Avaya - AES

- Administration, upgrades and maintenances
  - 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
- Troubleshooting
  - AES - TSAPI logging
  - AES - useful commands
  - Retrieve CTI desktop log from agent machine
- Lab
  - Avaya AES - TSAPI CTI link basic testing

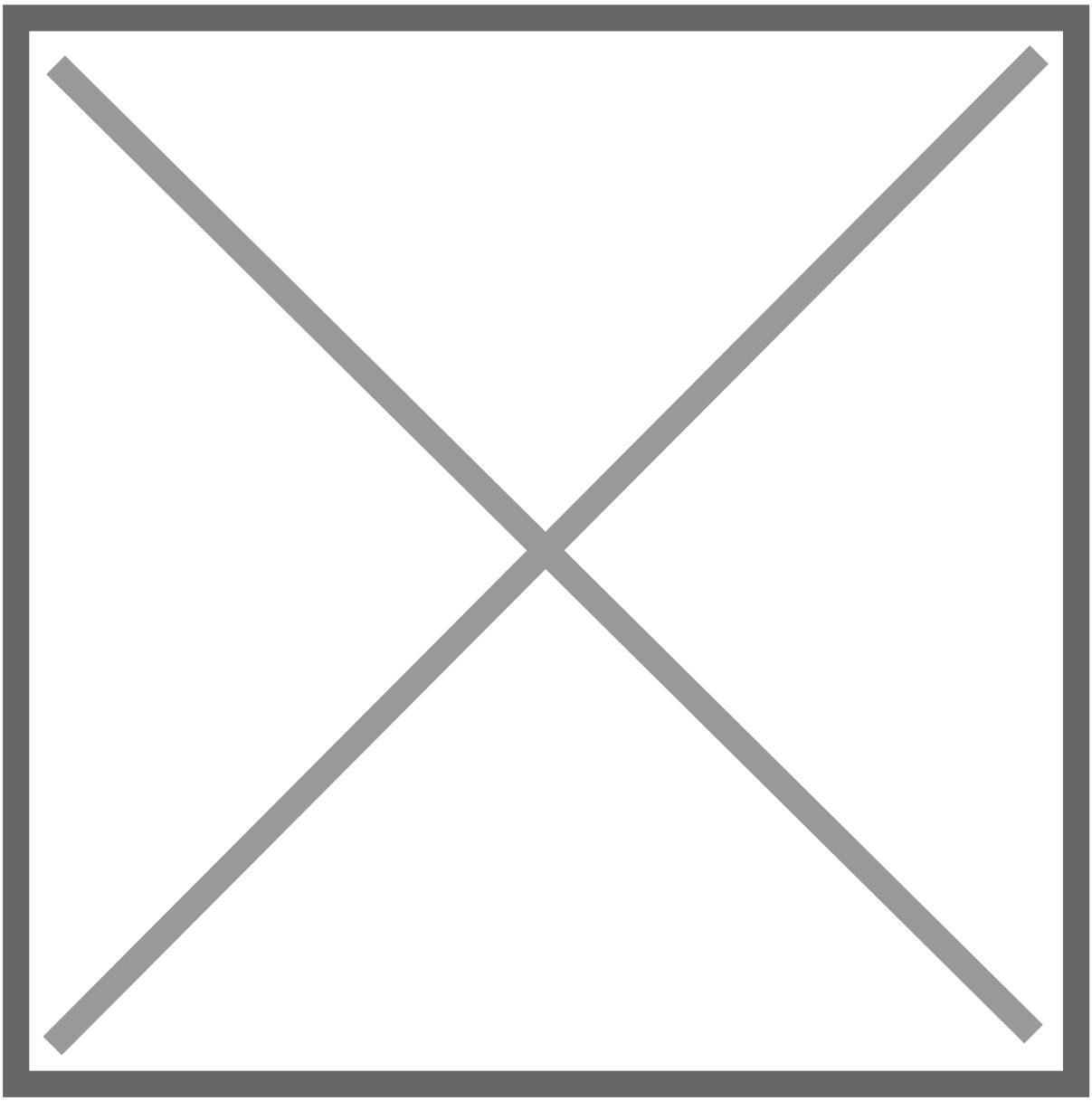
Administration, upgrades and maintenances

Everything related to Avaya AES Installations, upgrades and implementations

AES – Testing SMS Service

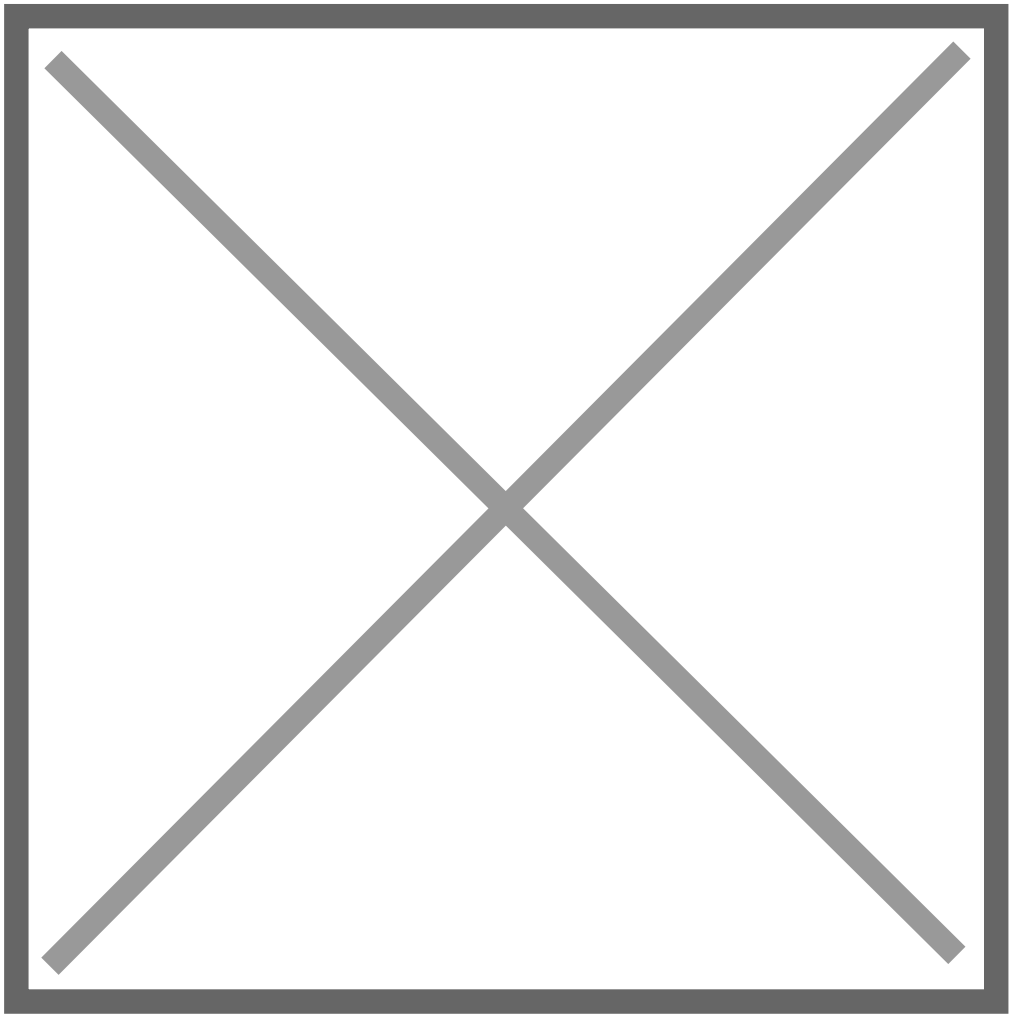
System Management Service (SMS) is an interesting service that all Application Enablement Servers run by default with no need for licensing, it exposes management features of Communication Manager. This service enables its clients to display, list, add, change and remove specific managed objects on Communication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

