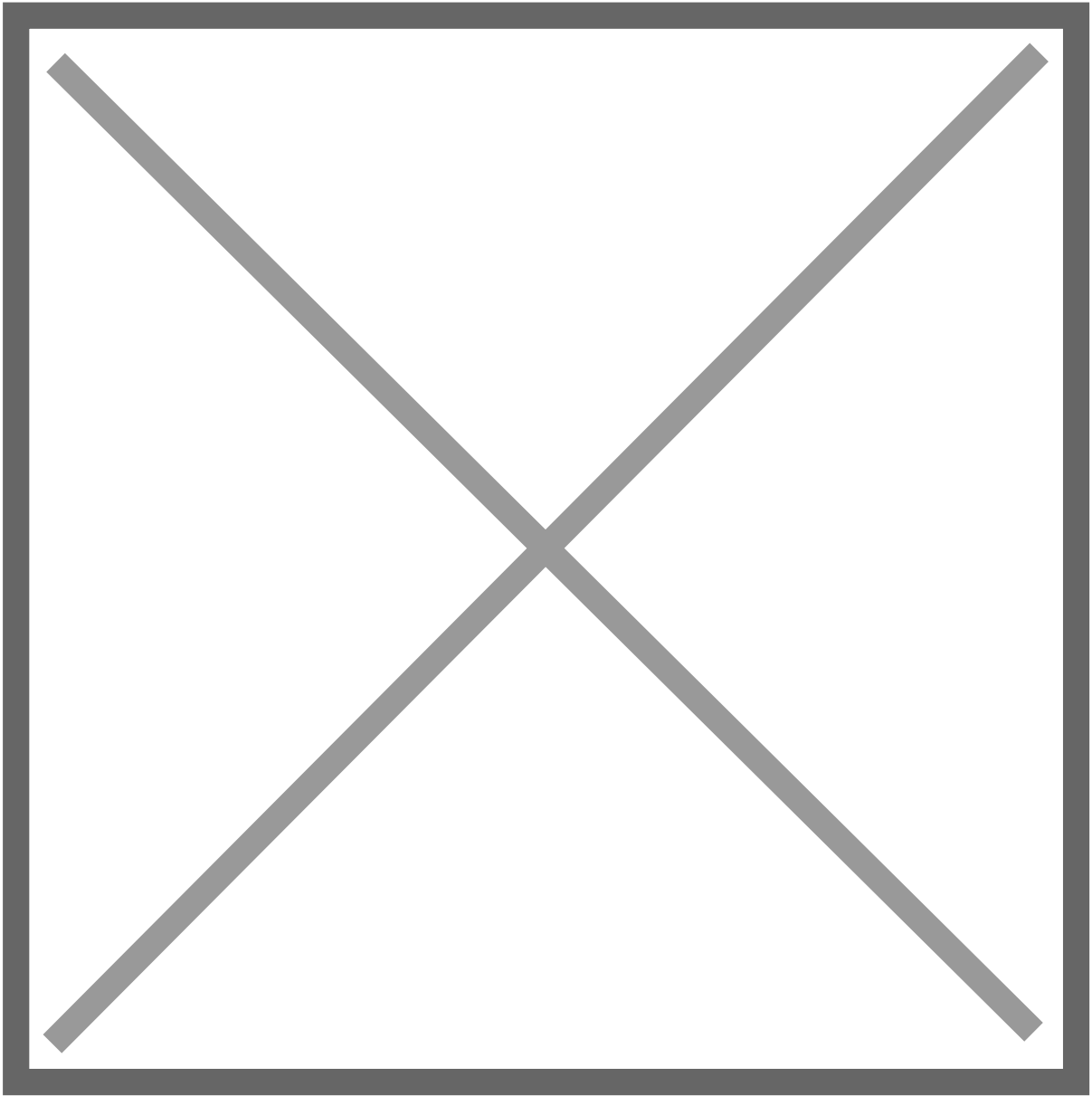
In the next screen type the same password set in the ***change ip-services*** command in the PBX, enable only the *Processor Ethernet* option, leave all other settings by default blank, but make sure the TLS is disabled.



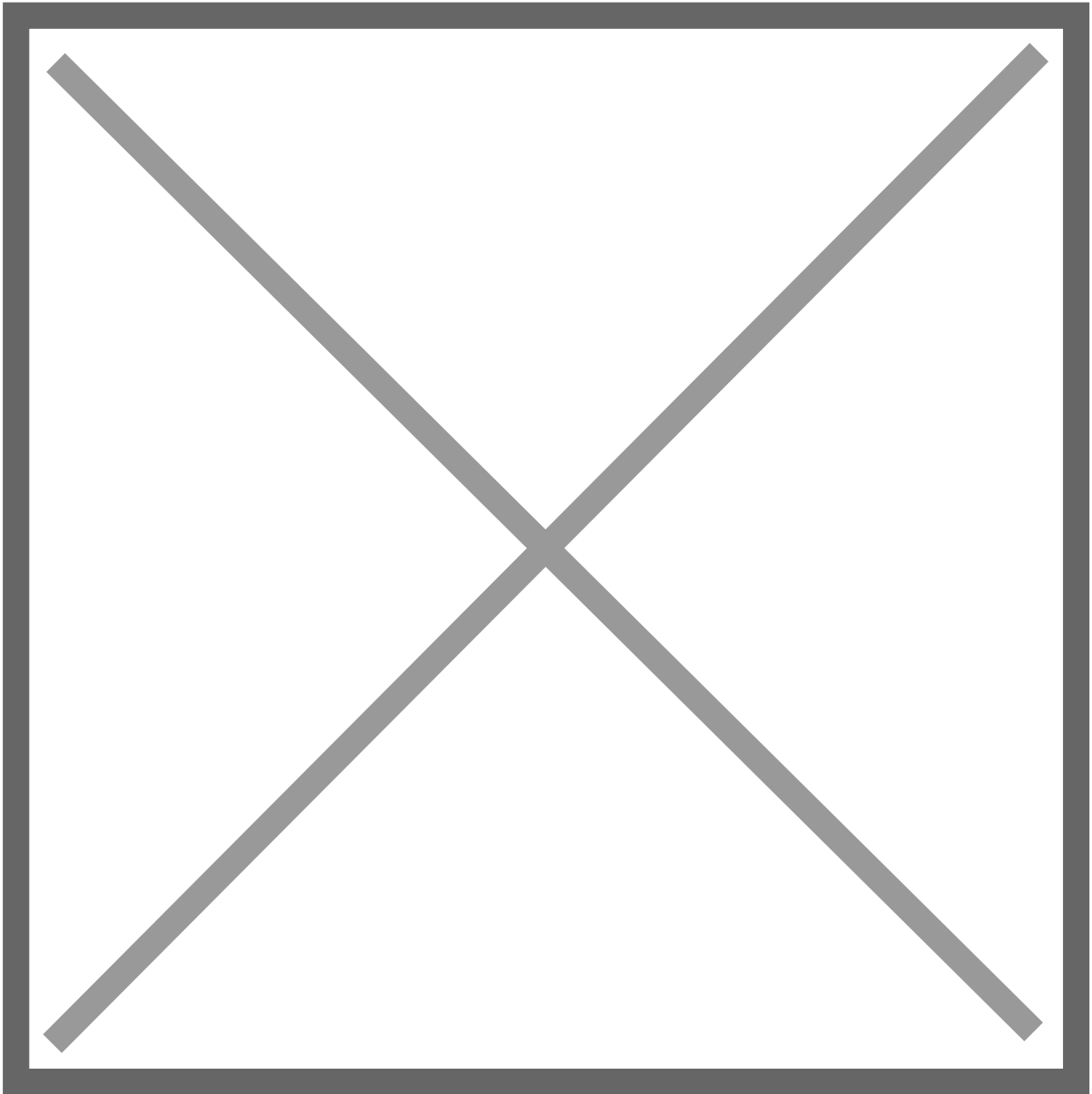
Once the new connection appears, select the connection, and select *Edit PE/CLAN IPs*:



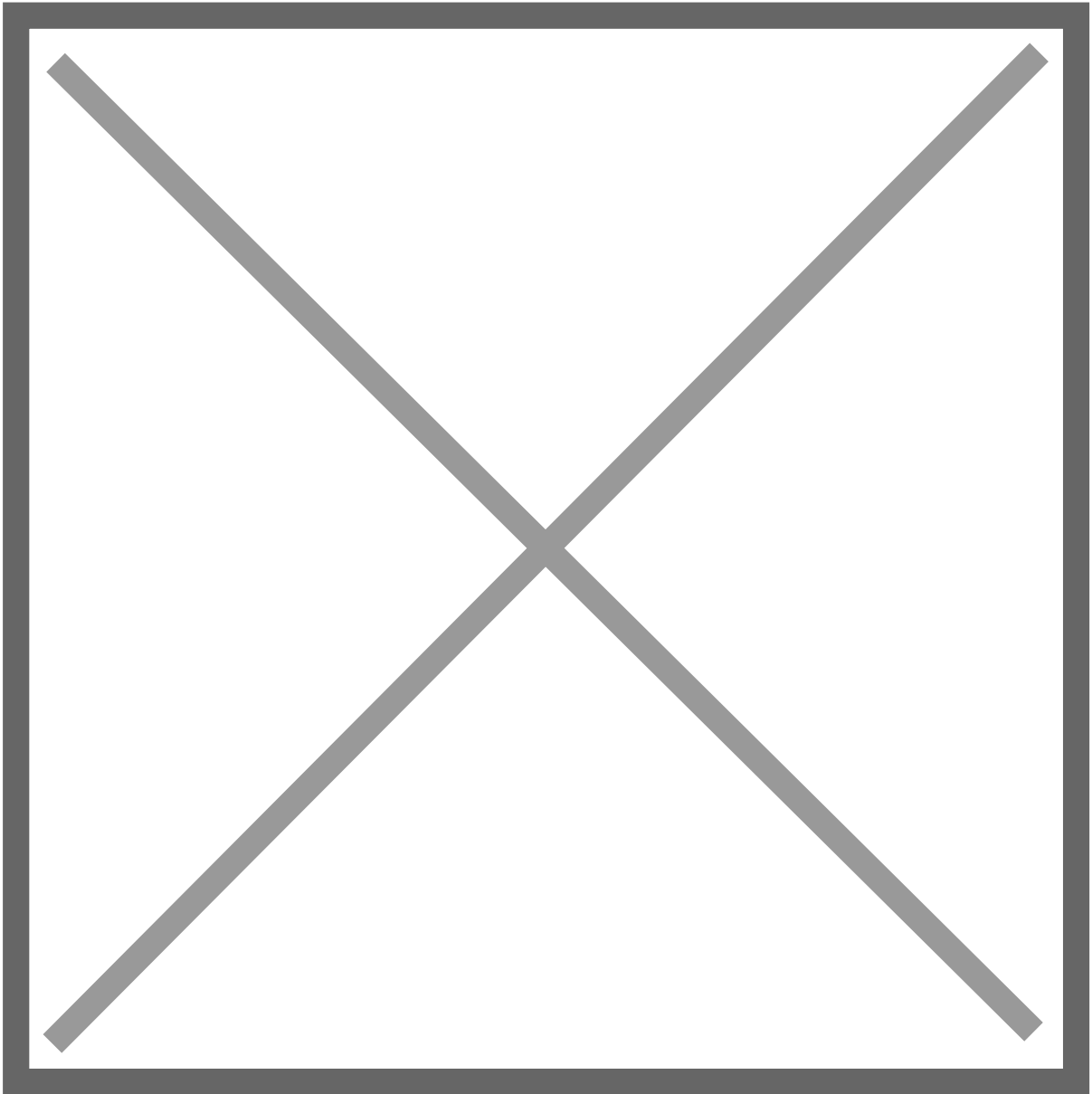
Type the IP address for the Processor Ethernet and click on *Add/Edit Name or IP*:



Navigate to **AE Services -> TSAPI -> TSAPI Links:**

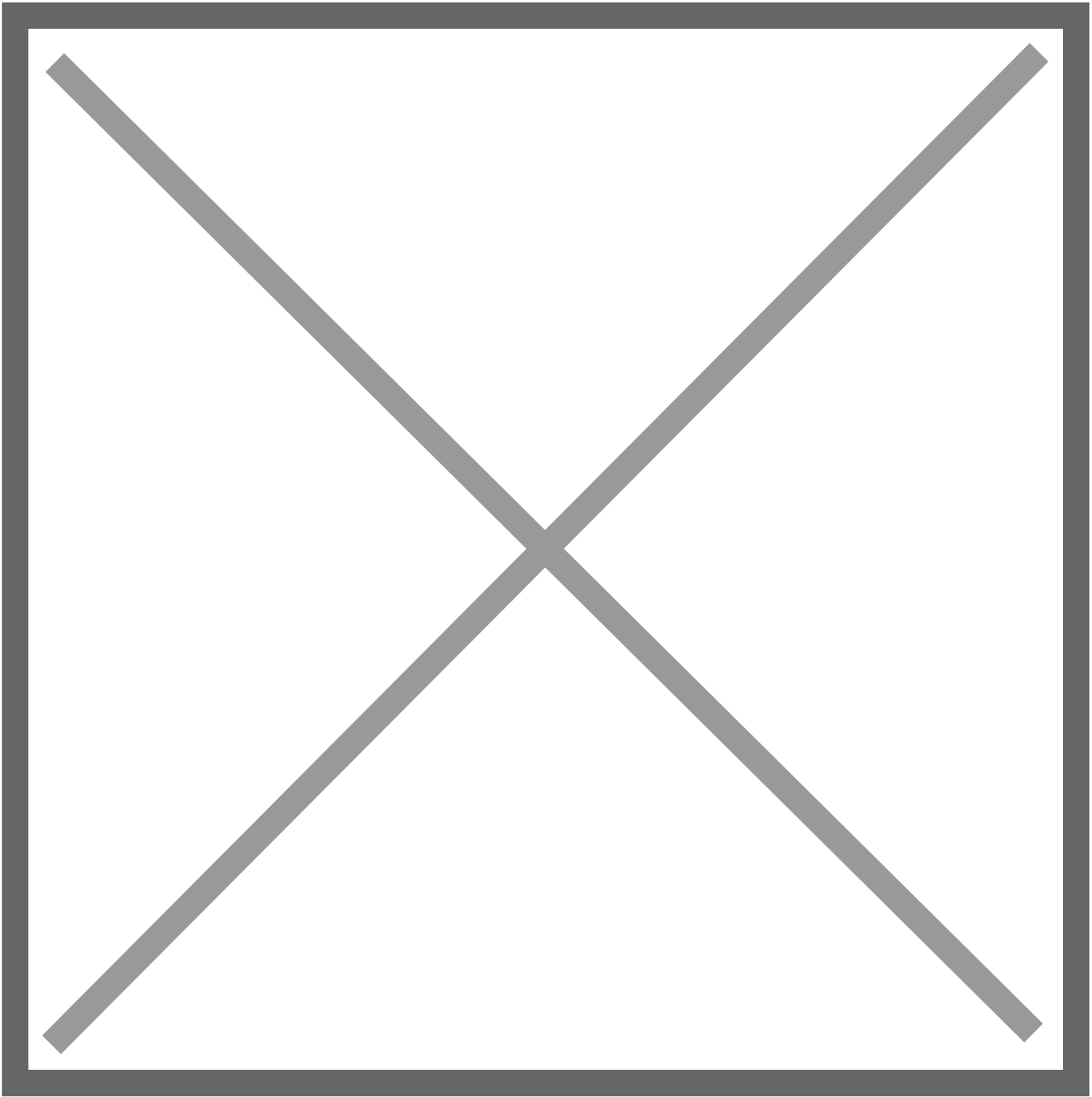


In the next screen assign a Link number, select the switch connection created and make sure you select the correct Switch CTI Link Number created in the PBX using the add cti x, in my case it is the cti link 1, on security you can select to have the TLINK encrypted, unencrypted or having both enabled.