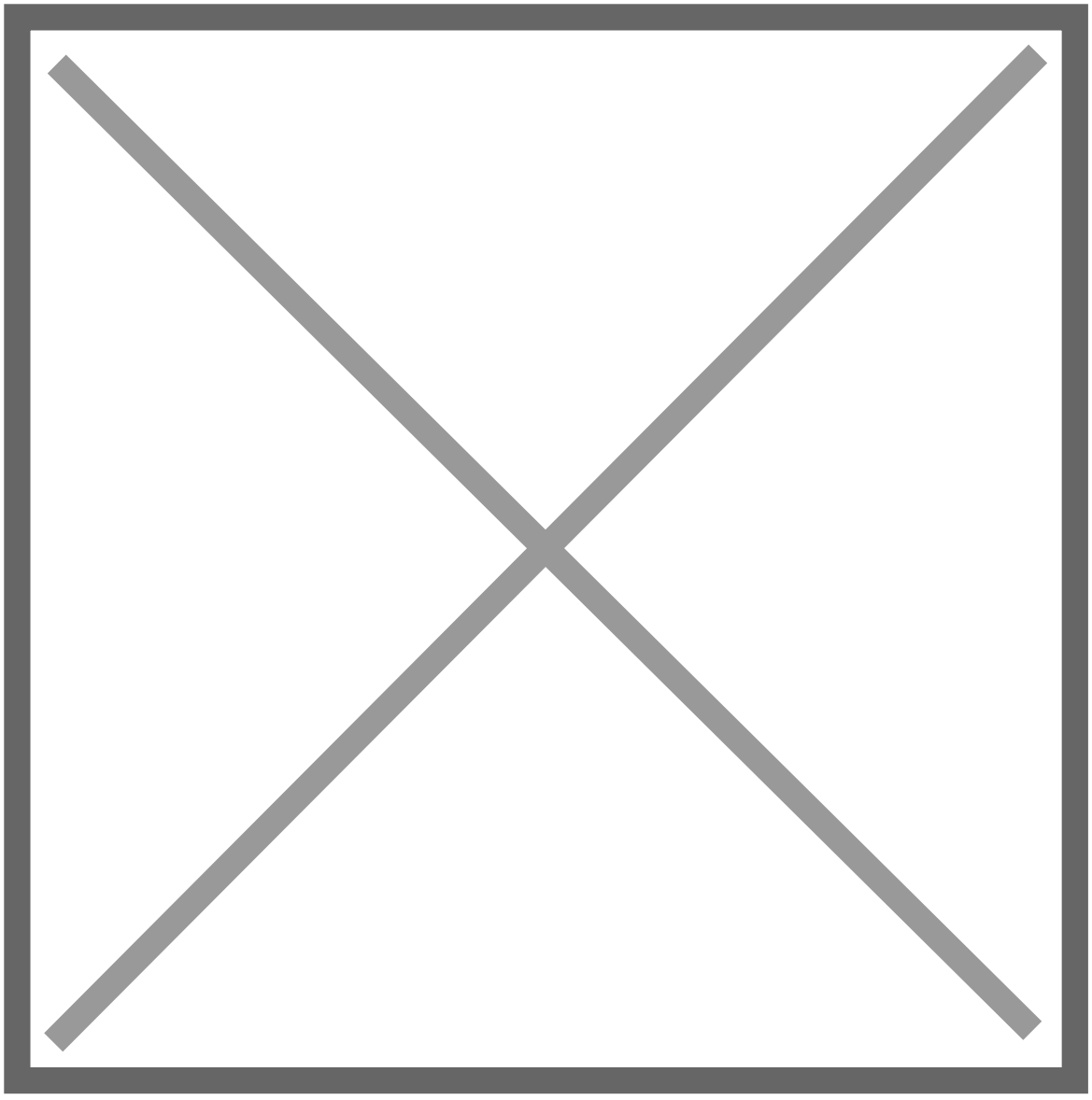
3) Press “Submit Request” Button

4) Repeat step 2) but setting Operation to “release”

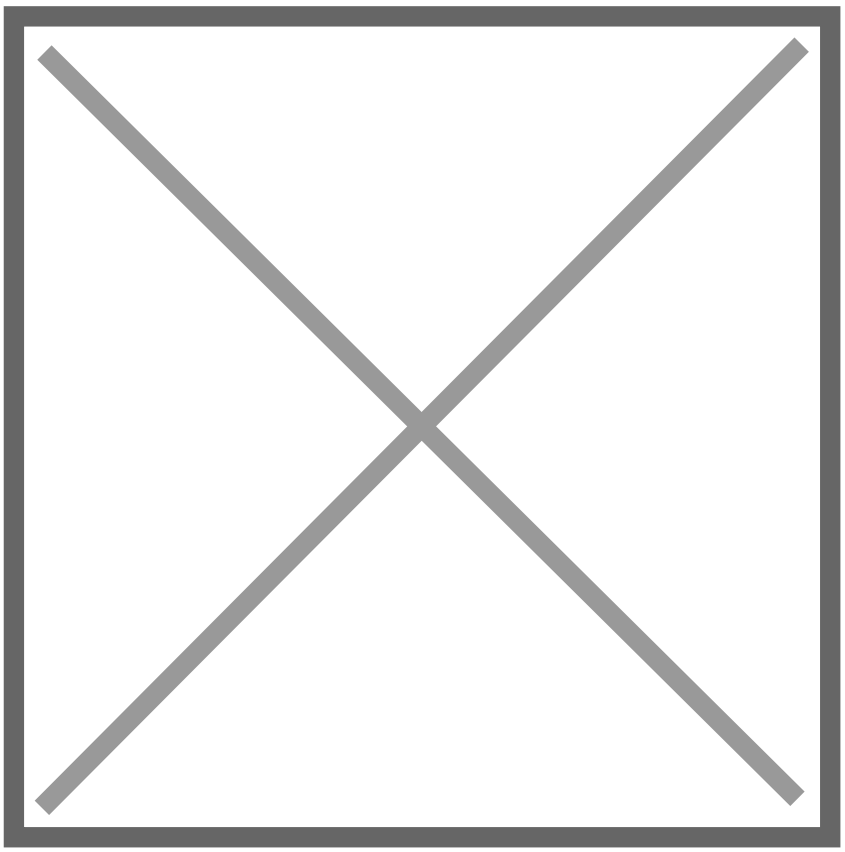
5) Press “Submit Request” Button

6) Press “Release” Button to disconnect session

Here is a screenshot for running the process described above:

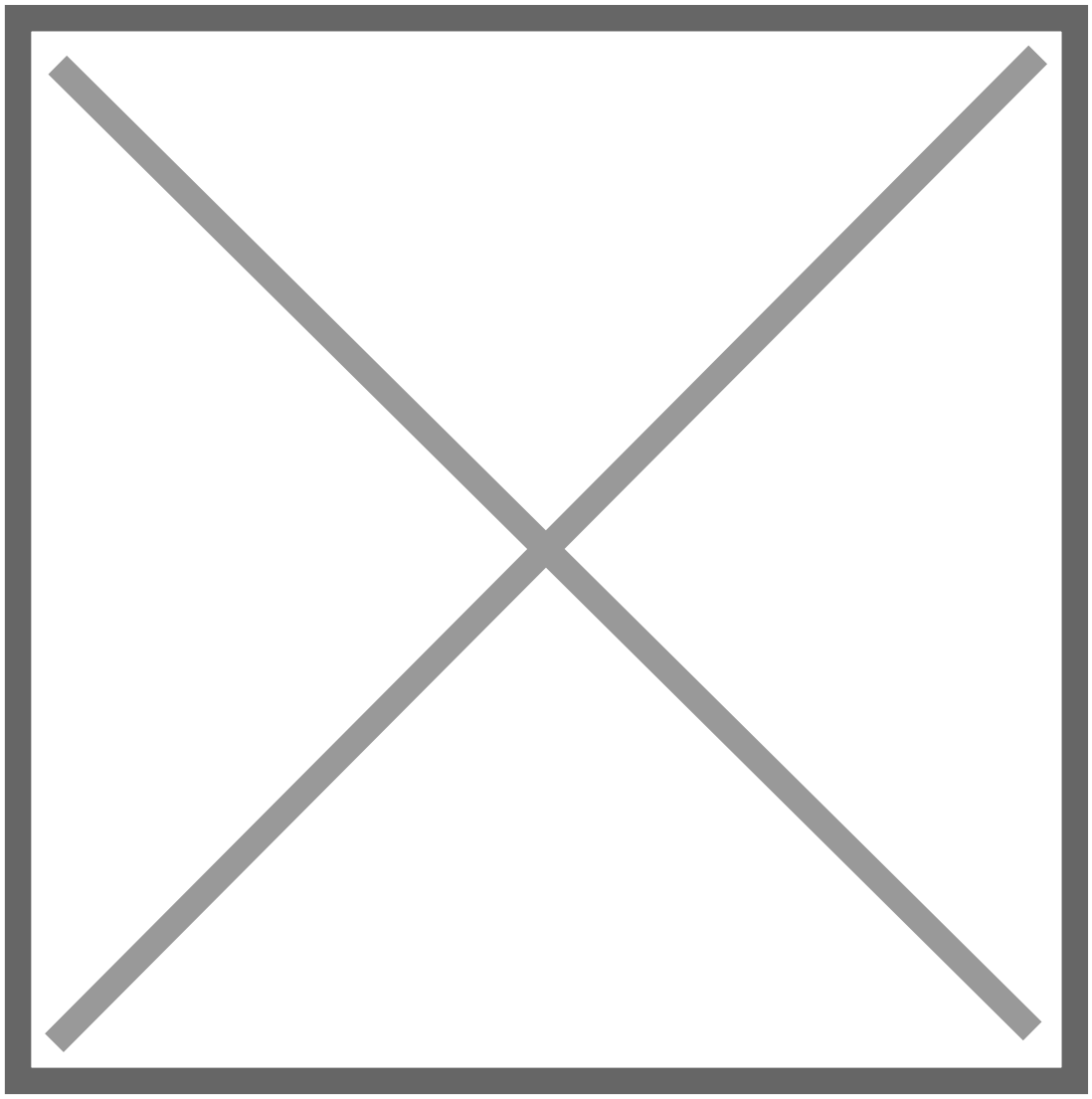


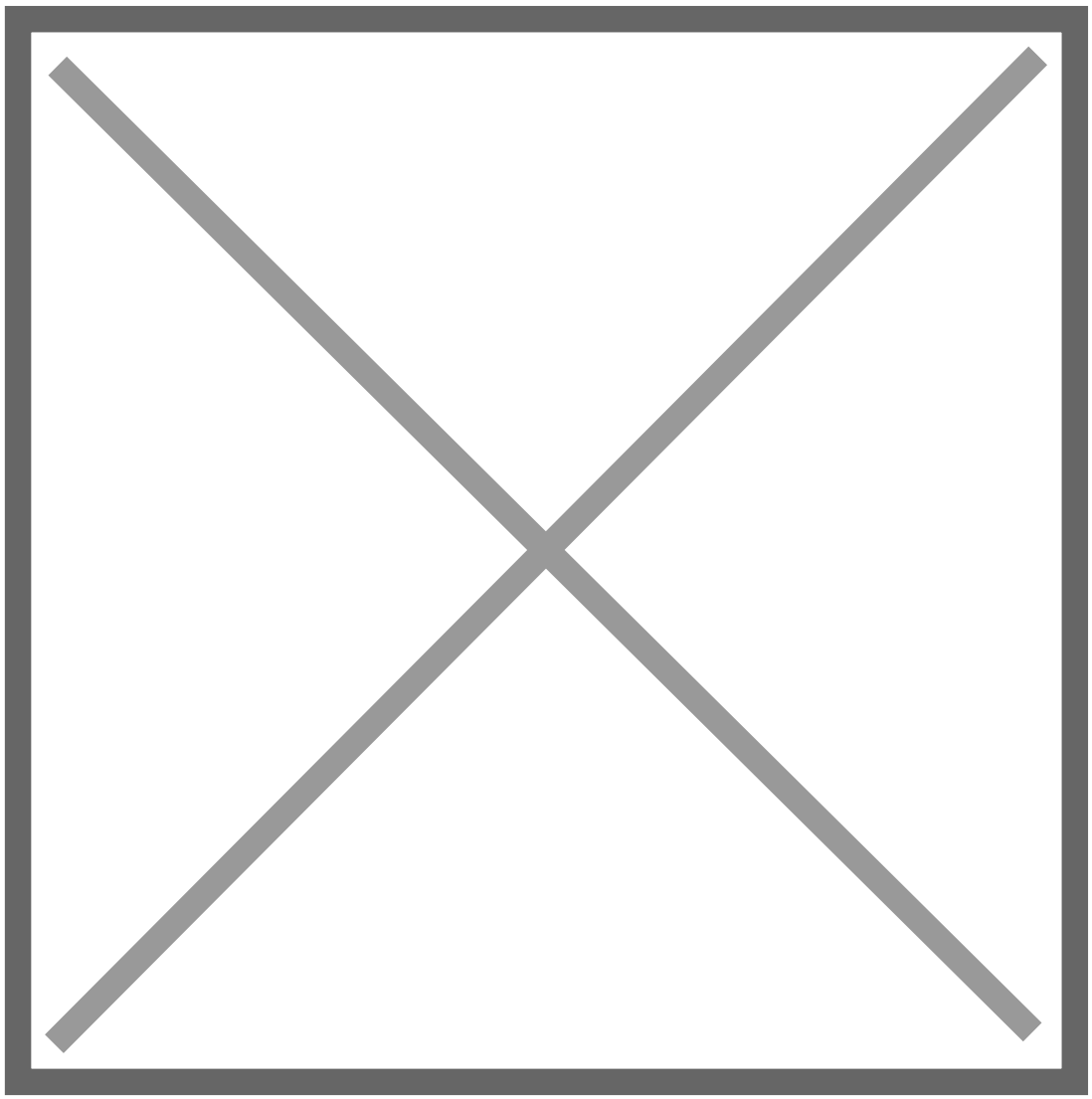
PBX commands after using the web page

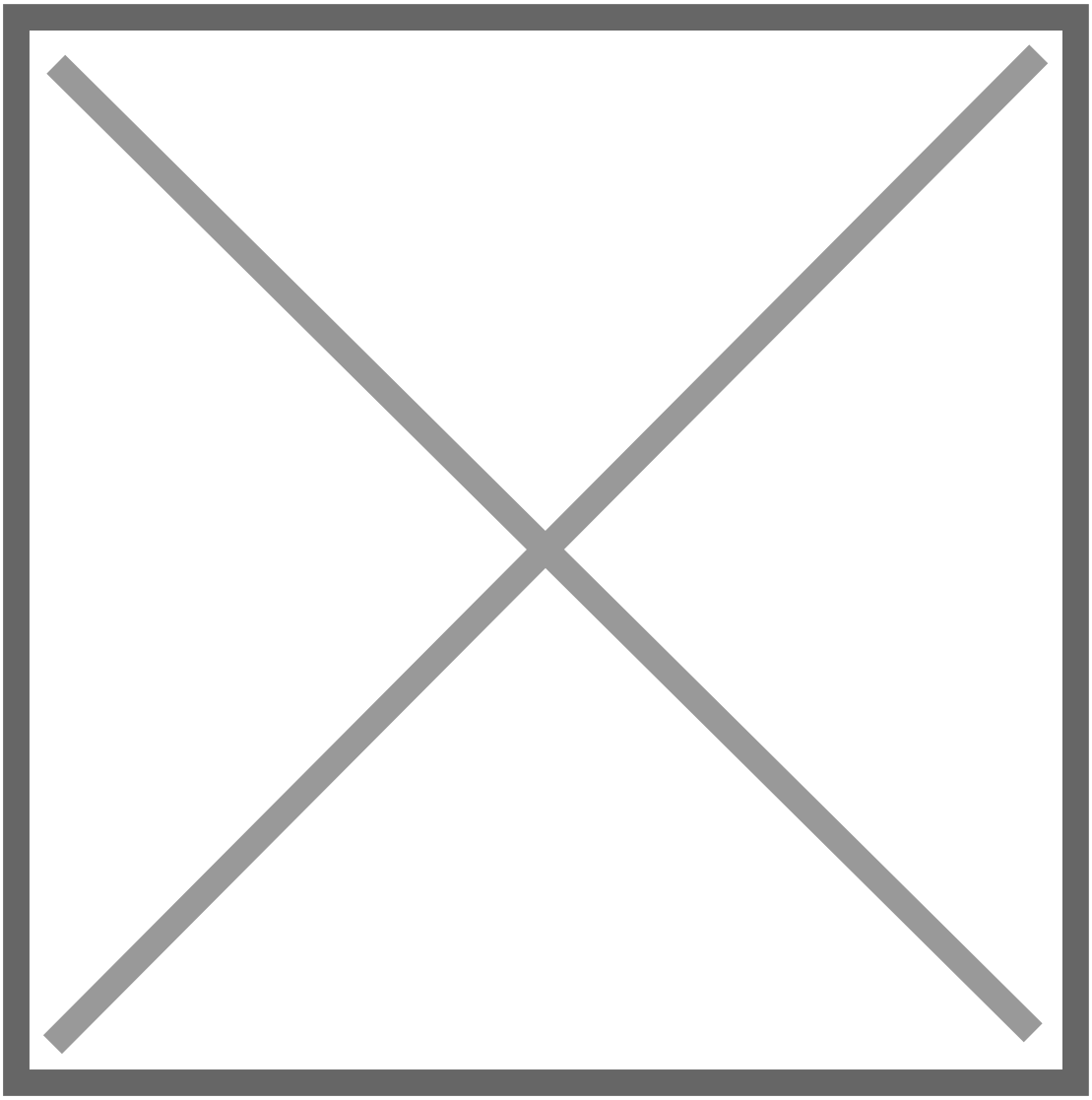


For more information visit Avaya devconnect program:

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







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

Administration, upgrades and maintenances

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***)

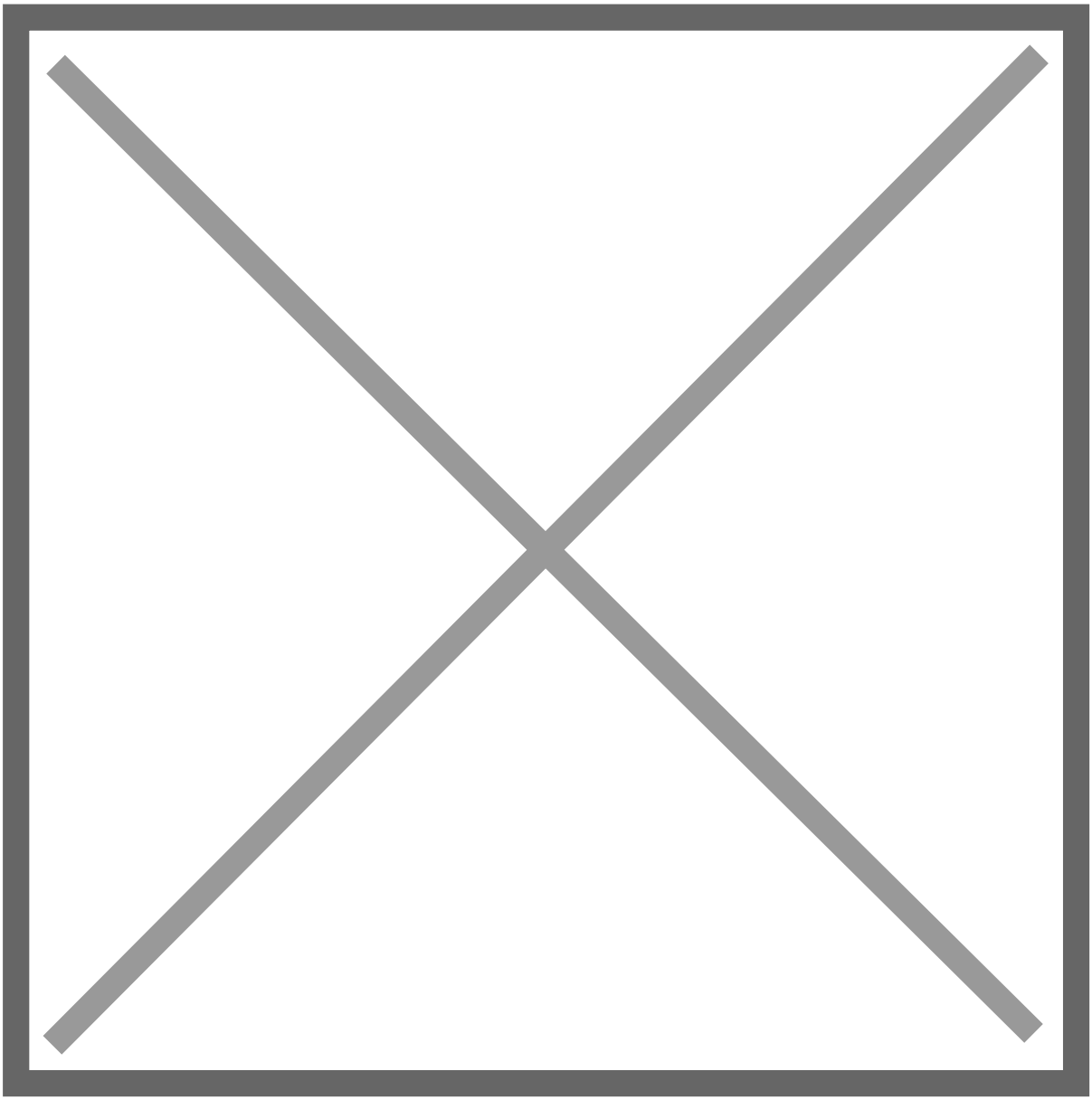
```
[root@denusvm-labaes1 tmp]# swversion
********************************************************************************
Application Enablement Services
********************************************************************************
Version: 8.1.3.4.0.2-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE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

Administration, upgrades and maintenances