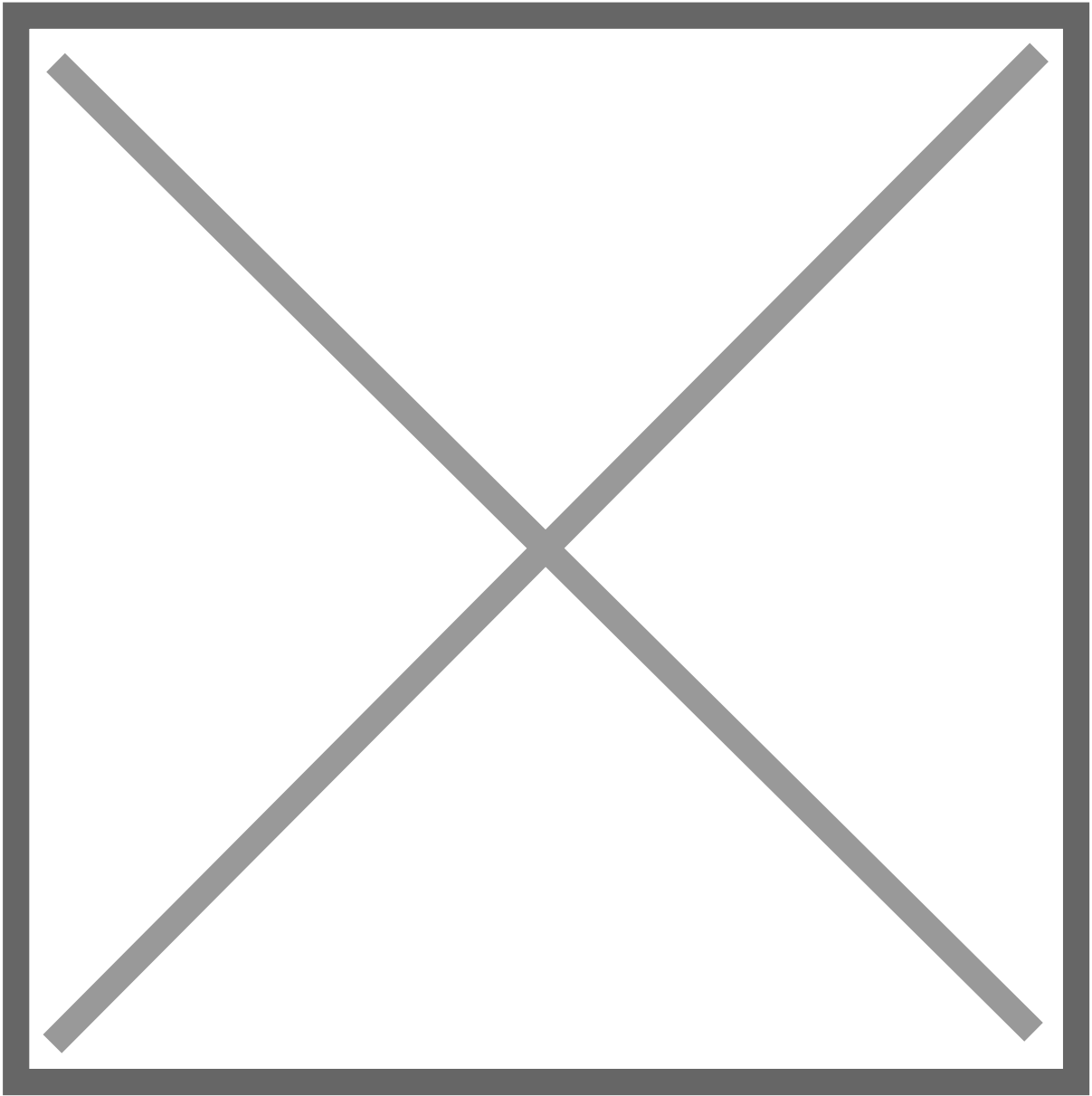


Lets complete this entry verifying the status of the CM Connection and the TSAPI CTI link:

Status -> Status and Control -> Switch Conn Summary



Status -> Status and Control -> TSAPI Service Summary



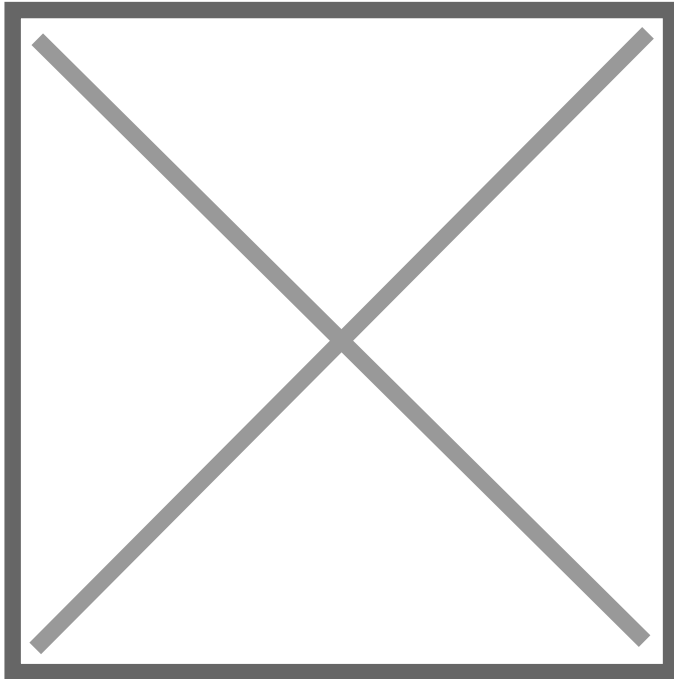
Source: <https://whereismyvoicepacket.com/avaya-aes-admin-task-aes-tsapi-cti-link-integration/>

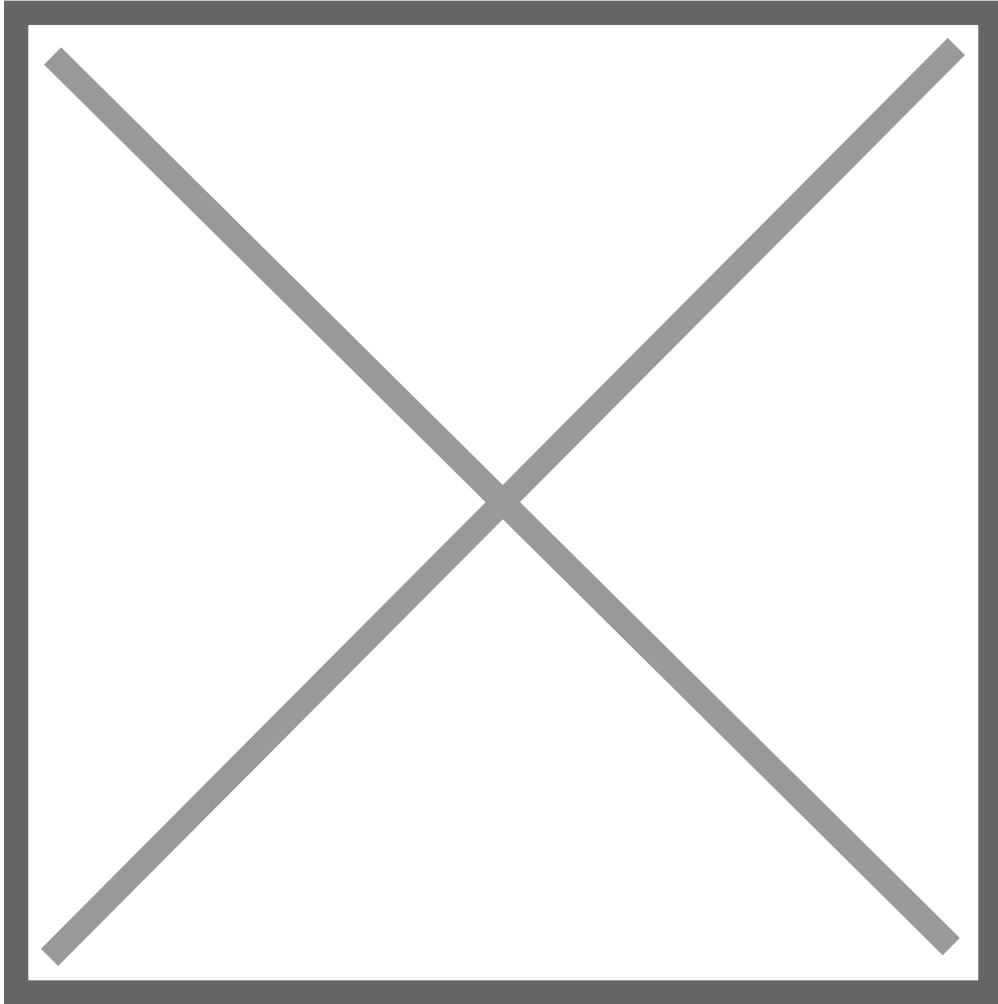
AES - Upgrade 8.0.1 to 8.1.3

In this entry we will focus in upgrading an AES version 8.1.2 to 8.1.3, to accomplish this we will first deploy a new VM with OVA 8.1.3 file version and we will connect it into the network using a temporary IP address, allowing us to perform preparation task and have the VM ready just for the cut over maintenance window.

In order to simplify the information presented and the simplicity of the OVA deploy, it will be omitted, the most important part in this step is setting up the network connection using a temporary IP address, this can be completed within the wizard or using the command (using the proper permissions):

```
/opt/mvap/bin/netconfig
```

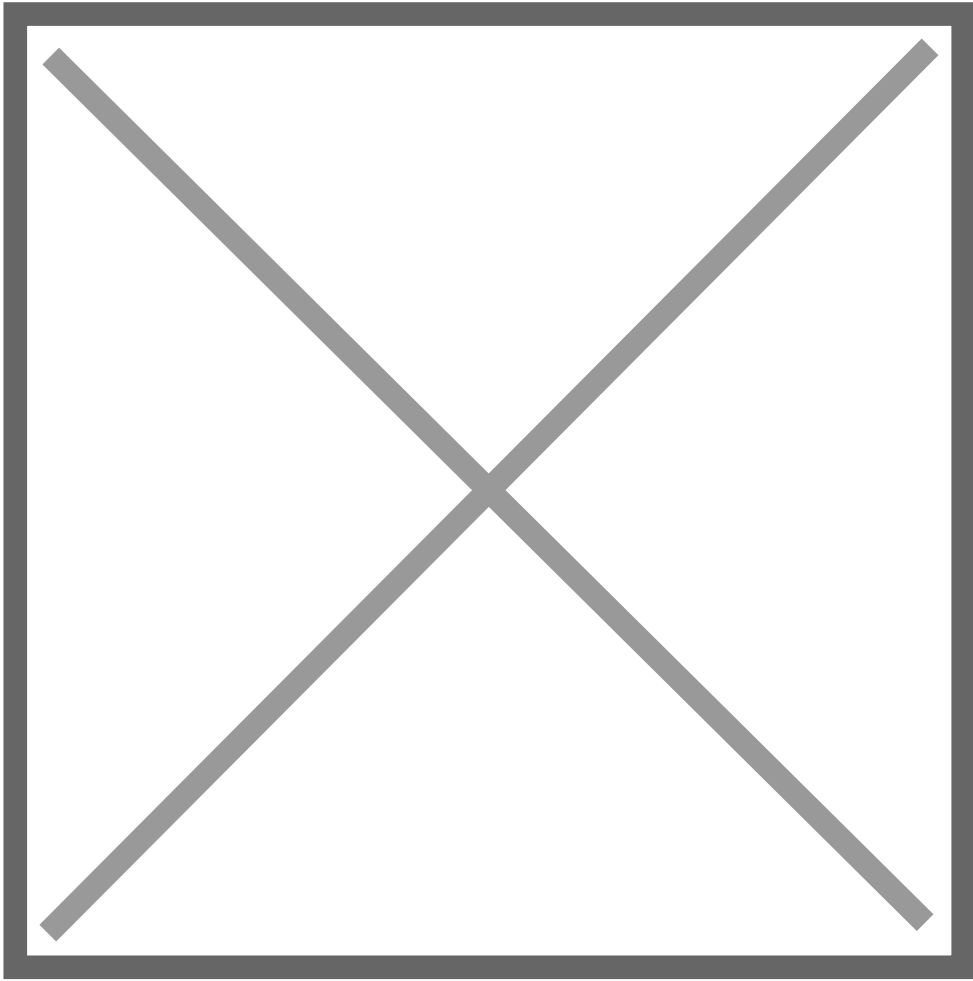


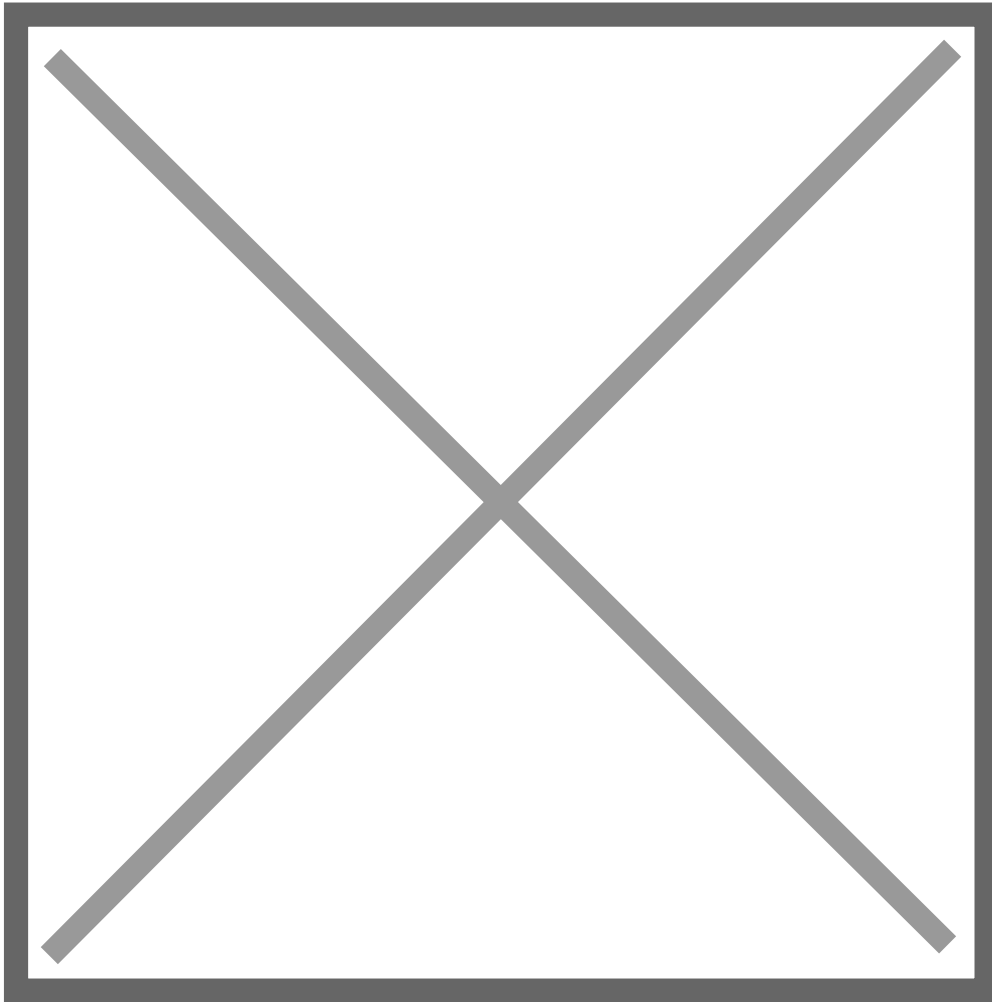


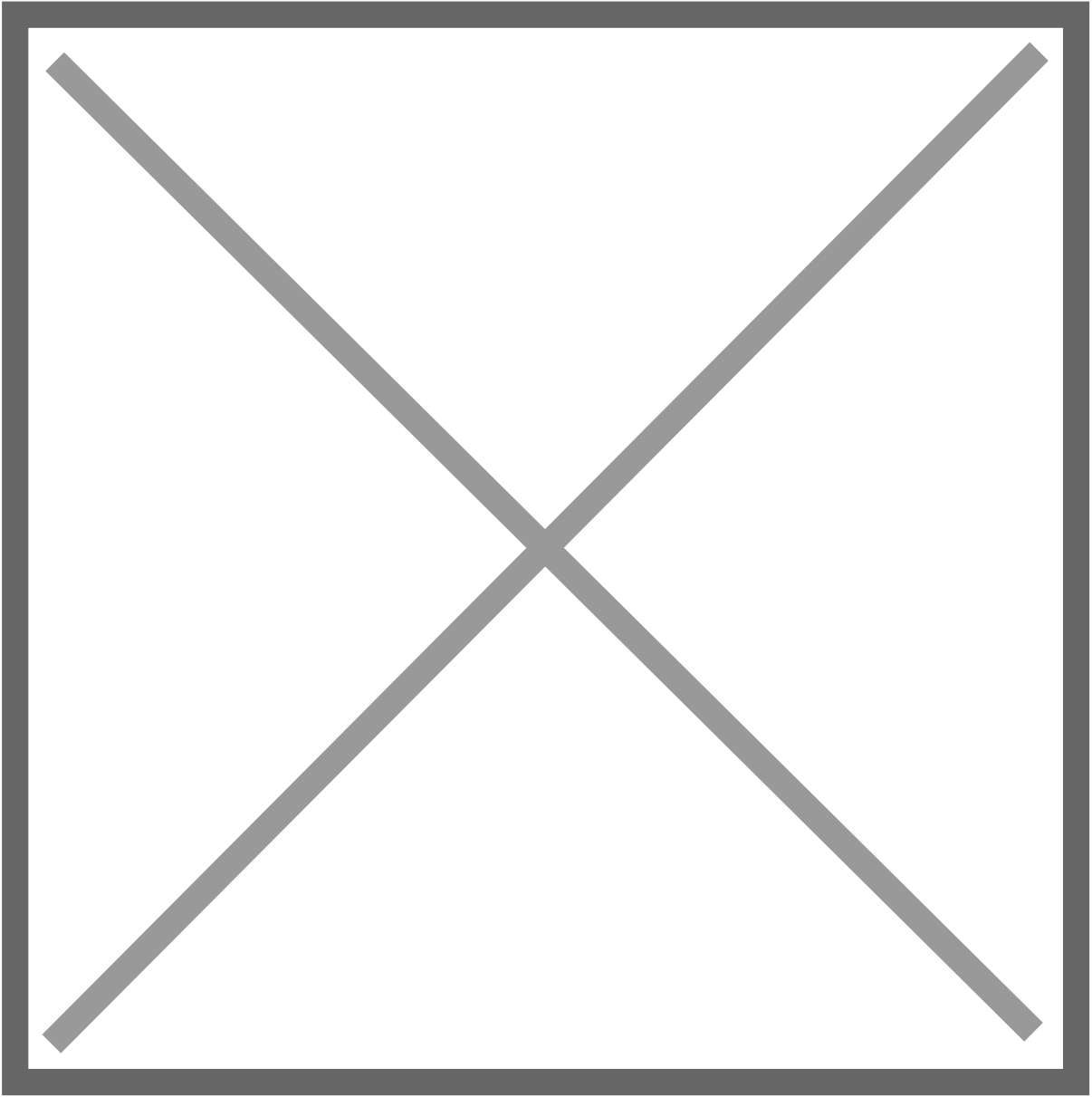
We will use the previous command later in this entry.

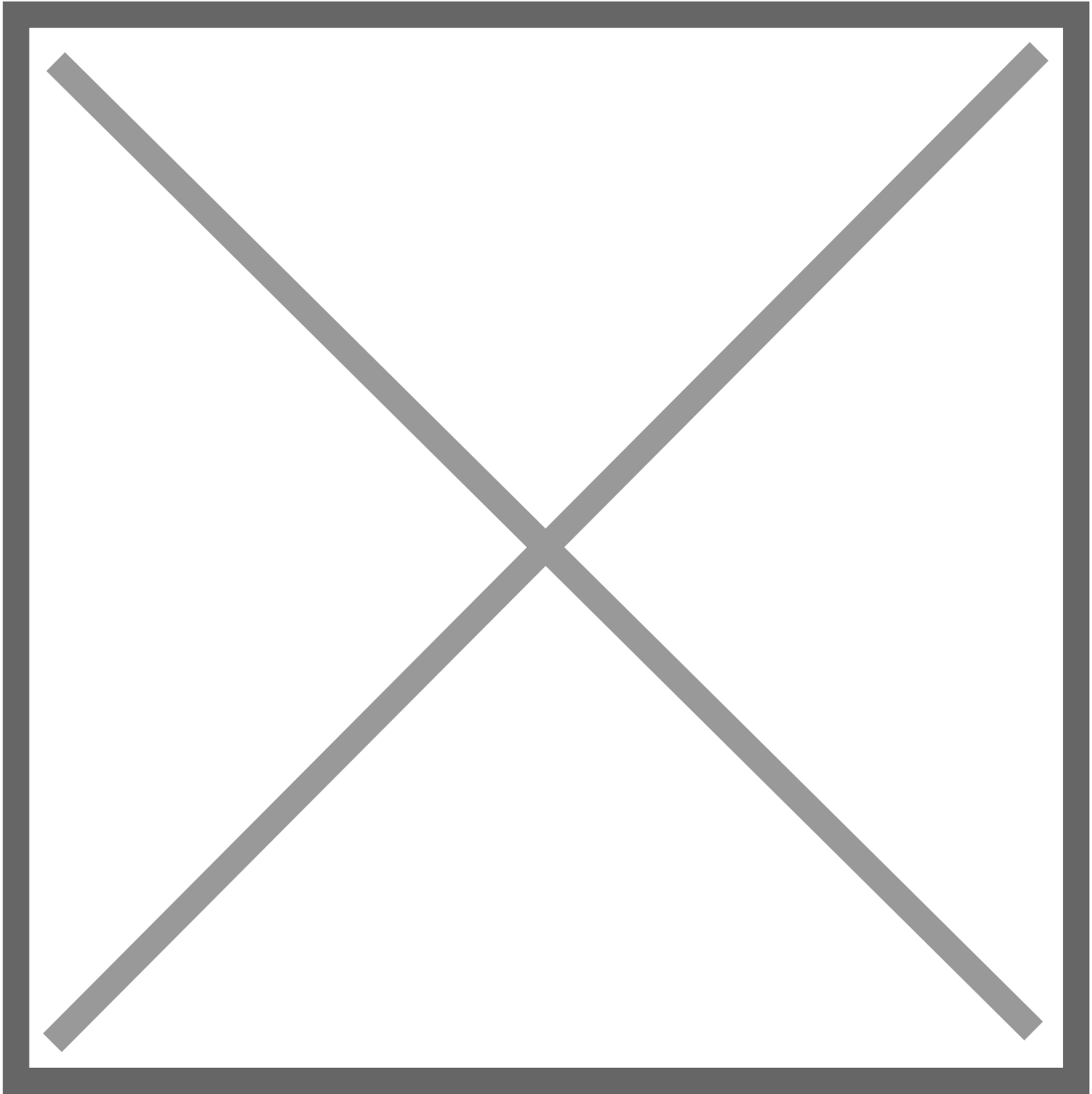
Here is the process to follow:

1. Apply the service pack/feature pack/Linux Security Update (refer to the entry **Avaya AES - Admin task - Update process** in case of any doubt)