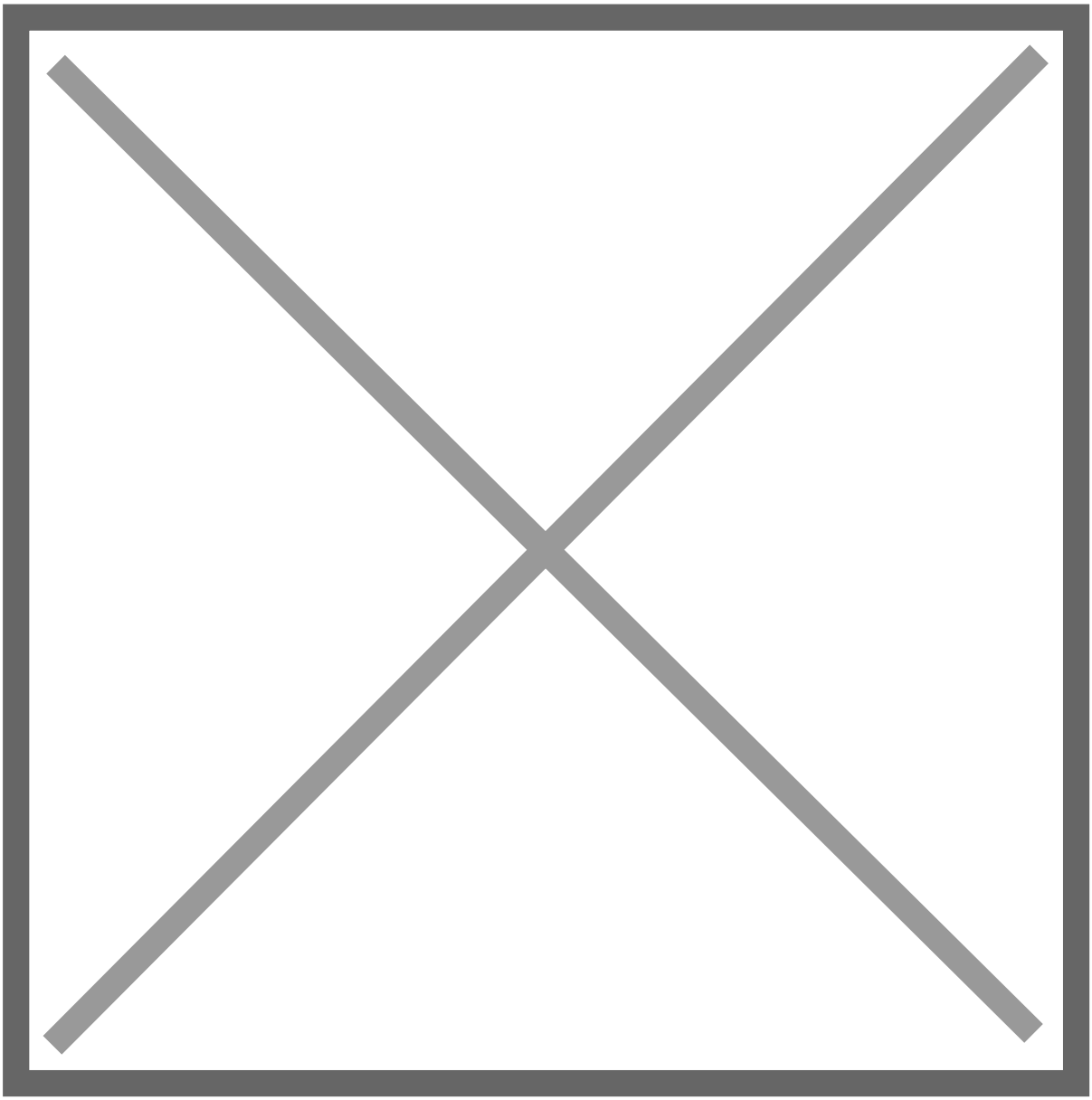
AES - TSAPI CTI link integration

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.

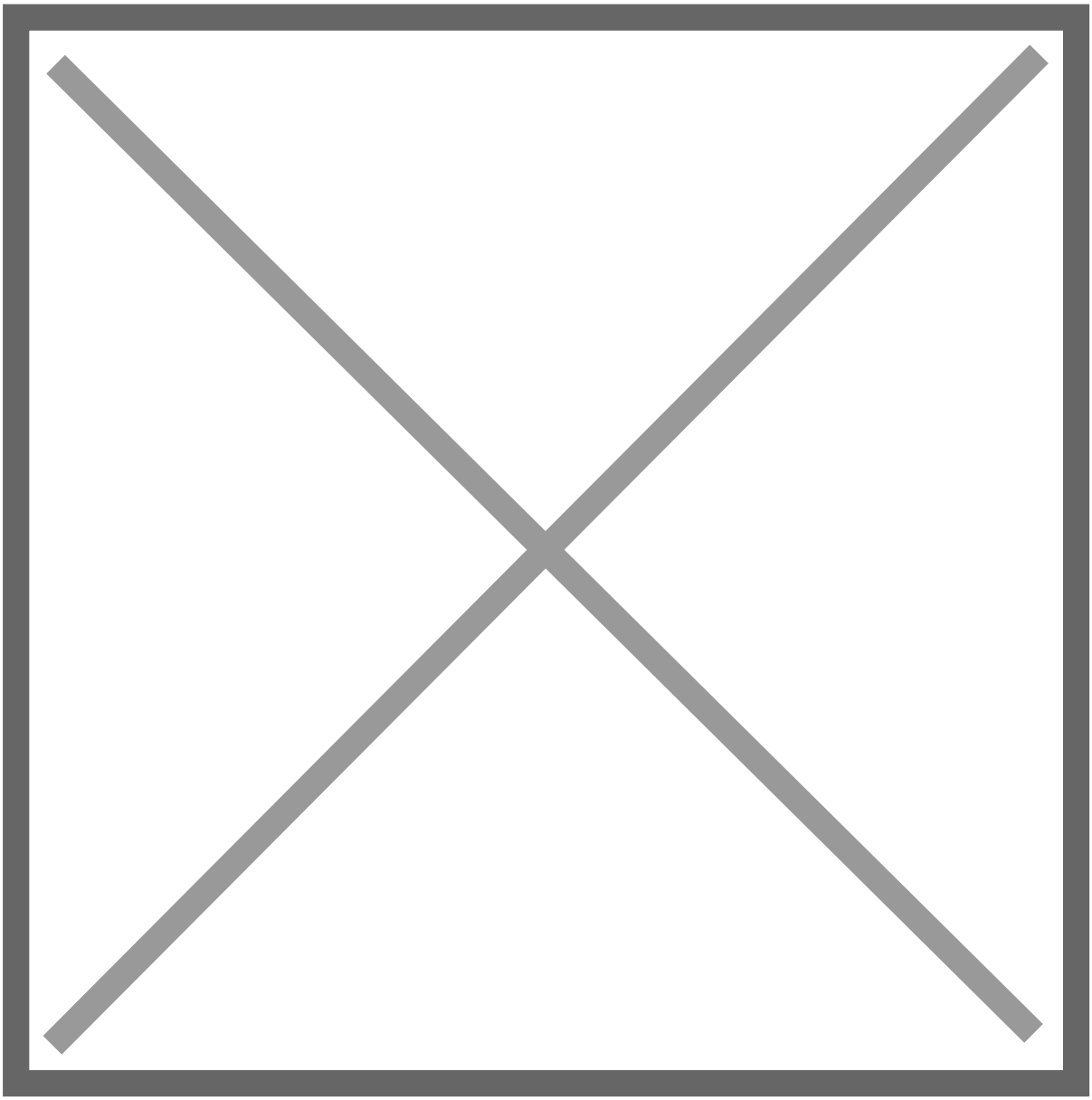
Let’s begin with ***change ip-services*** Set up in the first page enabling AESVCS running on port 8765 on Communication Manager:

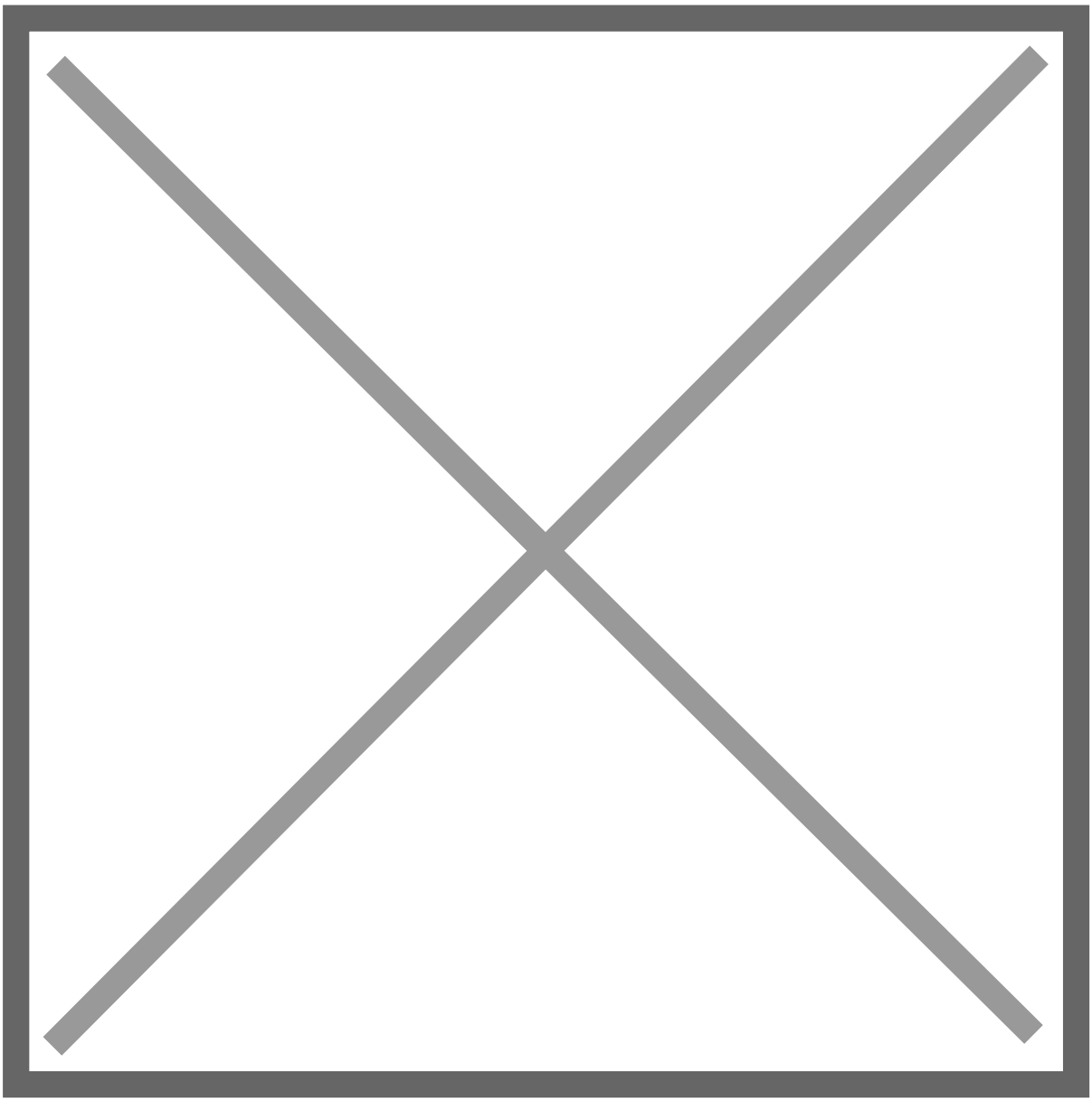


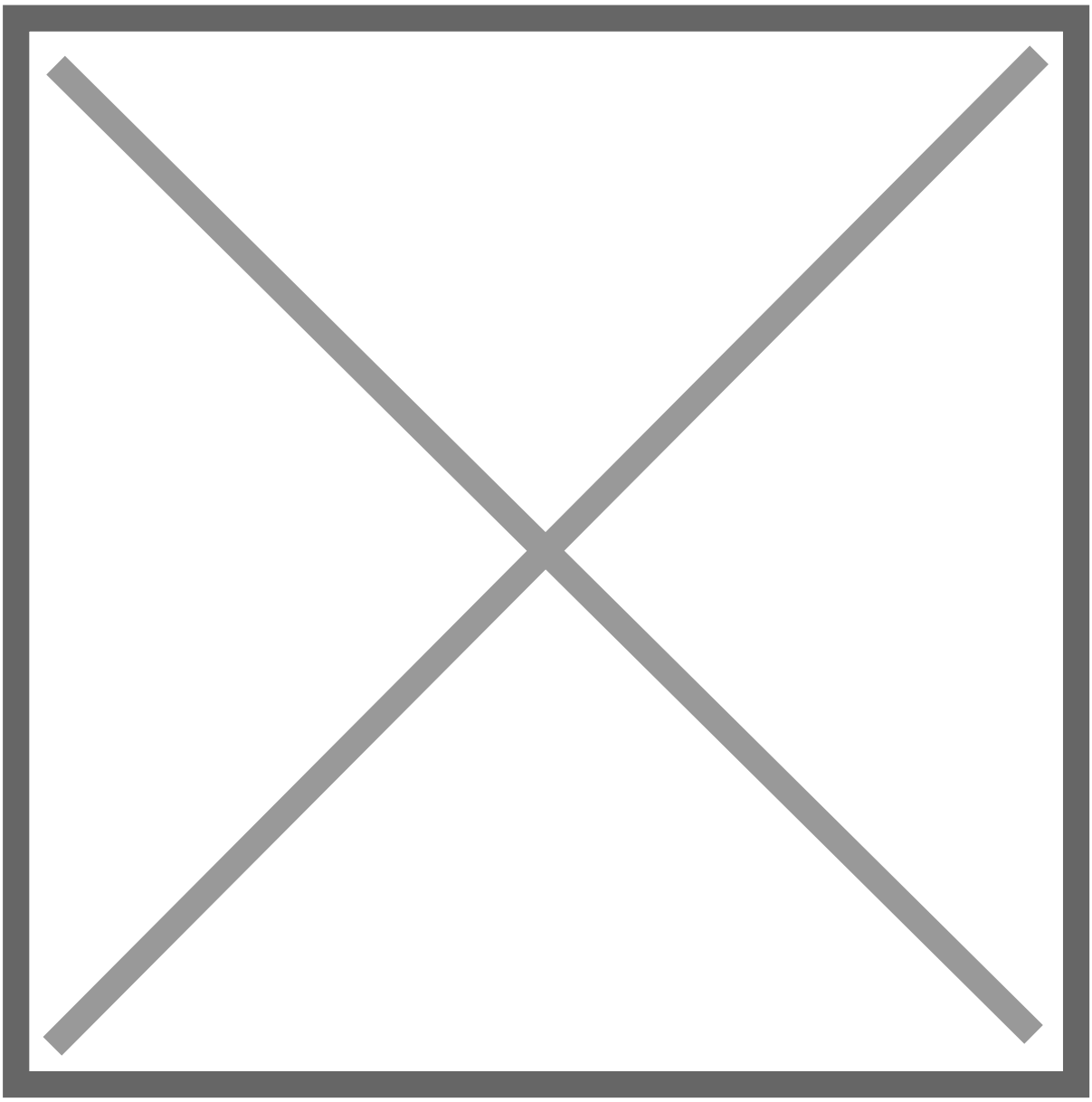
On the third page set up the hostname of the AE Server and password:



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

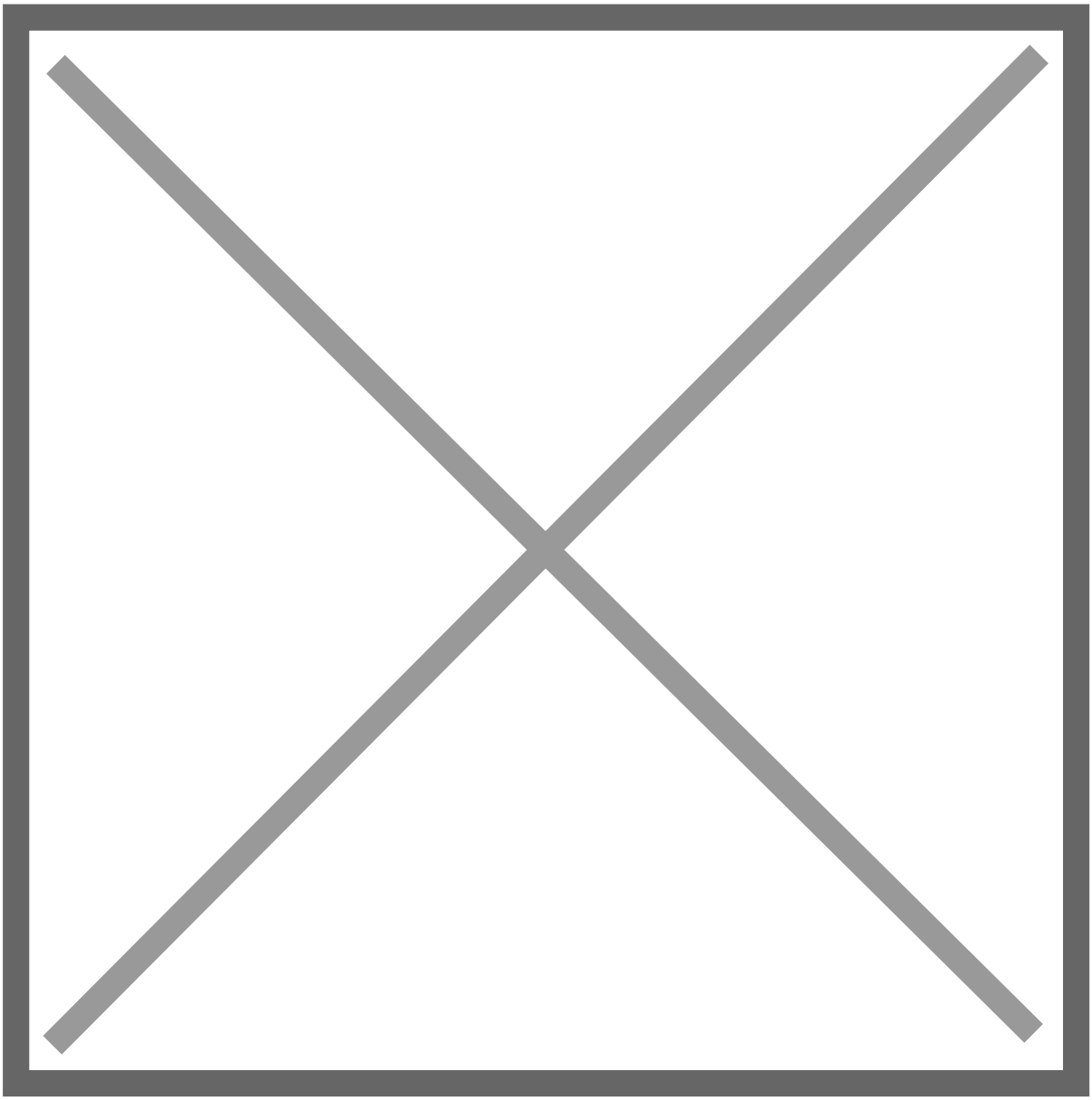




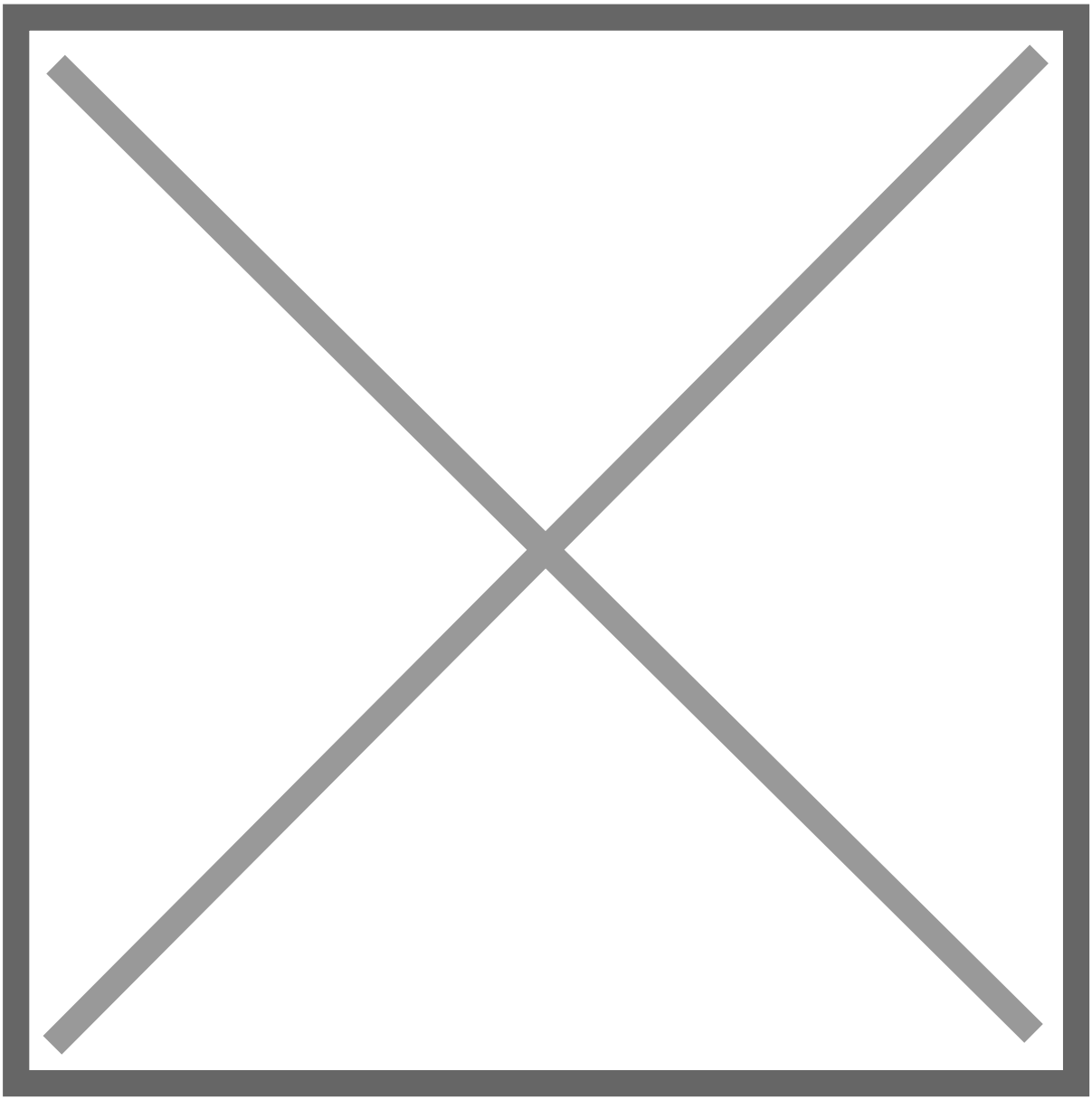


Now it’s time to make the changes in the AE Server:

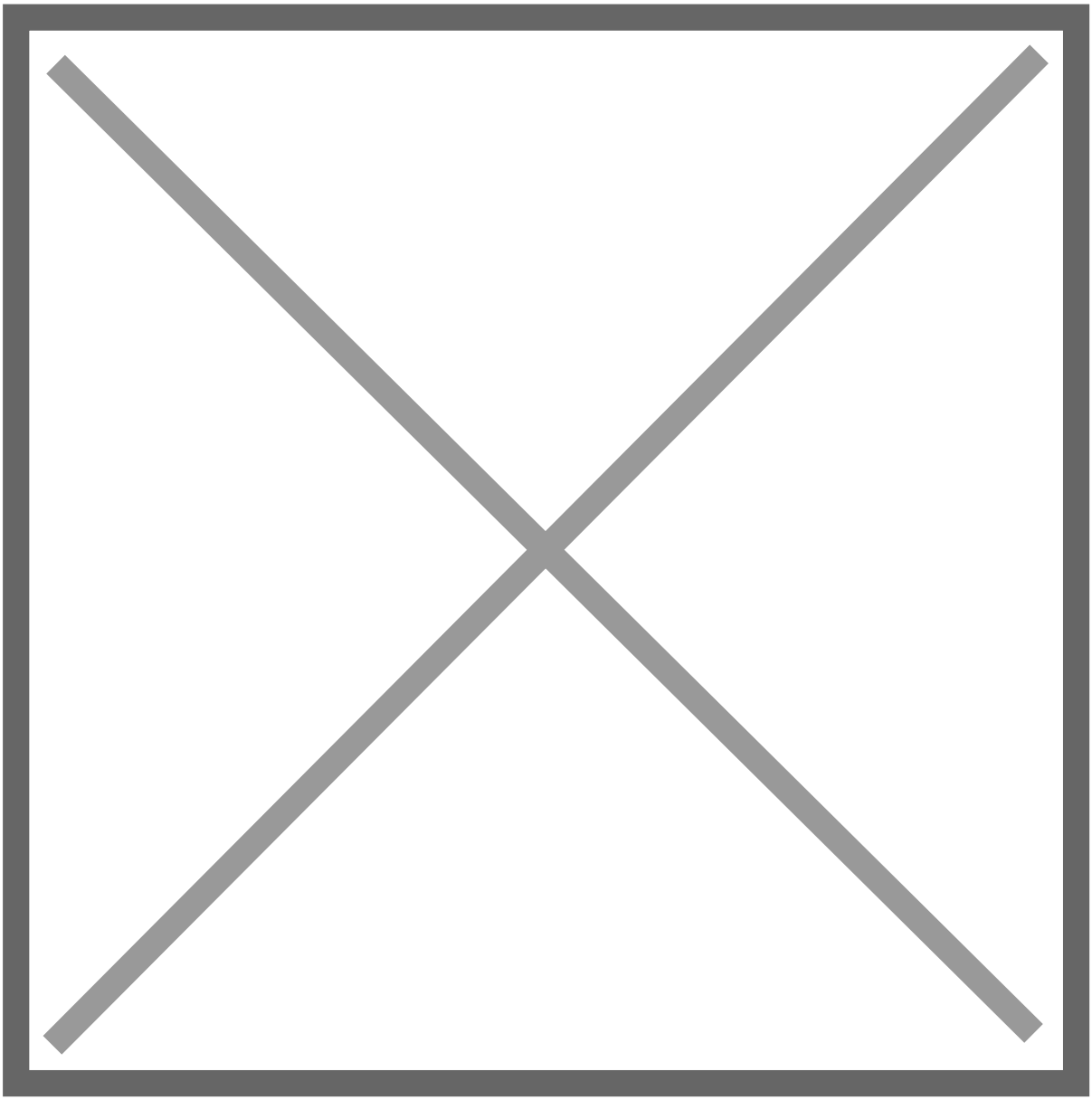
First, log in into the AES using the web portal and navigate to **Communication Manager Interface -> Switch Connections -> Add Connection**:



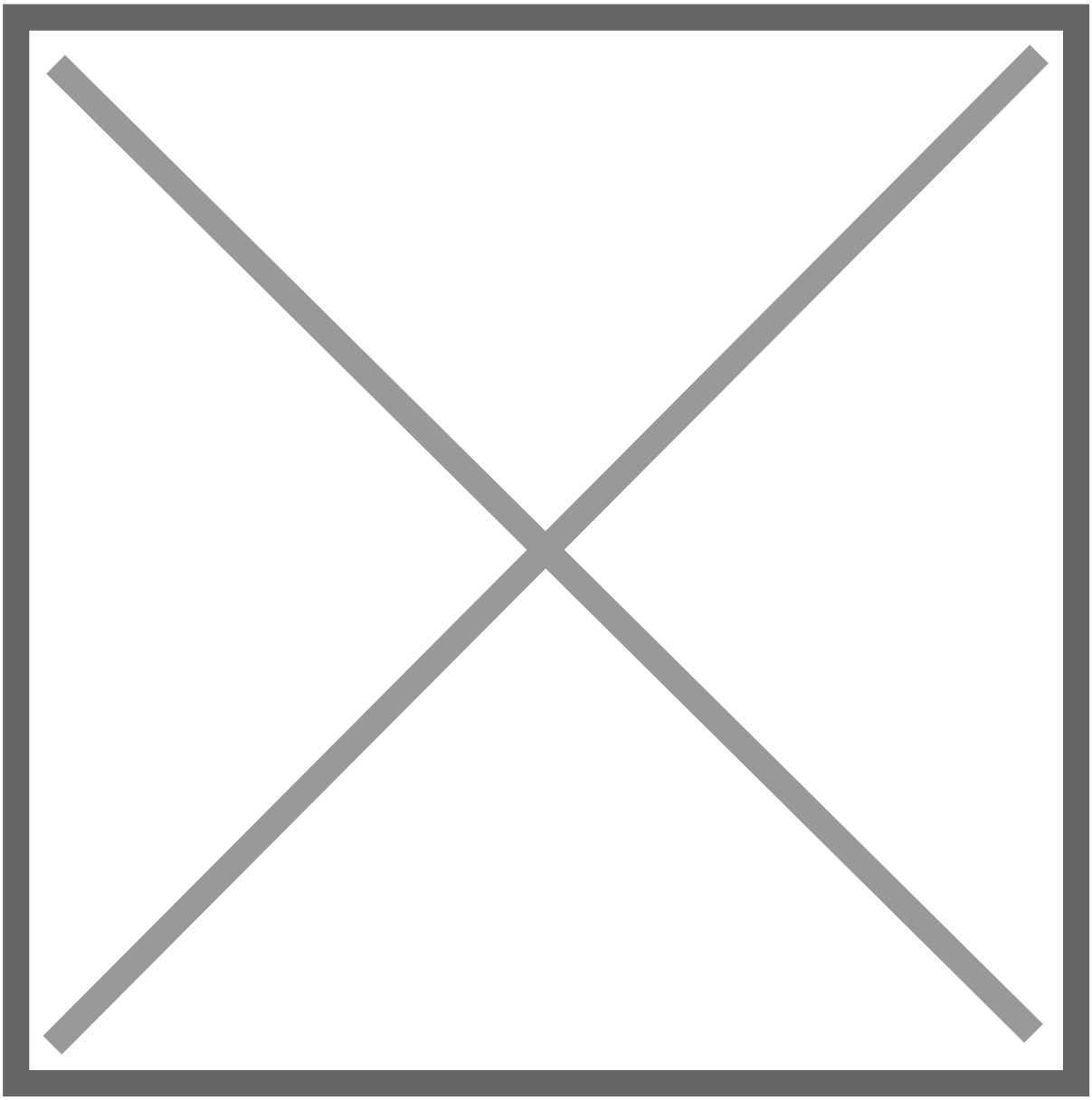