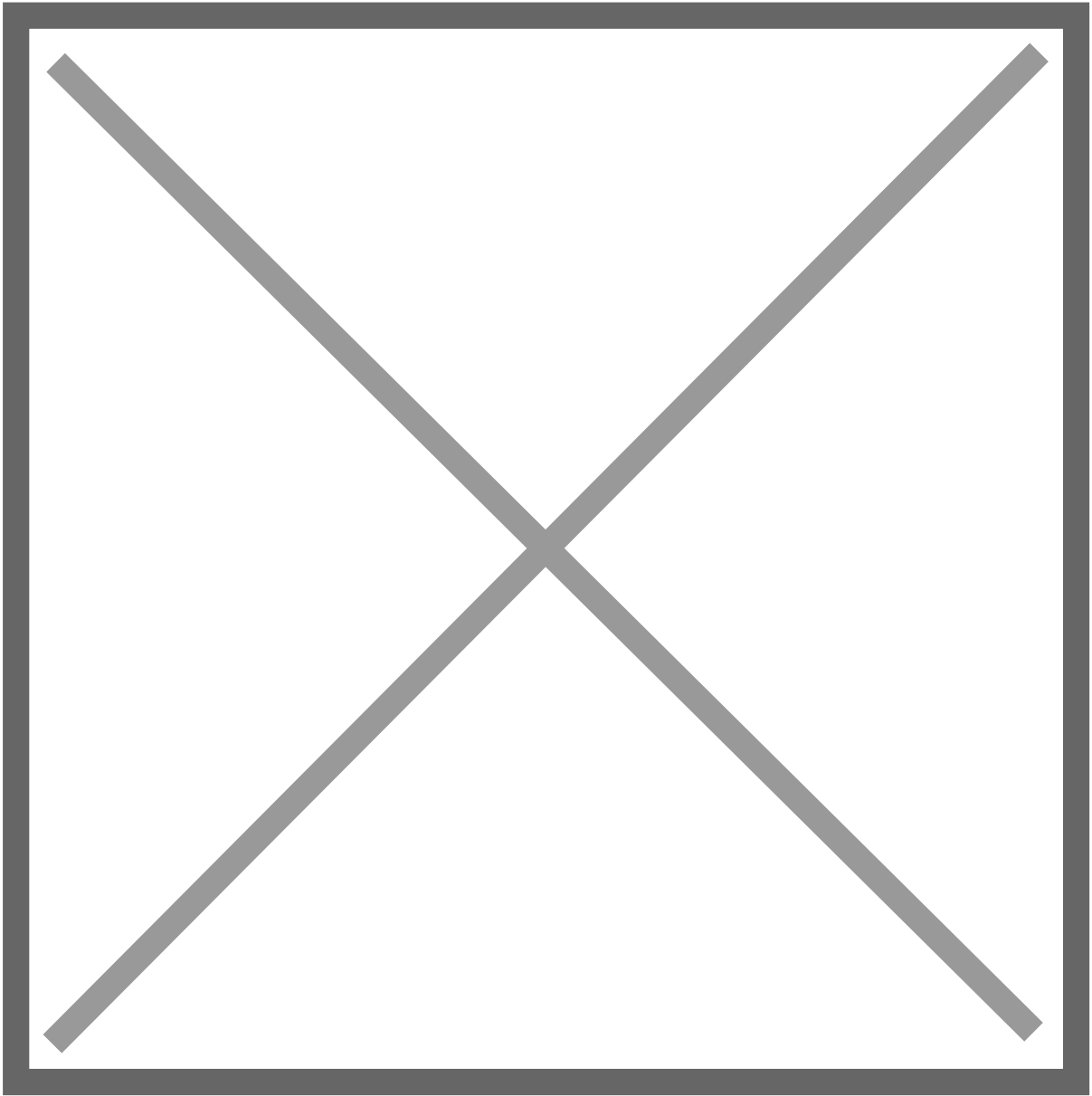




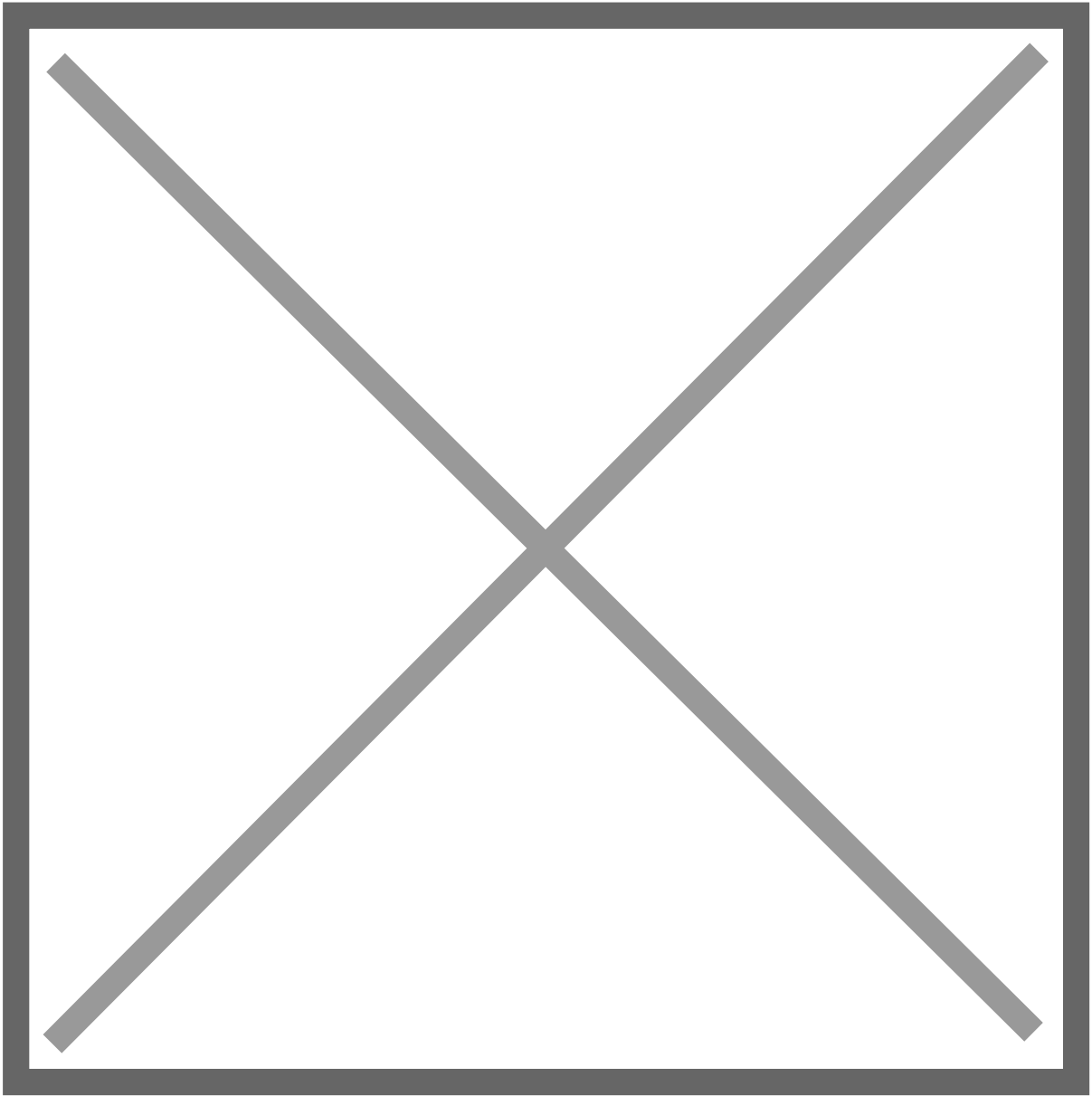


2. Keep track of the current configuration Backup configuration (Screenshots)

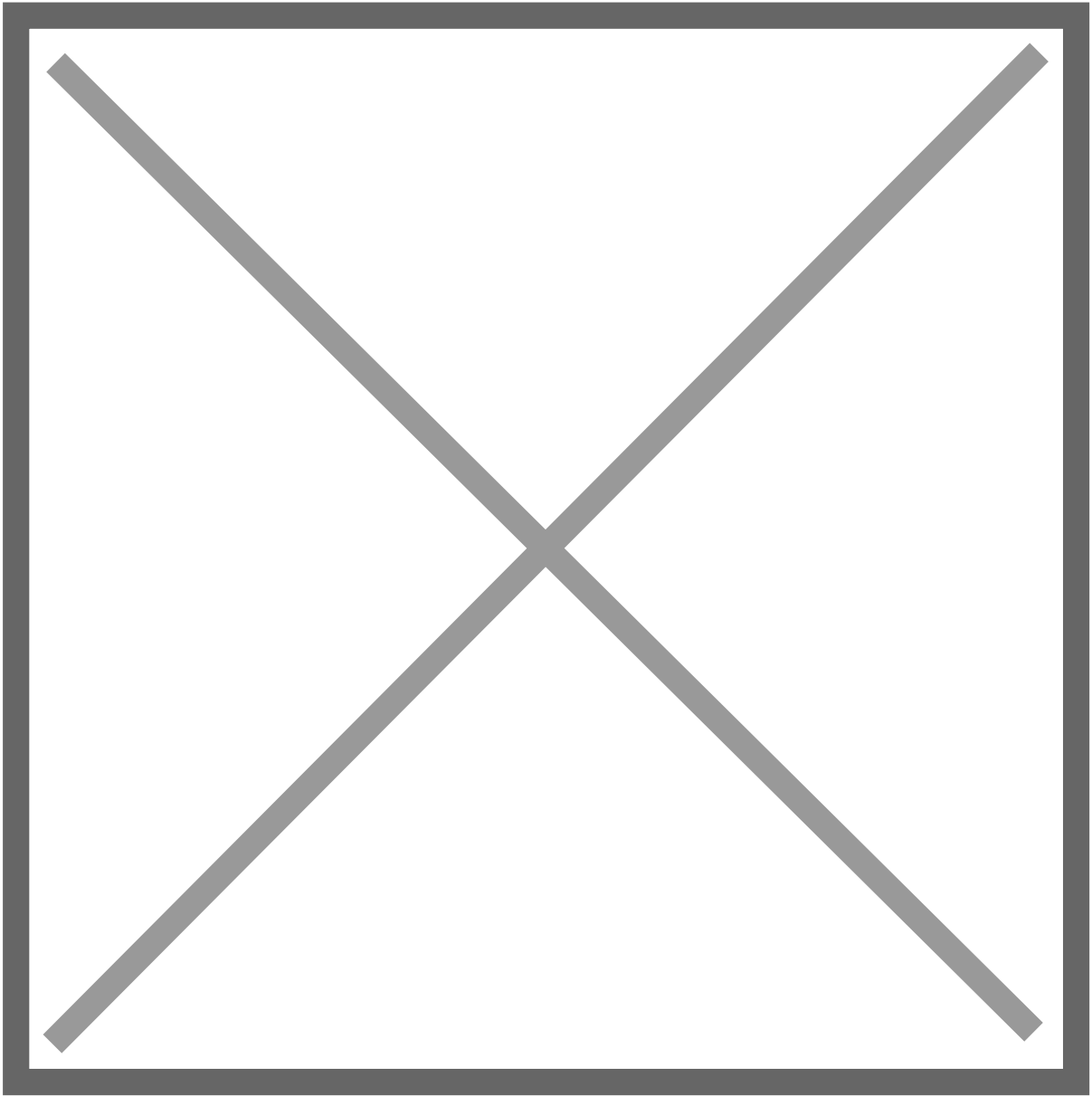
AE Services



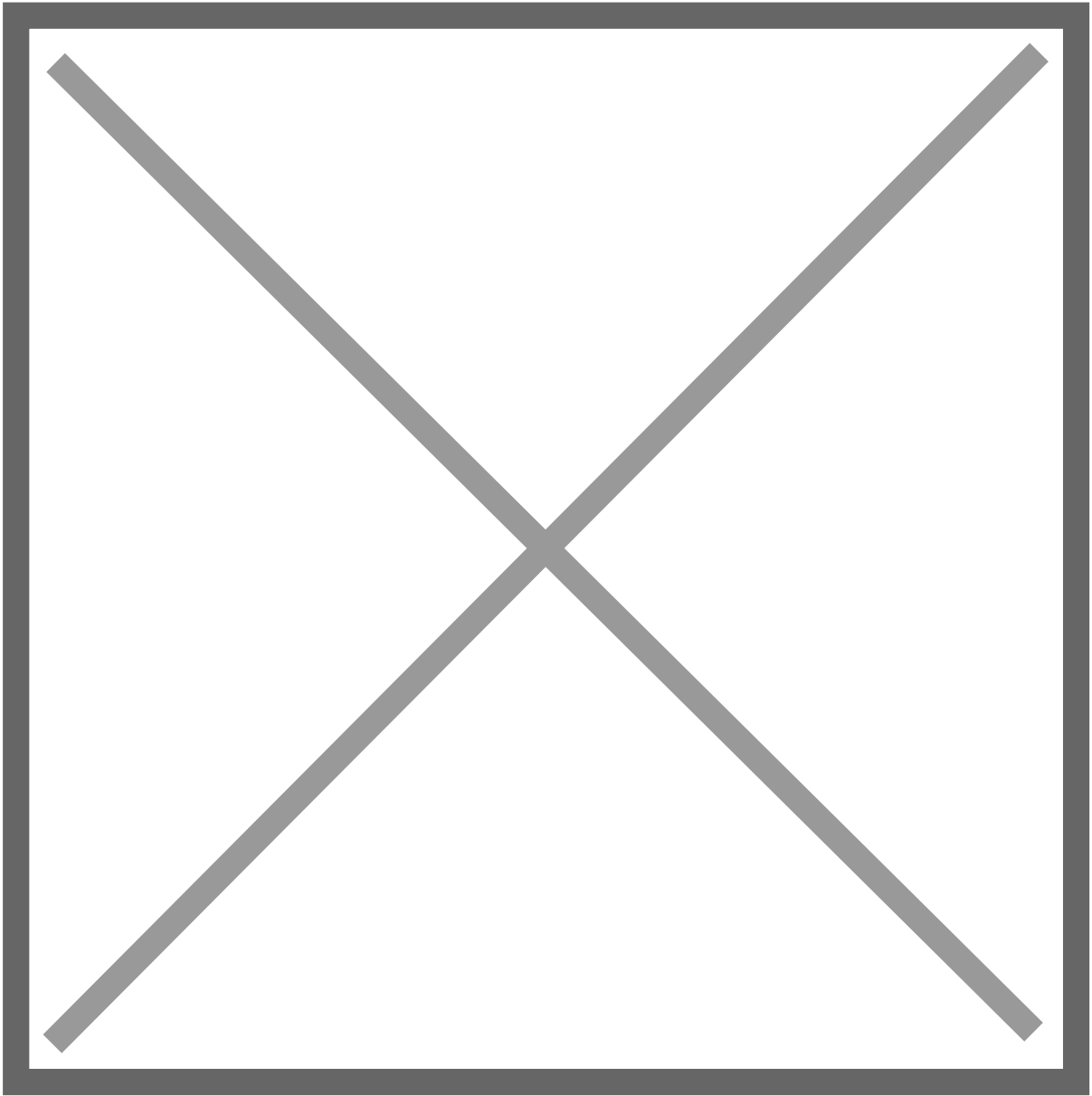
AES Services -> CVLAN -> CVLAN Links



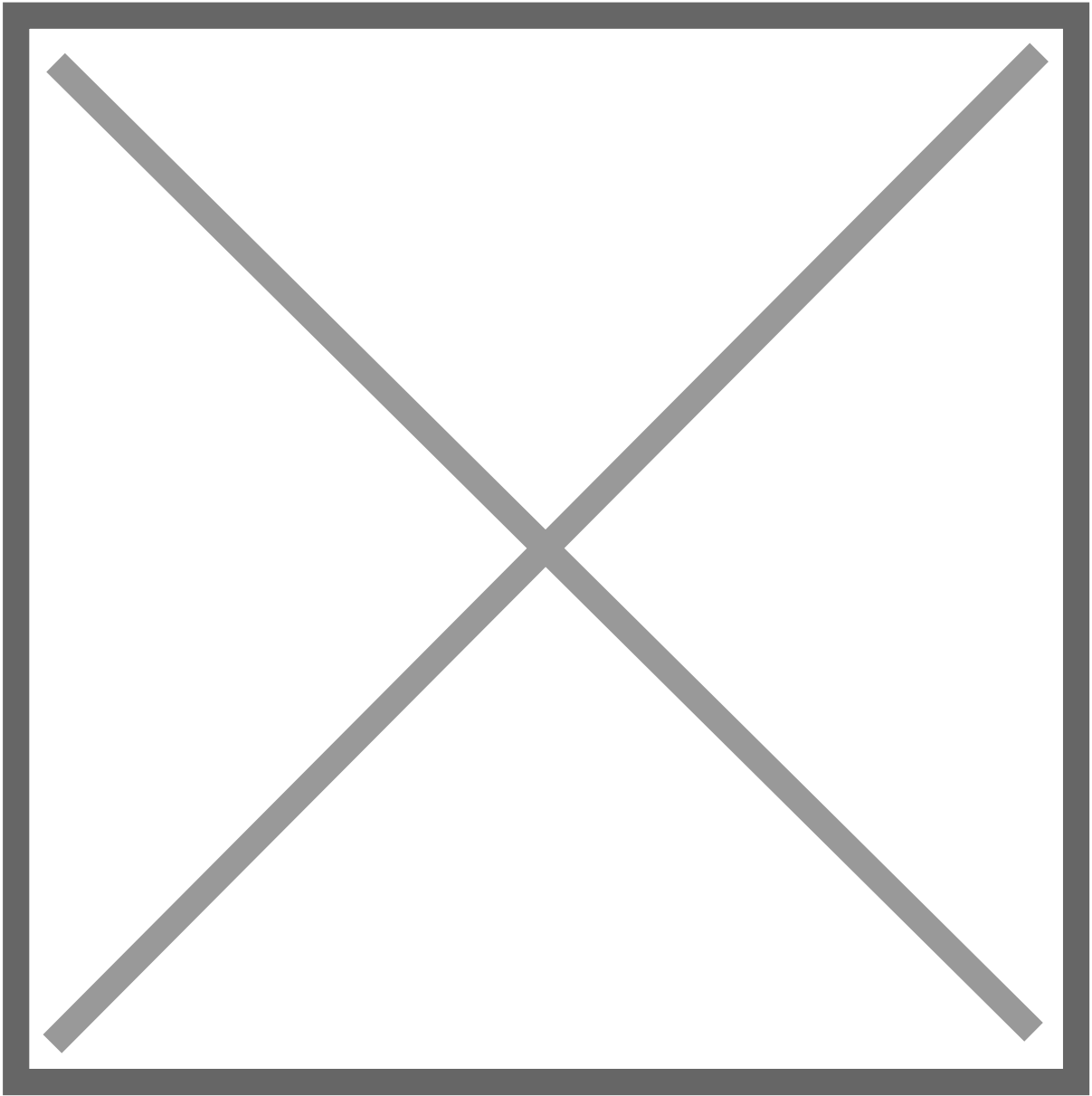
AES Services -> TSAPI -> TSAPI Links



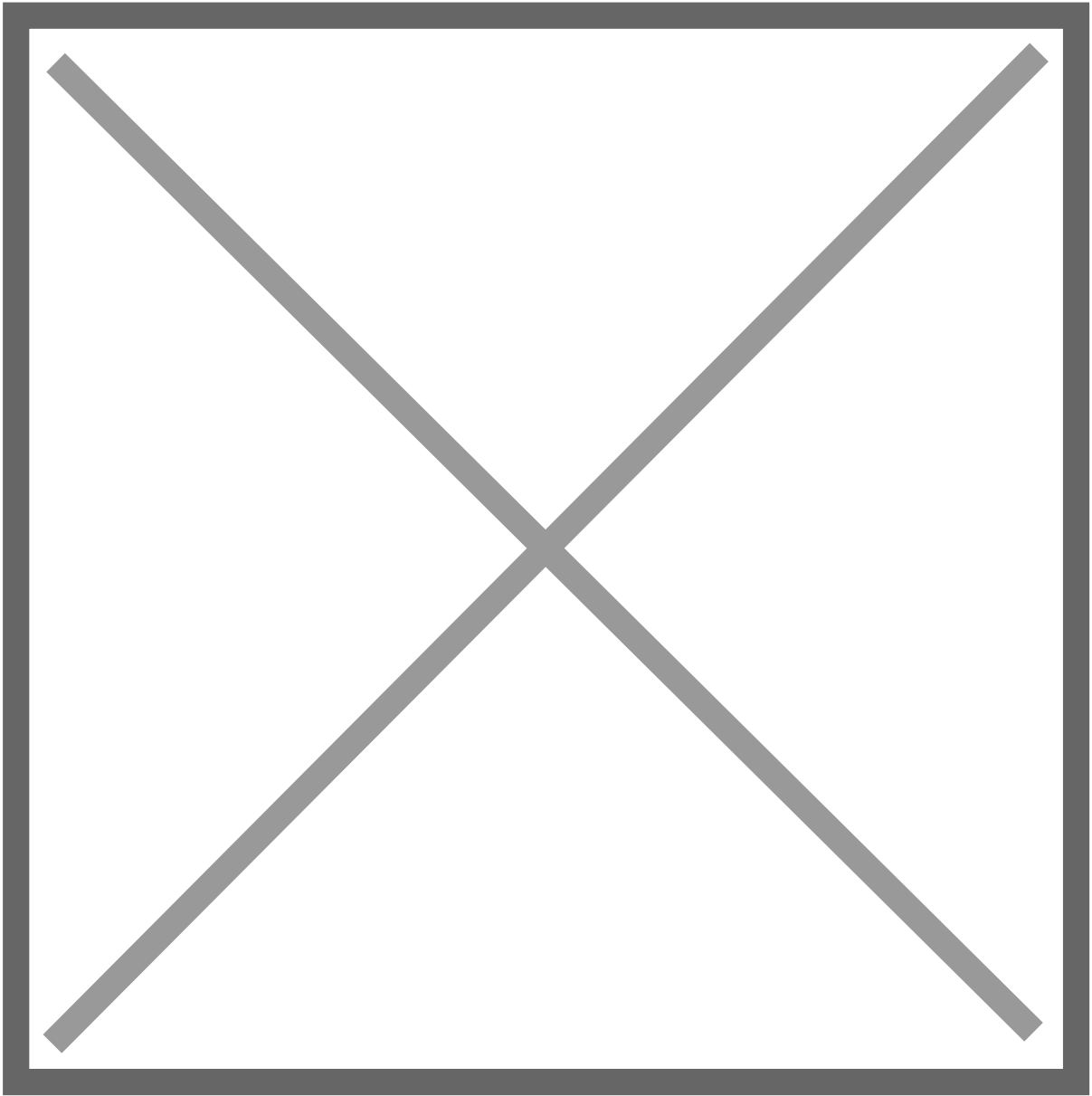
Communication Manager Interface -> Switch Connections



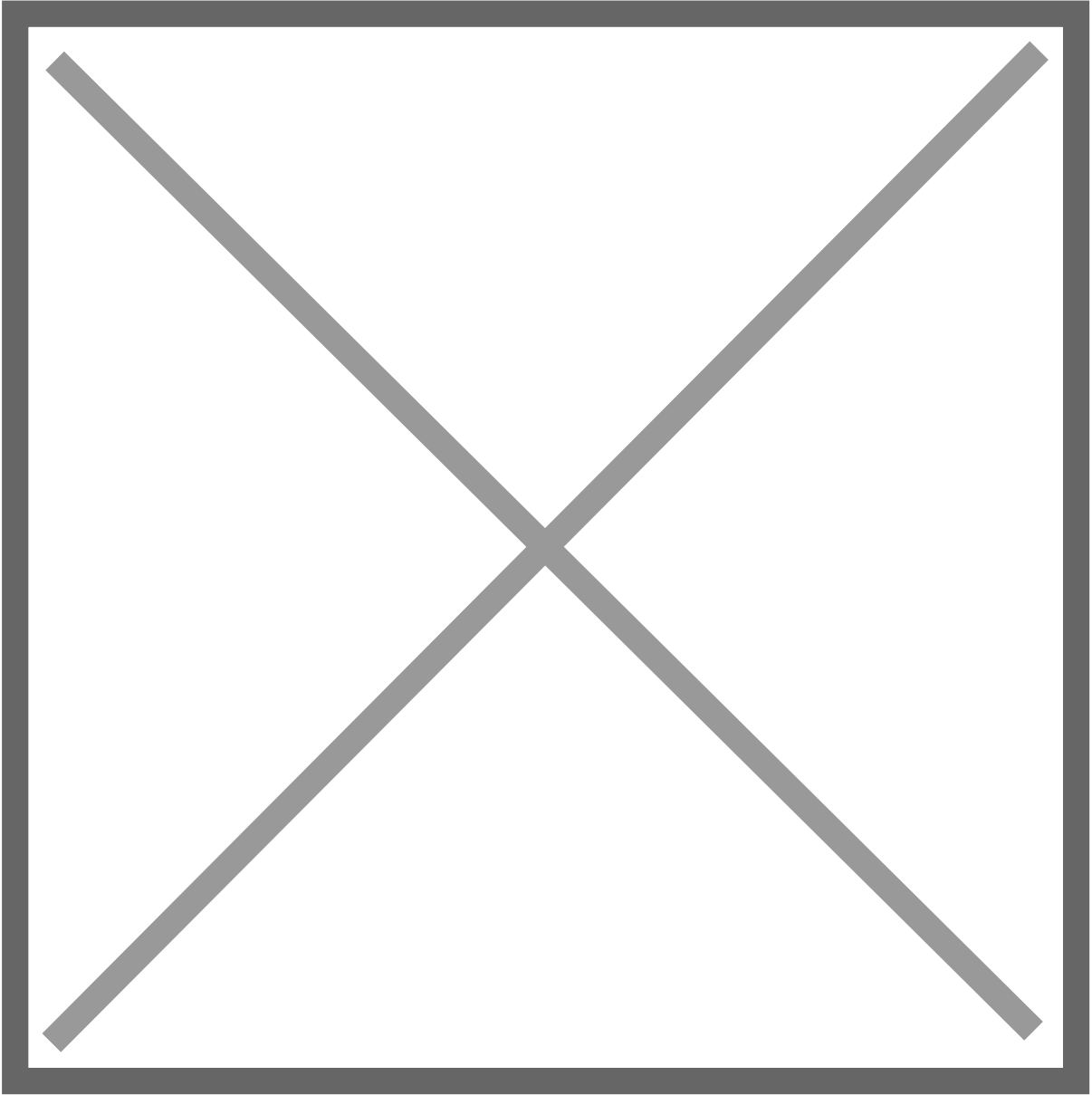
Communication Manager Interface -> Switch Connections -> Edit Connection



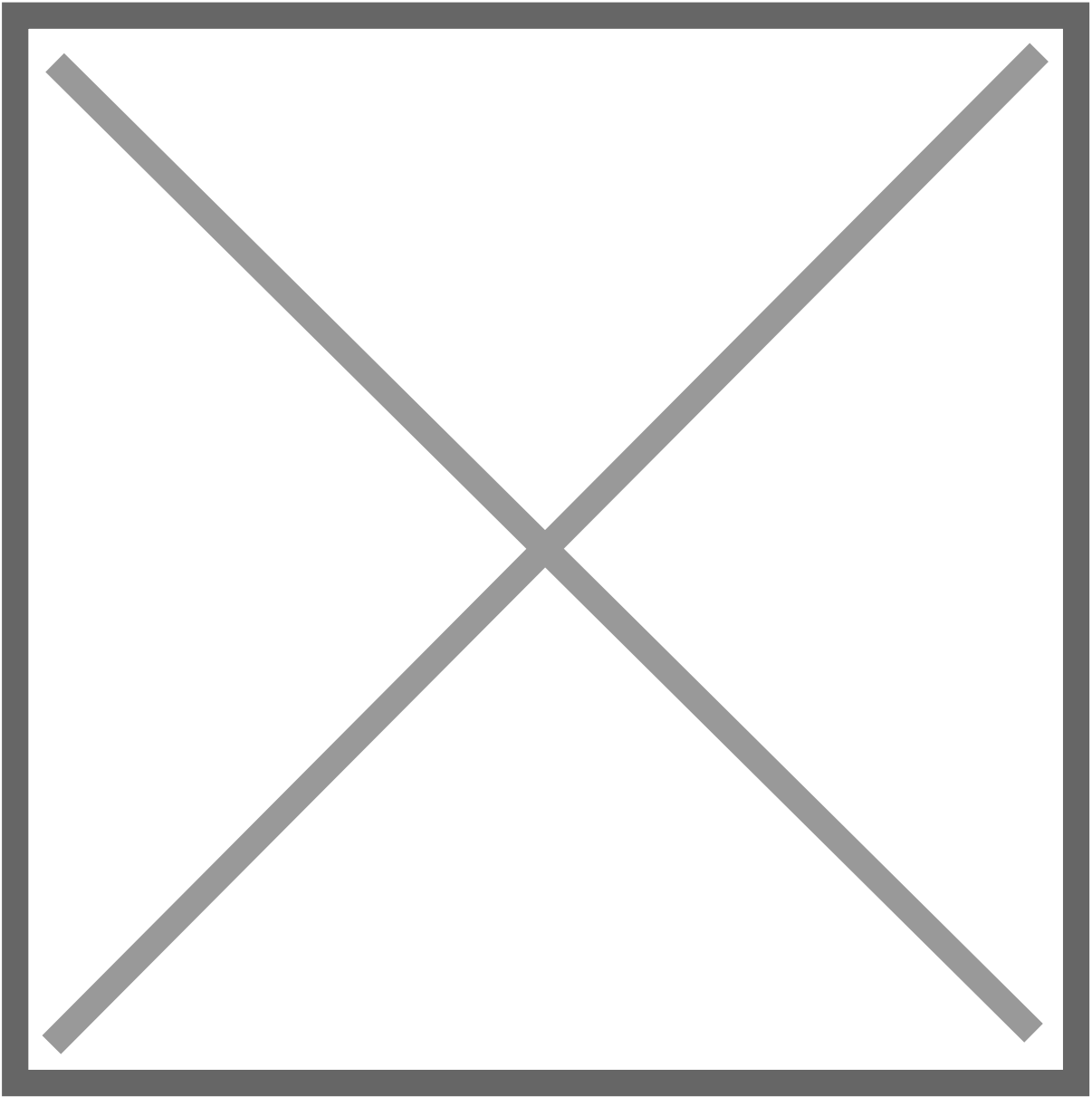
Communication Manager Interface -> Switch Connections -> Edit PE/CLAN IPs



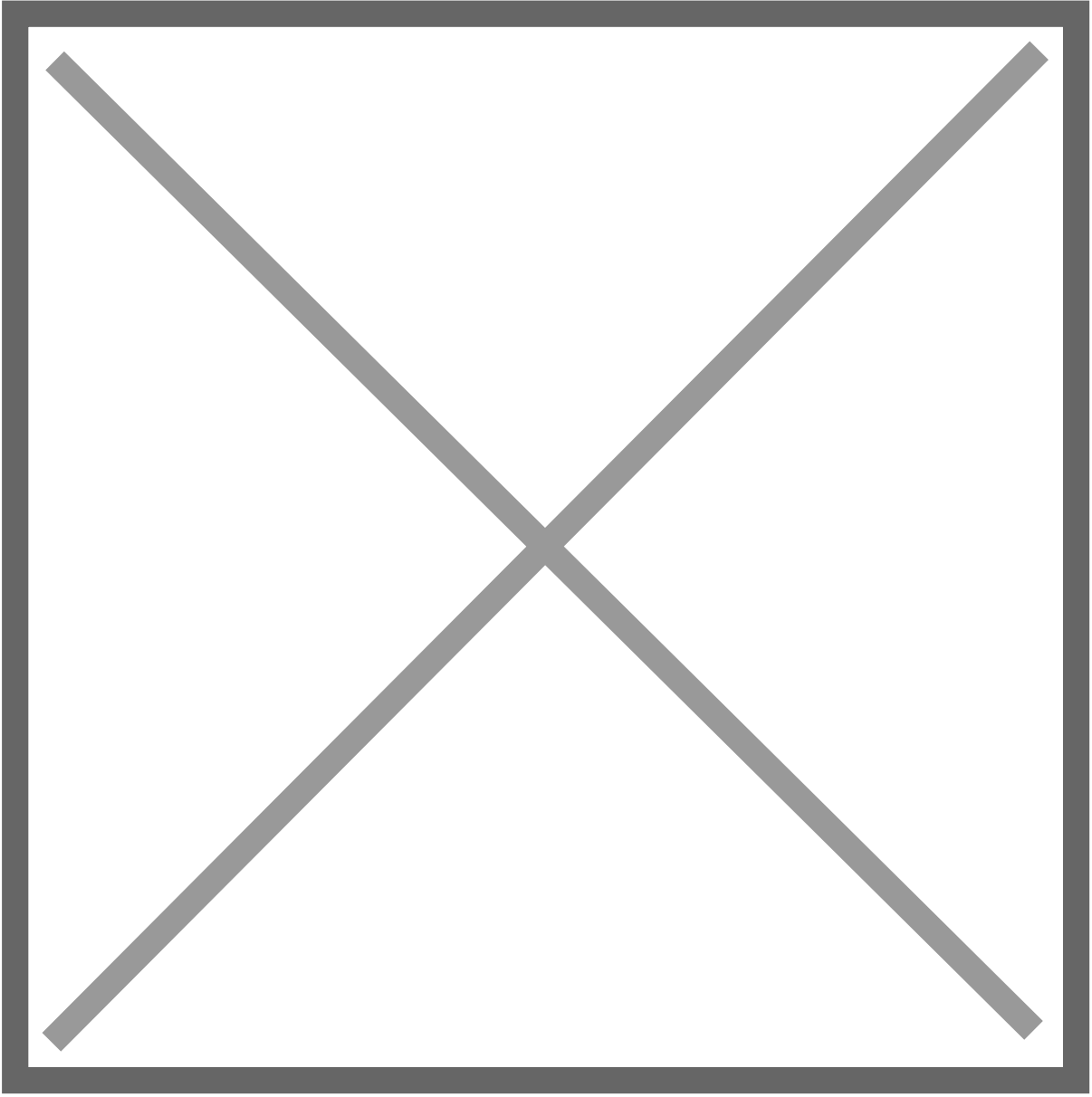
Communication Manager Interface -> Switch Connections -> Survivability Hierarchy

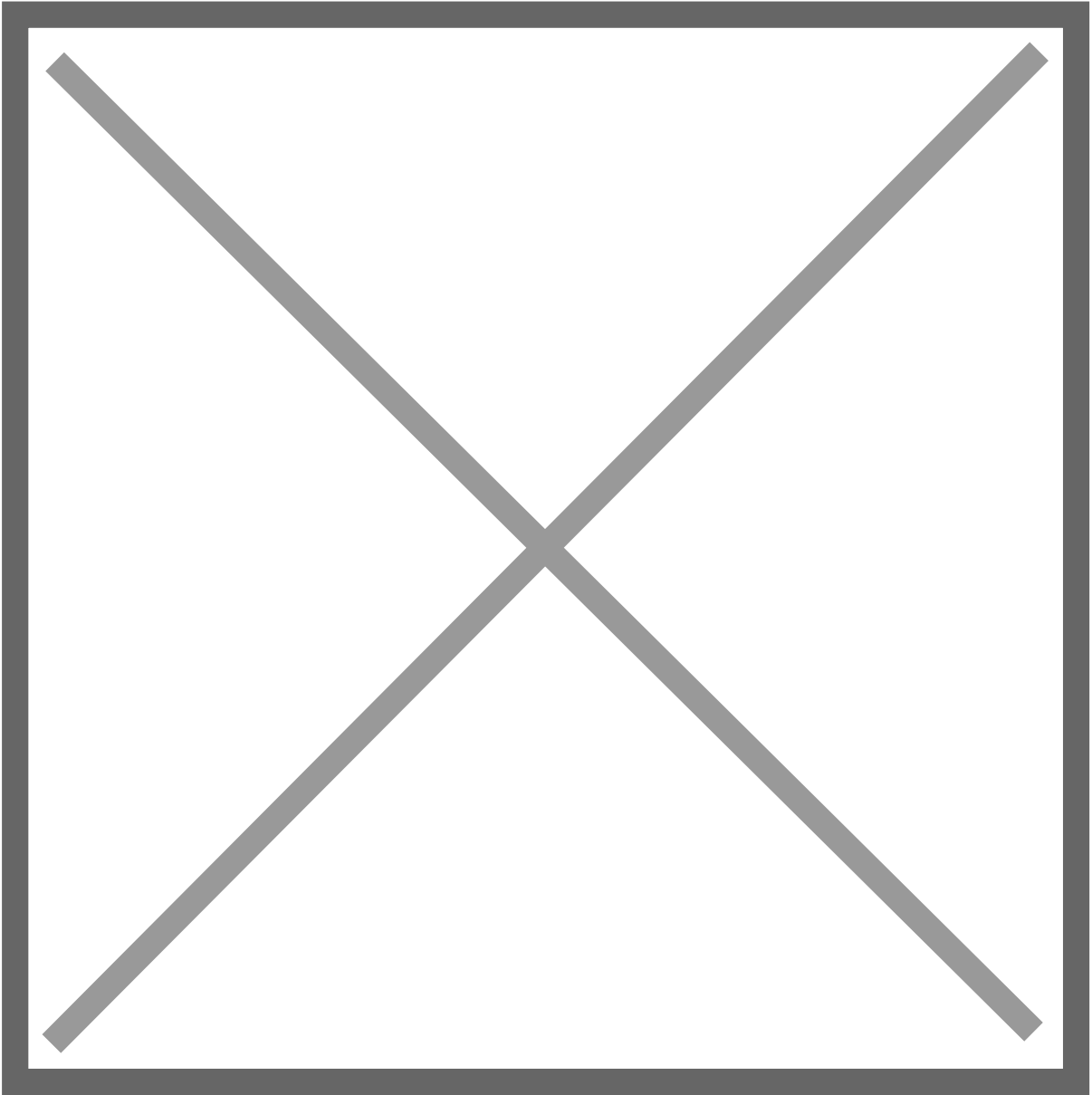


Maintenance -> Date Time/NTP Server

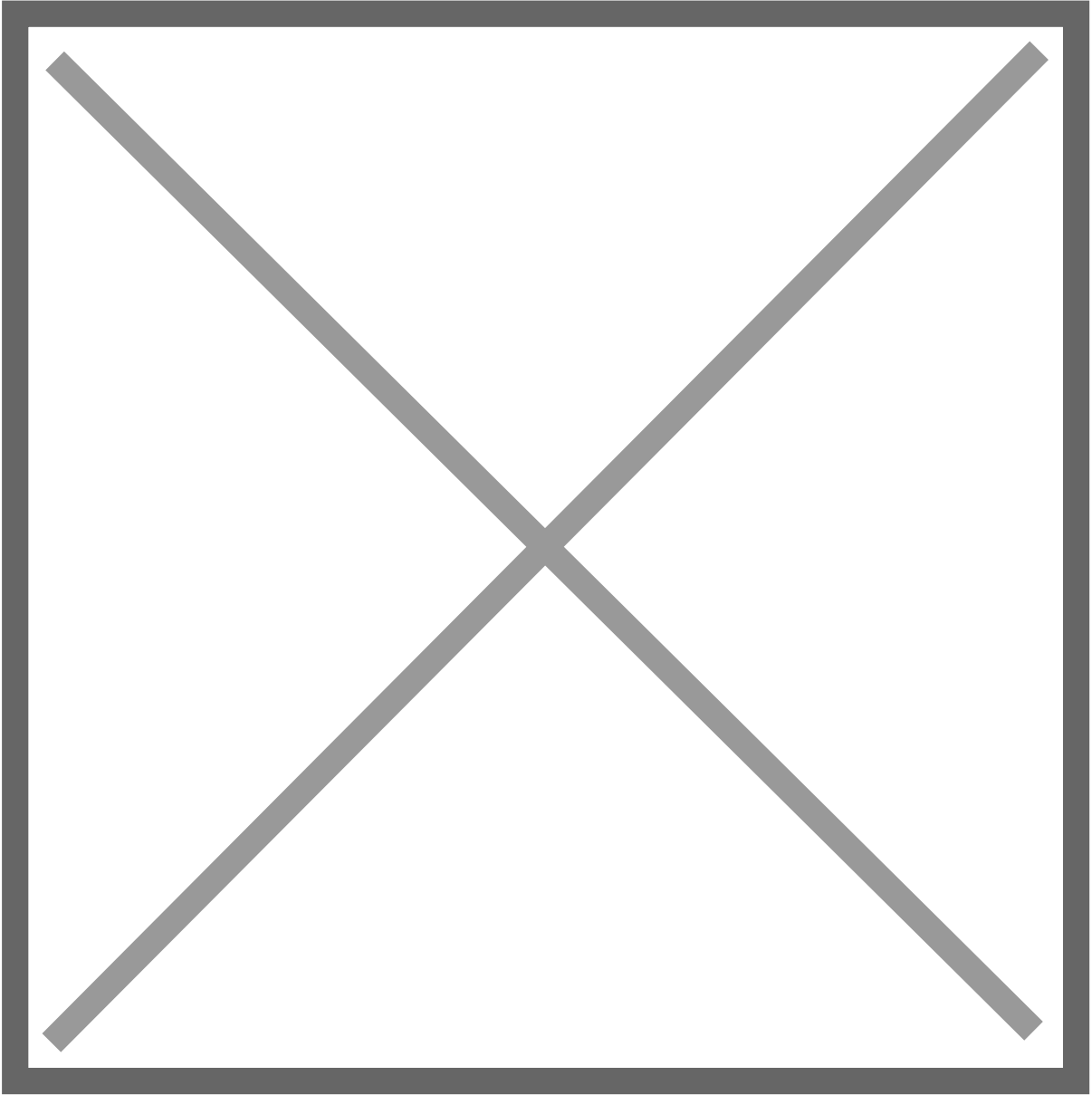


Networking -> Network Configure

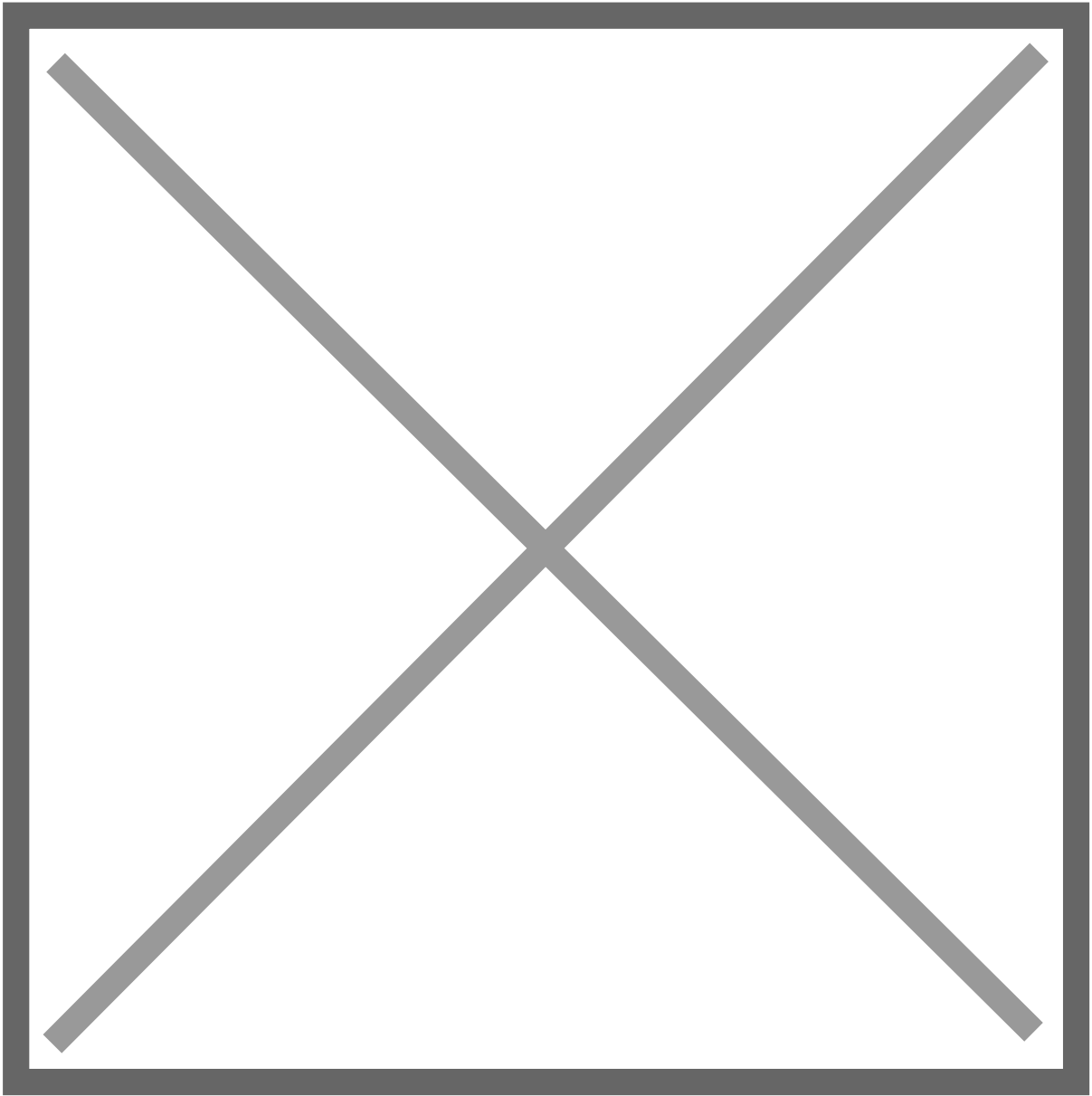




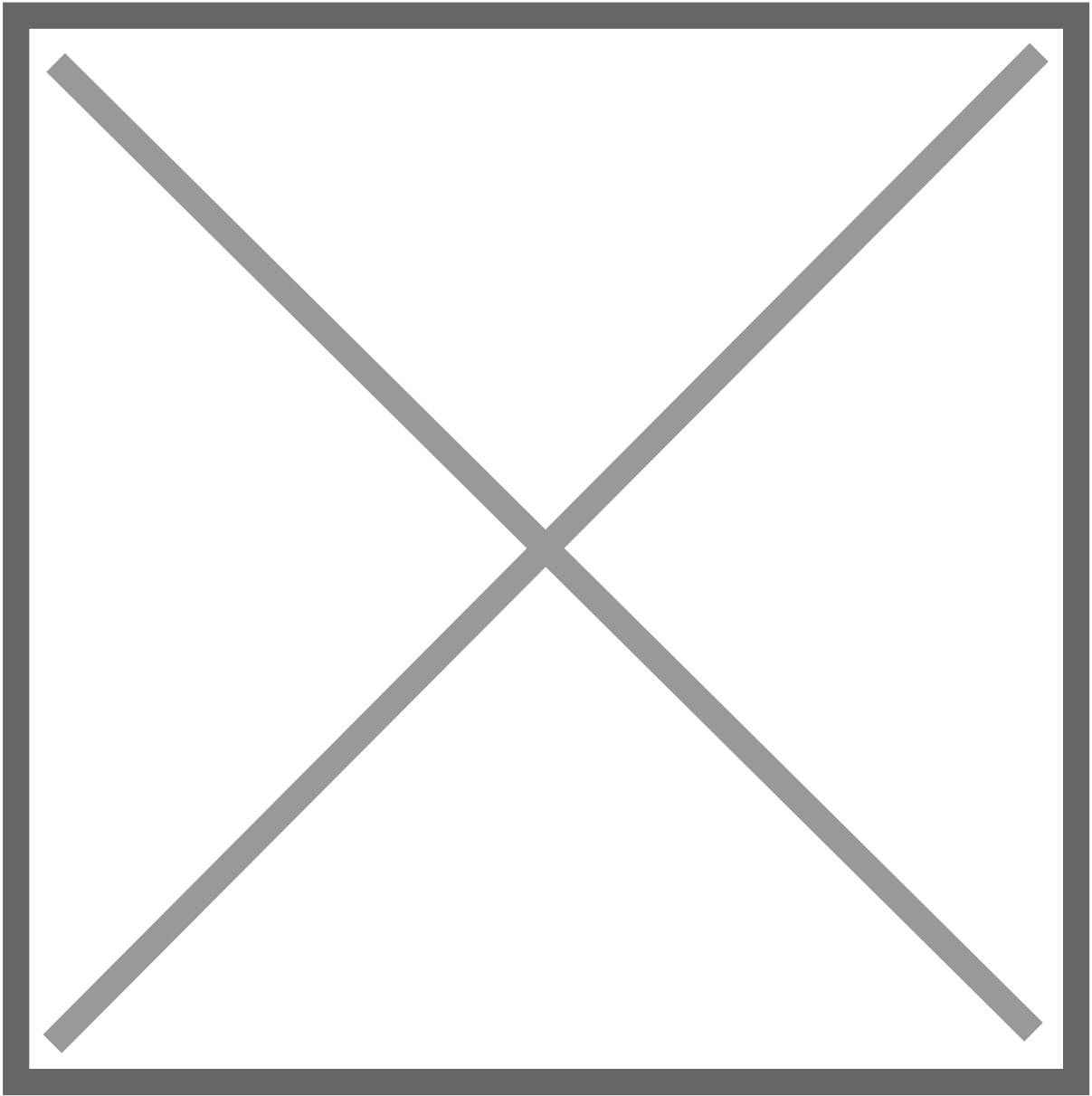
Security -> Security Database -> Tlinks



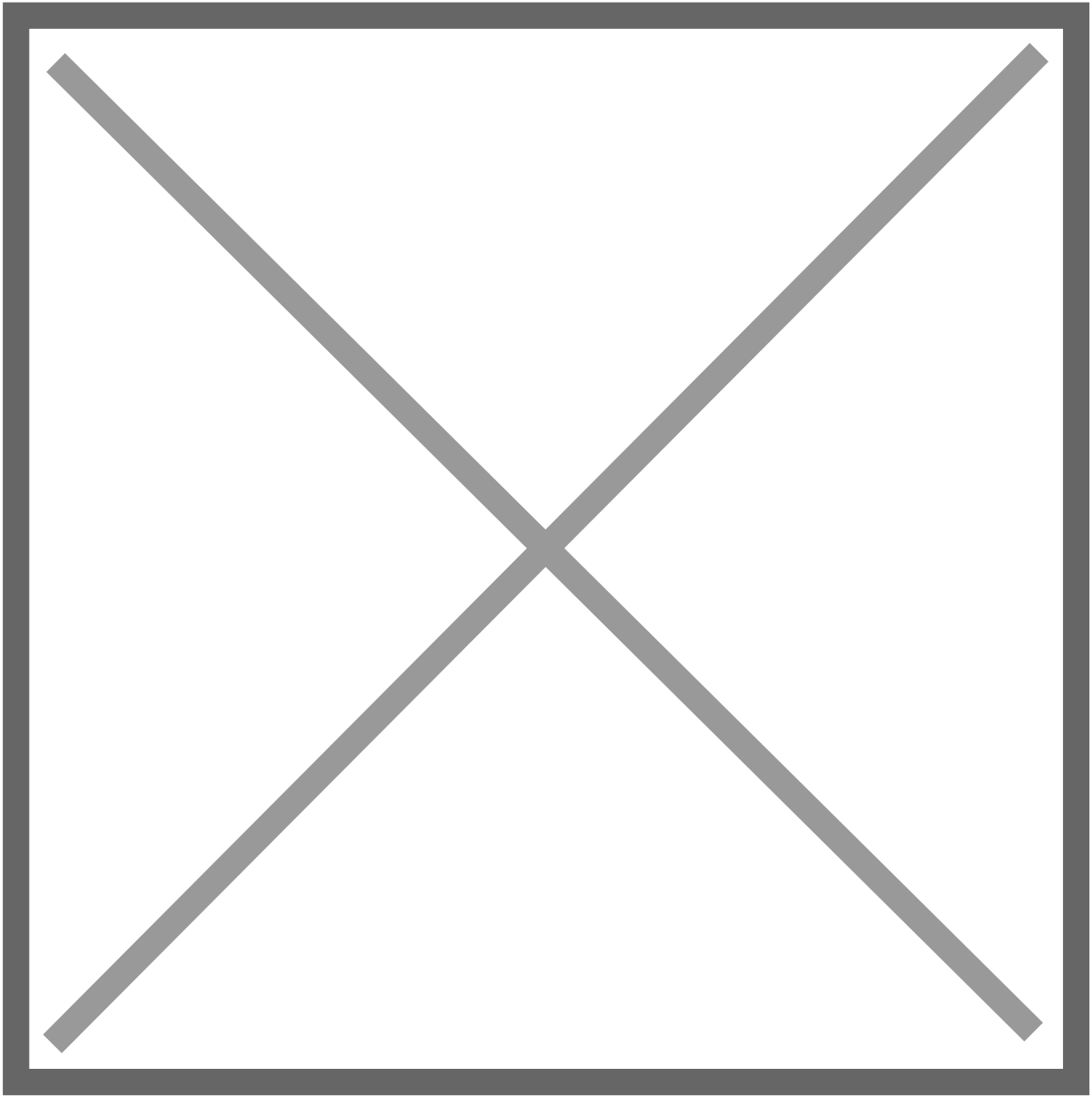
Status -> Switch Conn Summary



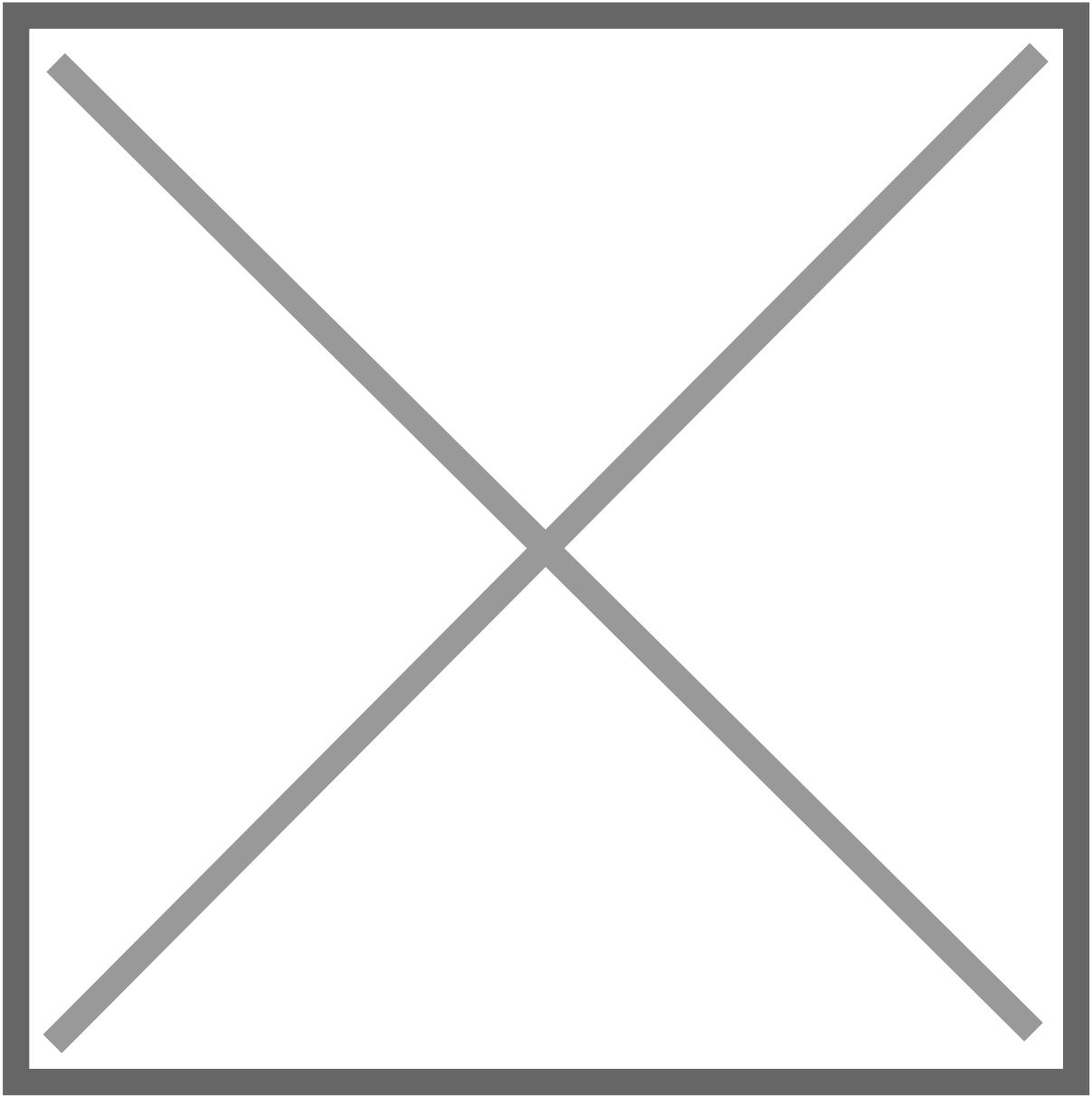
Status -> TSAPI Service Summary



Utilities -> SNMP -> SNMP Agent

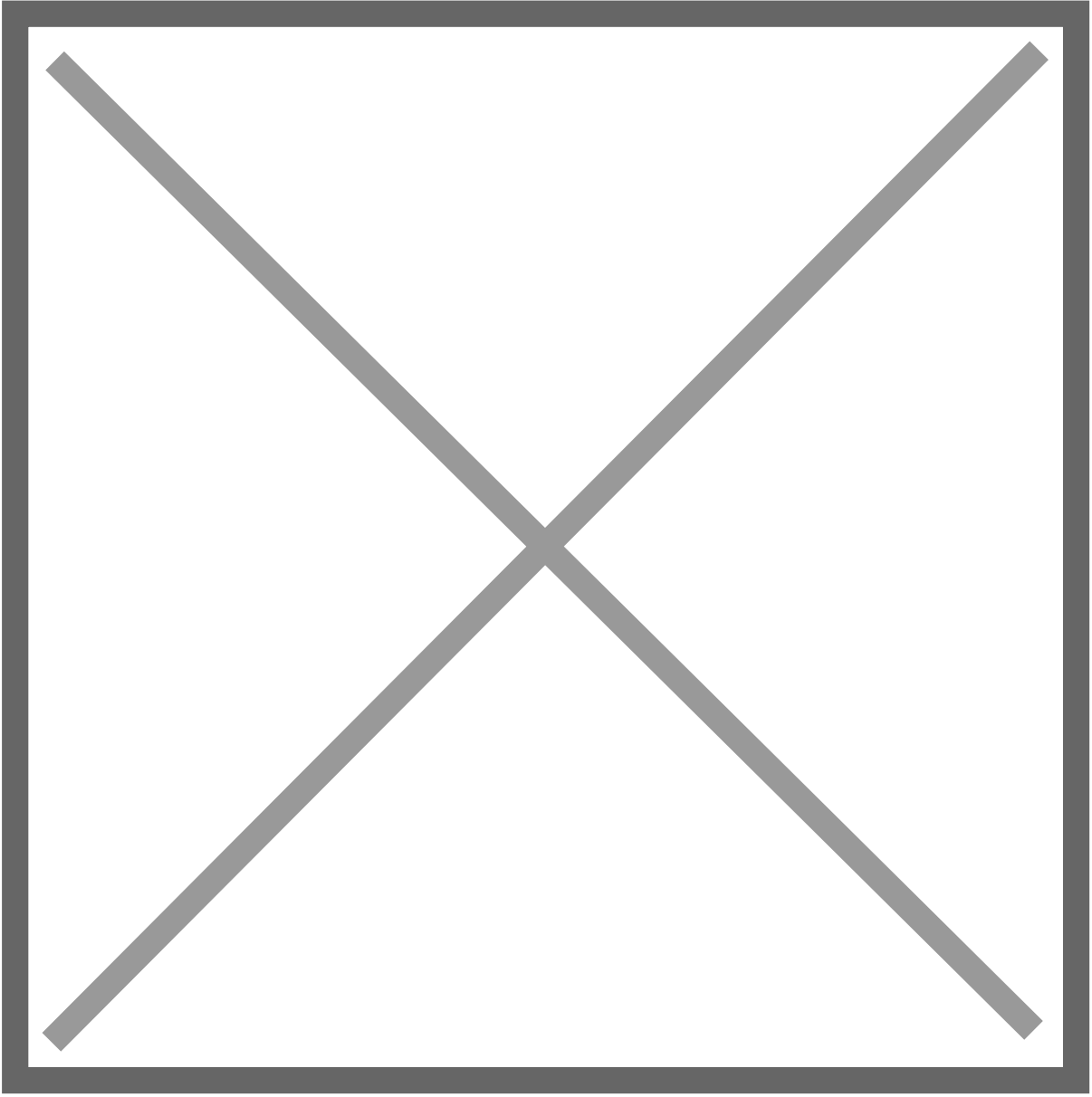


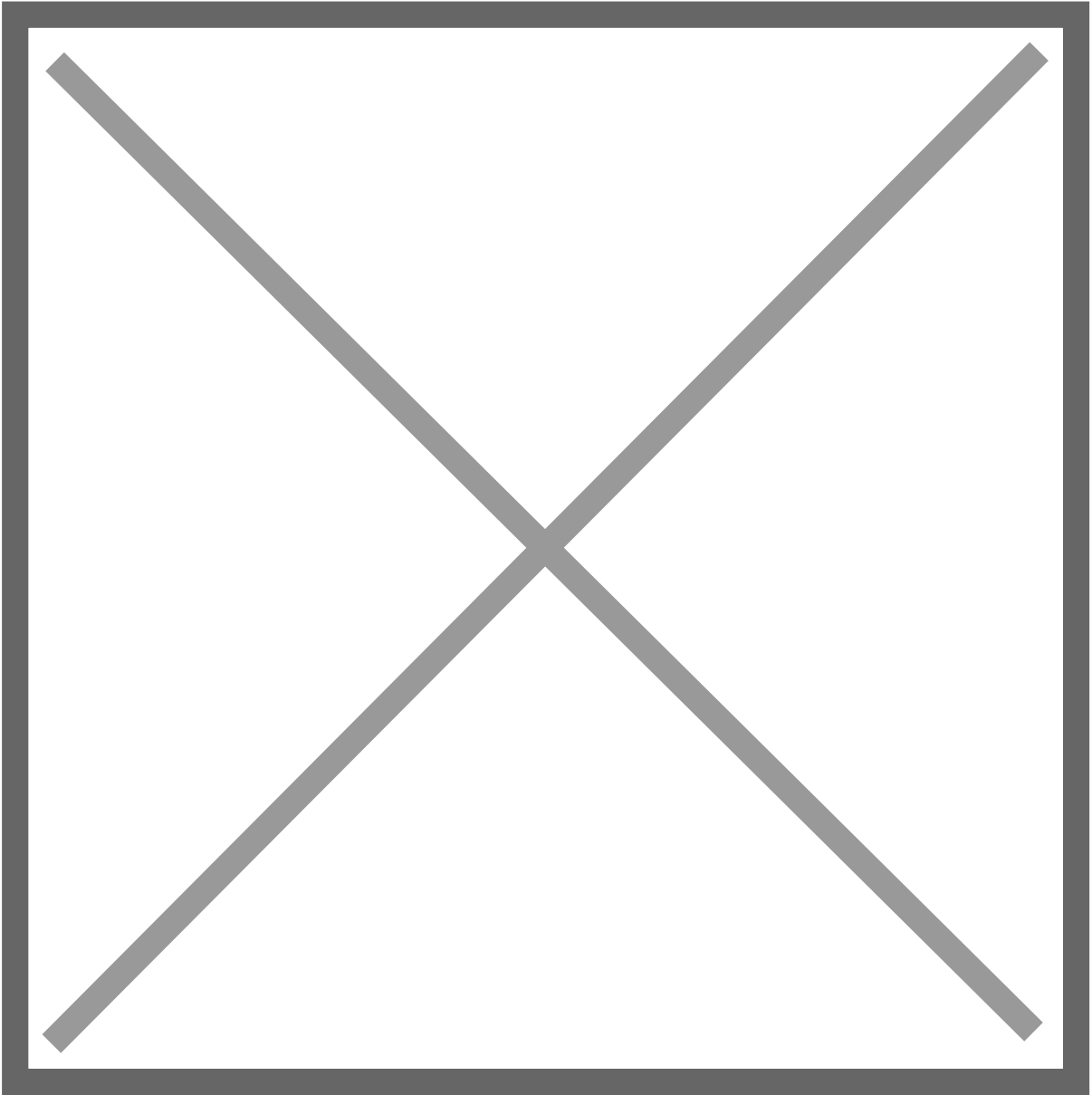
Utilities -> SNMP -> SNMP Trap Receivers



3. Maintenance window

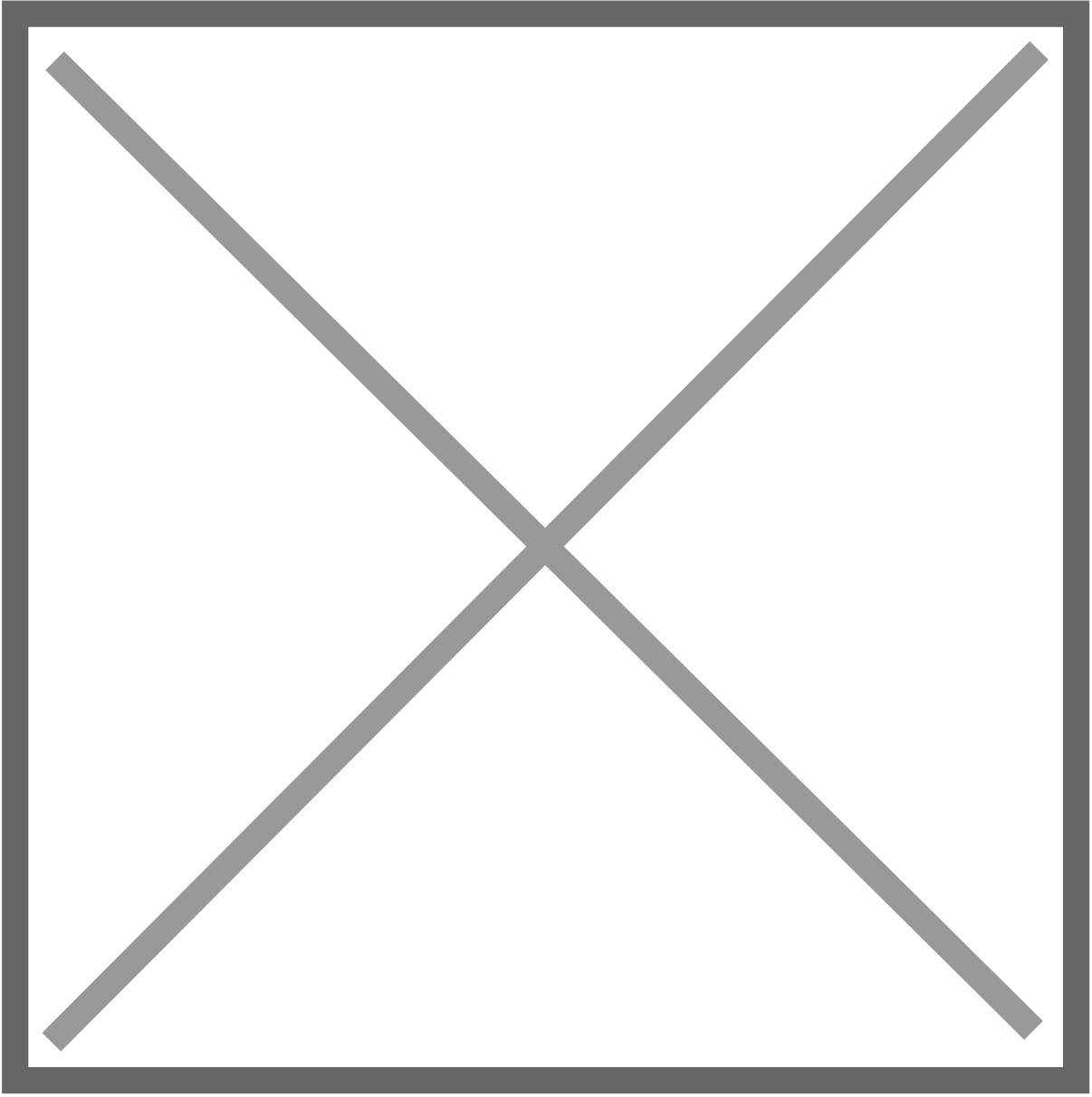
Create a backup file **Maintenance -> Server Data -> Backup** and download

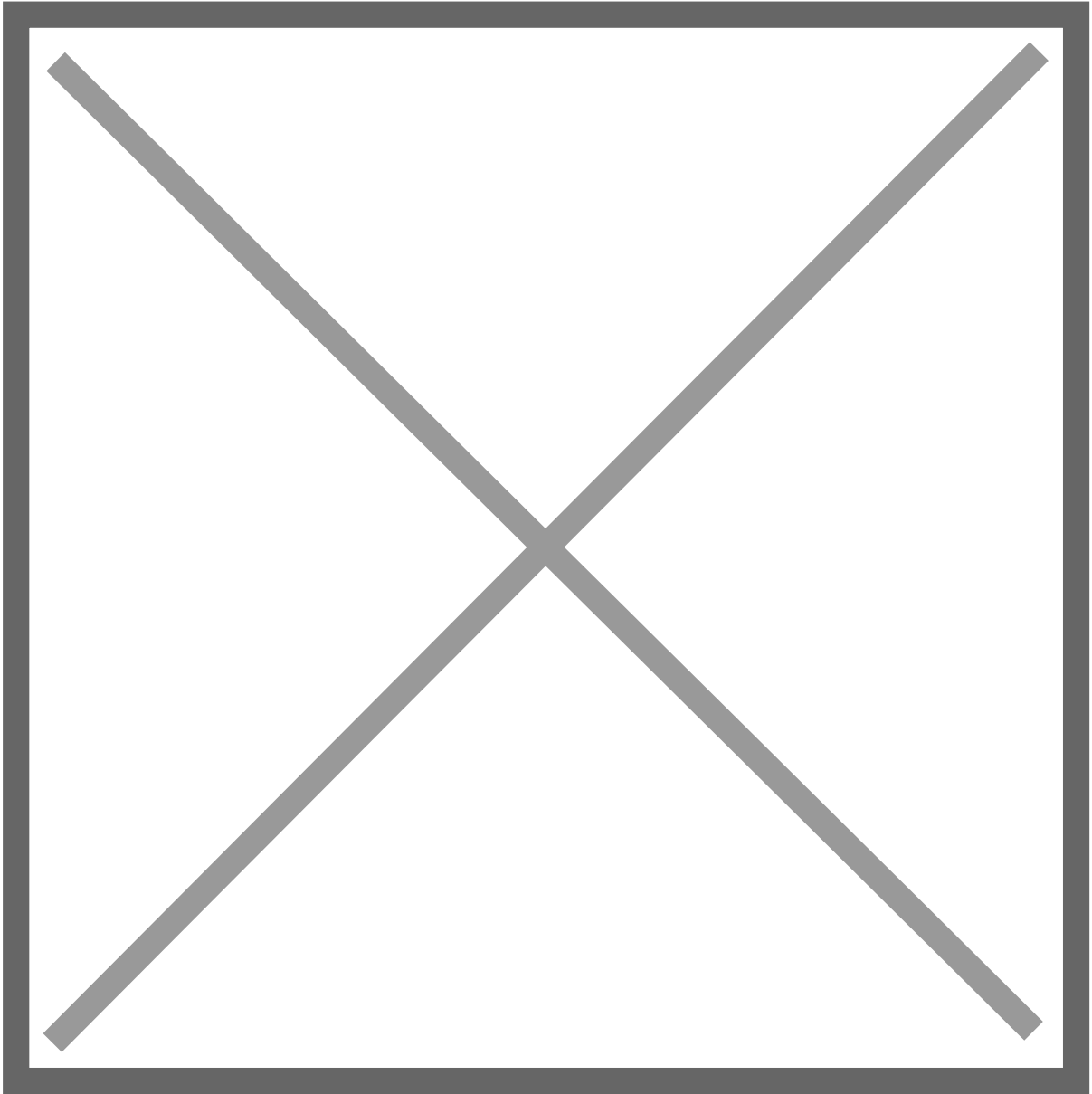




Shutdown production server

Restore backups





Last step is verifying all services and validate everything is up and running correctly to start testing applications. This concludes this entry.

Source: <https://whereismyvoicepacket.com/aes-upgrade/>

AES - Renew AES Cert using System Manager

AES certificate renewal if using SMGR certificate with CA Certificate and End Entity in place.

*This work will need a maintenance window for restarts of the AES.

1. Remove Certificate that is about to expire from AES.

Security | Certificate Management | Server Certificates Home | Help | Log

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
CA Trusted Certificates
Server Certificates

Server Certificates

Add Delete Export Import Renew View

Alias	Status	Issued To	Issued By	Expiration Date
aeservices	alert	sps-aes.euronetservices.net	System Manager CA	Mar 24, 2019

2. Restart AE Server

Maintenance | Service Controller Home | Help | Log

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

3. Go to the System Manager> Security> Certificates> Authority> Search End Entities

AVAYA
Aura® System Manager 7.0

Home Security * Adv

CA Functions

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

RA Functions

- Add End Entity
- End Entity Profiles
- Search End Entities**

Search End Entities

Search end entity with username

Search end entity with Certificate SN (hex)

Search end entities with status --

Search end entities with certificates expiring within Days

Made by PrimeKey Solutions AB, 2002–2014.

4. Verify the certificate for your AES by the CN and select *Edit End Entity*

Search end entities with certificates expiring within Days

Select	Username	CA	CN	OU	O (organization)	Status	
<input type="checkbox"/>	INBOUND_OUTBOUND_TLStmdefaultca	chi-smm.euronetservices.net			Avaya	Generated	View End Entity Edit End Entity View Certificates View History
<input type="checkbox"/>	avaya	tmdefaultca	chi-aes.euronetservices.net	SDP	AVAYA	Generated	View End Entity Edit End Entity View Certificates View History
<input type="checkbox"/>	avaya1	tmdefaultca	sps-aes.euronetservices.net	SDP	AVAYA	Generated	View End Entity Edit End Entity View Certificates View History

5. Change the status to New, enter the passwords and then Save

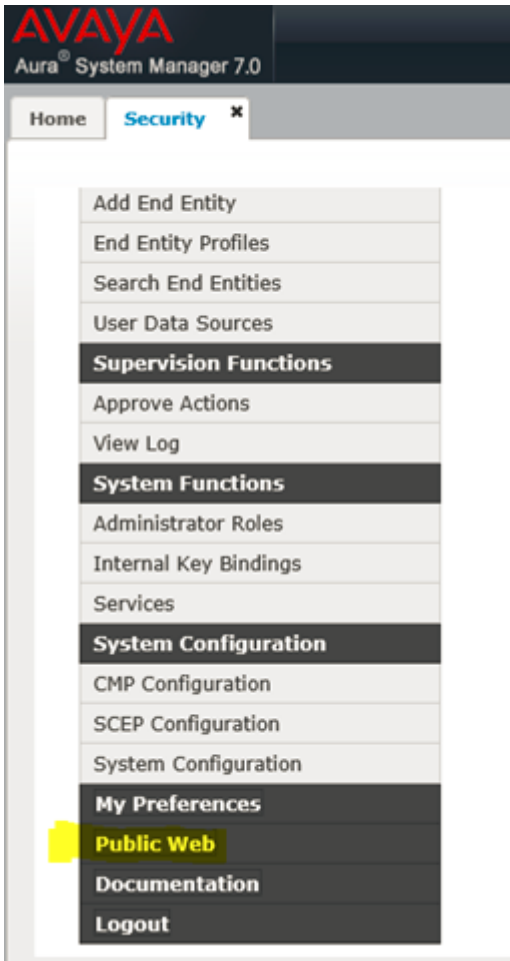
Edit End Entity

End Entity Profile INBOUND_OUTBOUND_TLS Req

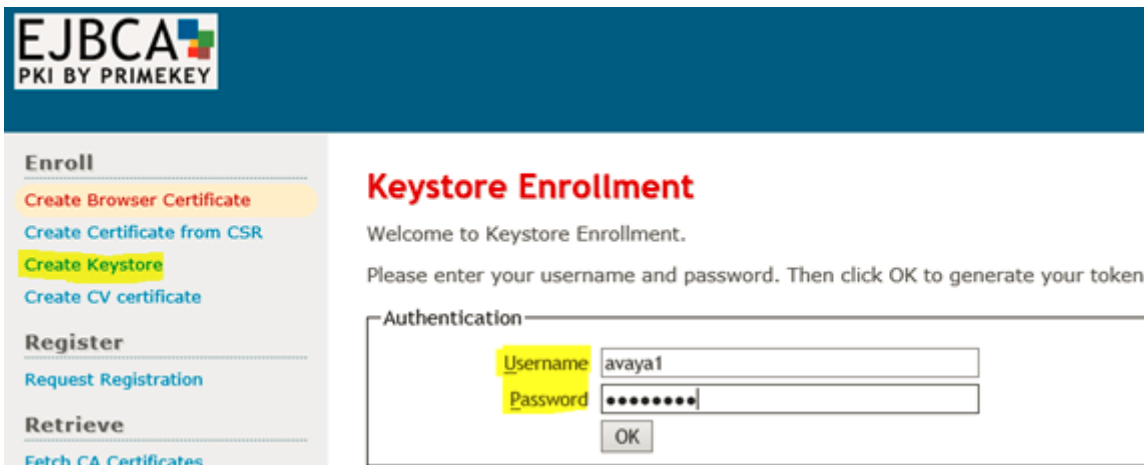
Status **New**

Username avaya1	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	<input type="checkbox"/>
Confirm Password	<input type="checkbox"/>
Maximum number of failed login attempts <input type="radio"/> <input type="text"/> <input checked="" type="radio"/> Unlimited	<input type="checkbox"/>
Remaining login attempts <input type="text"/> <input type="checkbox"/> Reset login attempts	<input type="checkbox"/>
E-mail address <input type="text"/> @ <input type="text"/>	<input type="checkbox"/>
Subject DN	
CN, Common name <input type="text" value="sps-aes.euronetservices.net"/>	<input checked="" type="checkbox"/>
CN, Common name <input type="text"/>	<input type="checkbox"/>
O, Organization <input type="text" value="AVAYA"/>	<input type="checkbox"/>
C, Country (ISO 3166) <input type="text" value="US"/>	<input type="checkbox"/>
OU, Organizational Unit <input type="text" value="SDP"/>	<input type="checkbox"/>
L, Locality <input type="text"/>	<input type="checkbox"/>
ST, State or Province <input type="text"/>	<input type="checkbox"/>
Other subject attributes	
Subject Alternative Name	
DNS Name <input type="text"/>	<input type="checkbox"/>
DNS Name <input type="text"/>	<input type="checkbox"/>
IP Address <input type="text"/>	<input type="checkbox"/>
Main certificate data	
Certificate Profile <input type="text" value="ID_CLIENT_SERVER"/>	<input checked="" type="checkbox"/>
CA <input type="text" value="tmdefaultca"/>	<input checked="" type="checkbox"/>
Token <input type="text" value="P12 file"/>	<input checked="" type="checkbox"/>

6. Scroll to the bottom of the page and select *Public Web*.



7. Select Create Keystore and then enter the username and password from the End Entity and select OK.



8. Select 2048 bits and then Select Enroll.

Enroll

Create Browser Certificate

Create Certificate from CSR

Create Keystore

Create CV certificate

Register

Request Registration

Retrieve

Fetch CA Certificates

Fetch CA CRLs

List User's Certificates

Fetch User's Latest Certificate

Inspect

EJBCA Token Certificate Enrollment

Welcome to keystore enrollment.

If you want to, you can manually install the CA certificate(s) in your browser, other automatically when your certificate is retrieved.

Install CA certificates:

[Certificate chain](#)

Please choose a key length, then click OK to fetch your certificate.

Options

Leave values as default if unsure.

Key length: 2048 bits

Enroll

Once you click enroll the certificate will be downloaded (depending on your browser you can select where it is saved or find it in downloads from windows explorer).

Next Import the new AE Services server certificate into the AES

1. Using the AE Services Management Console navigate to "Security > Certificate Management > Server Certificates"
2. Click on the Import button and upload the new AE Services server certificate you created above (this will be the .p12 file). Select an alias (server) from the drop down menu
3. Click the "Apply" button.

- > AE Services
- > Communication Manager Interface
- > High Availability
- > Licensing
- > Maintenance
- > Networking
- ▼ Security
- > Account Management
- > Audit
- ▼ Certificate Management
- CA Trusted Certificates
- ▣ Server Certificates

Server Certificates

Add Delete Export Import Renew View

Alias	Status	Issued To	Issued By

4. Select Choose file, Establish Chain of Trust and Certificate Alias.

Security | Certificate Management | Server Certificates

- > AE Services
- > Communication Manager Interface
- > High Availability
- > Licensing
- > Maintenance
- > Networking
- ▼ Security
- > Account Management
- > Audit
- ▼ Certificate Management
- CA Trusted Certificates
- ▣ Server Certificates

Server Certificate Import

File Path*: Choose file Dave.p12

Establish Chain of Trust

Certificate Alias* server

Apply Close

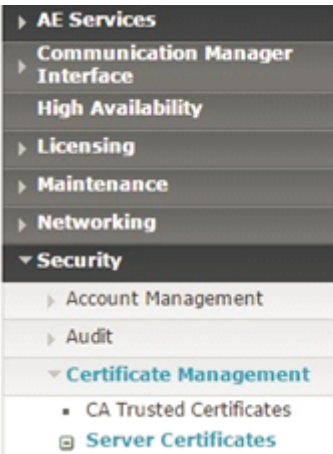
5. Enter the PKCS12 password (from the End Entity) and select Apply and then on the next page Apply again.



Server Certificate Import Continue

PKCS12 Password*

Apply Close



Server Certificate Import

Warning! You are importing the server certificate.
The new server certificate can only take effect when the AE services restarts.

⚠ Please use the Maintenance -> Service Controller page to restart AE Server.

Apply Cancel

6. Restart the Linux server.

Maintenance | Service Controller

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server