In the next screen type the same password set in the ***change ip-services*** command in the PBX, enable only the *Processor Ethernet* option, leave all other settings by default blank, but make sure the TLS is disabled.



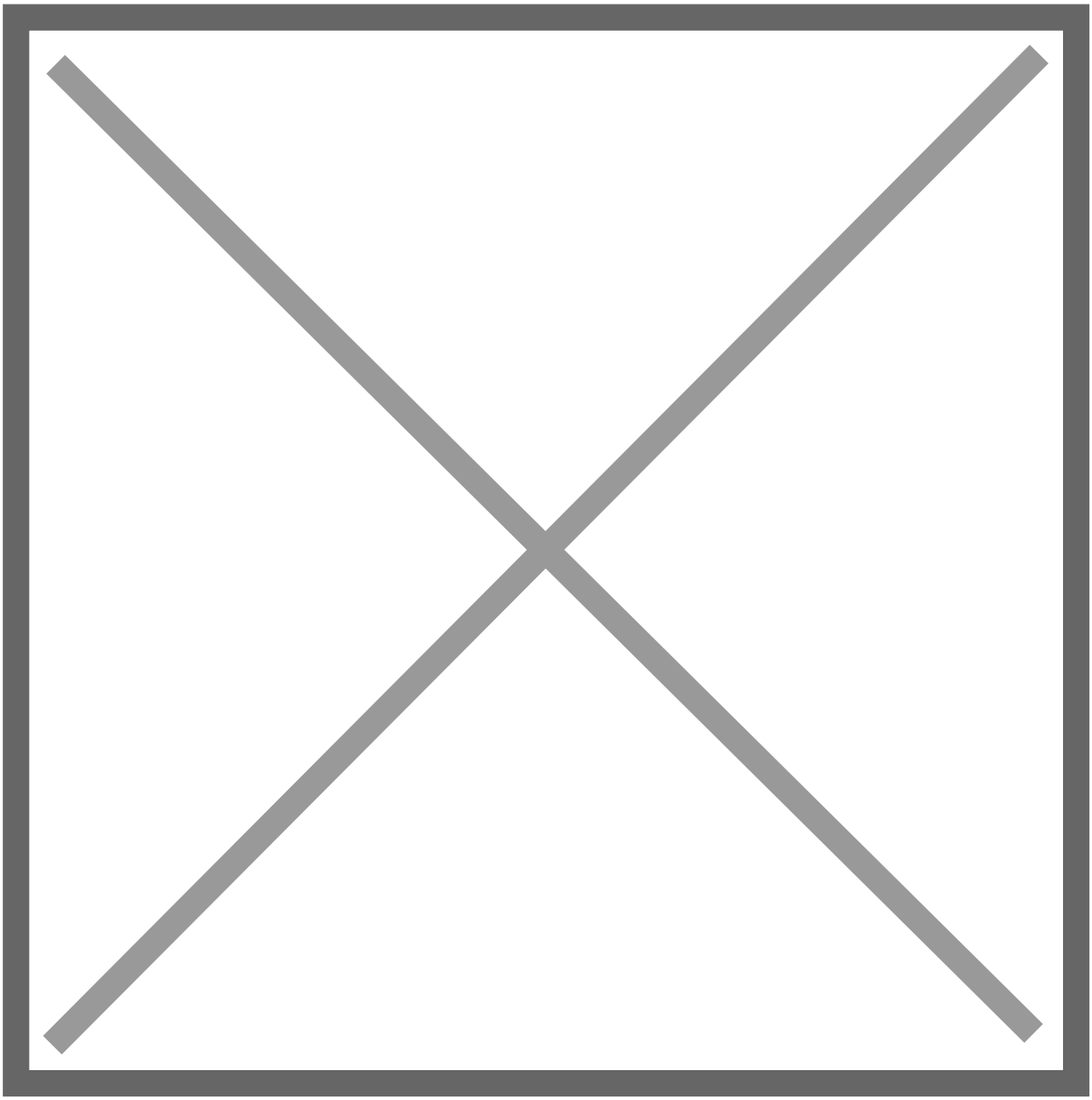
Once the new connection appears, select the connection, and select *Edit PE/CLAN IPs*:



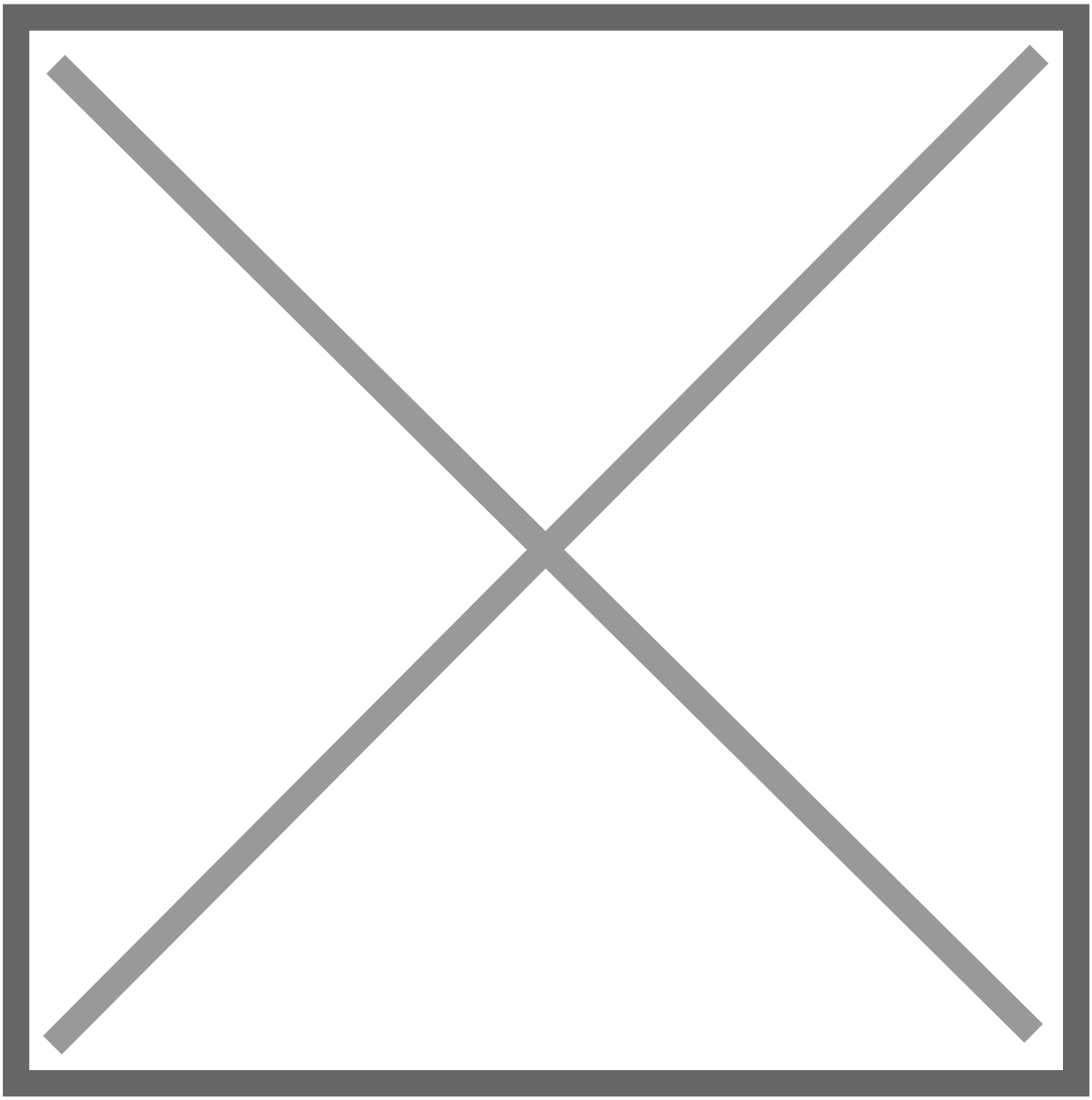
Type the IP address for the Processor Ethernet and click on *Add/Edit Name or IP*:



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

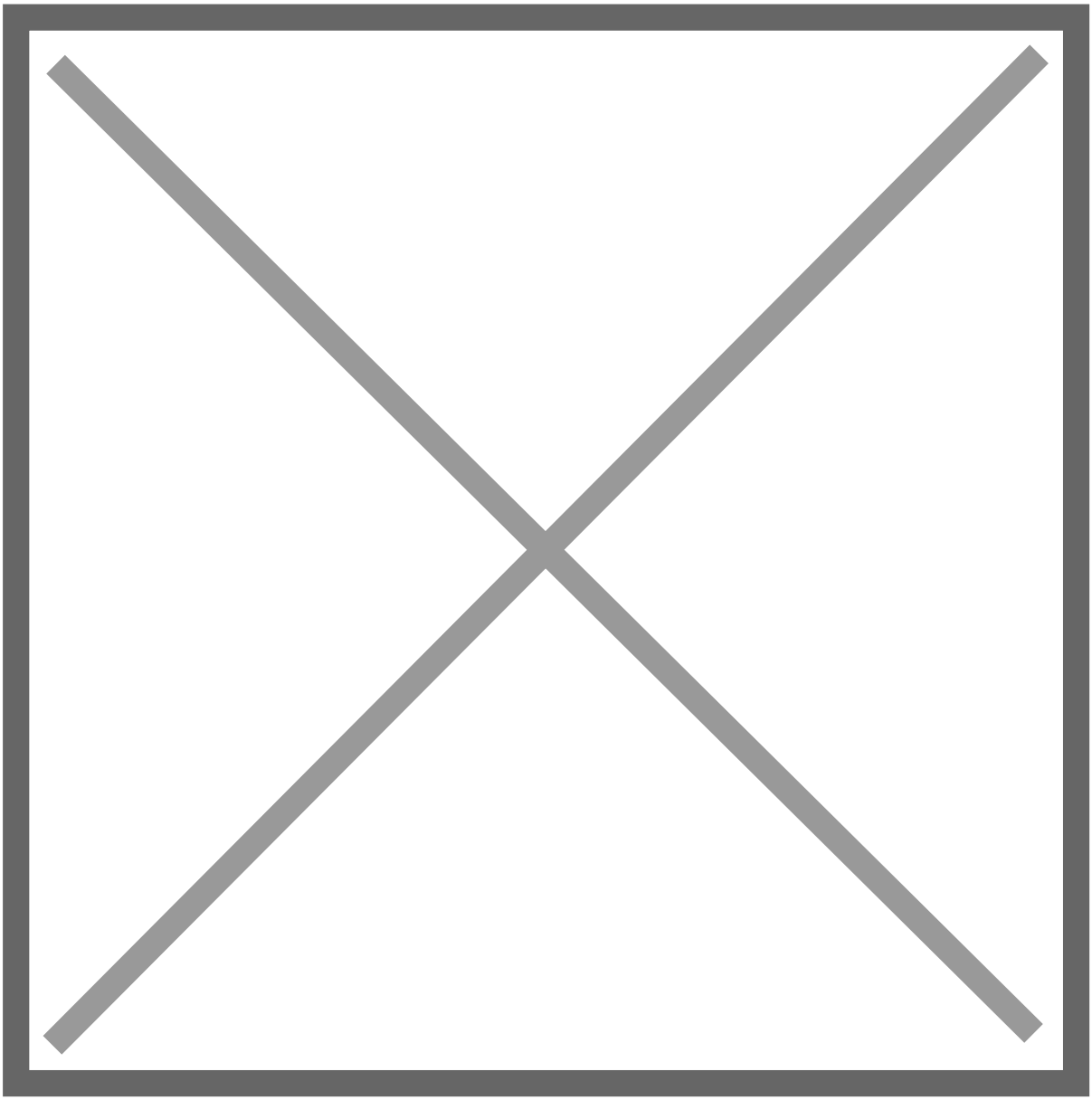


In the next screen assign a Link number, select the switch connection created and make sure you select the correct Switch CTI Link Number created in the PBX using the add cti x, in my case it is the cti link 1, on security you can select to have the TLINK encrypted, unencrypted or having both enabled.

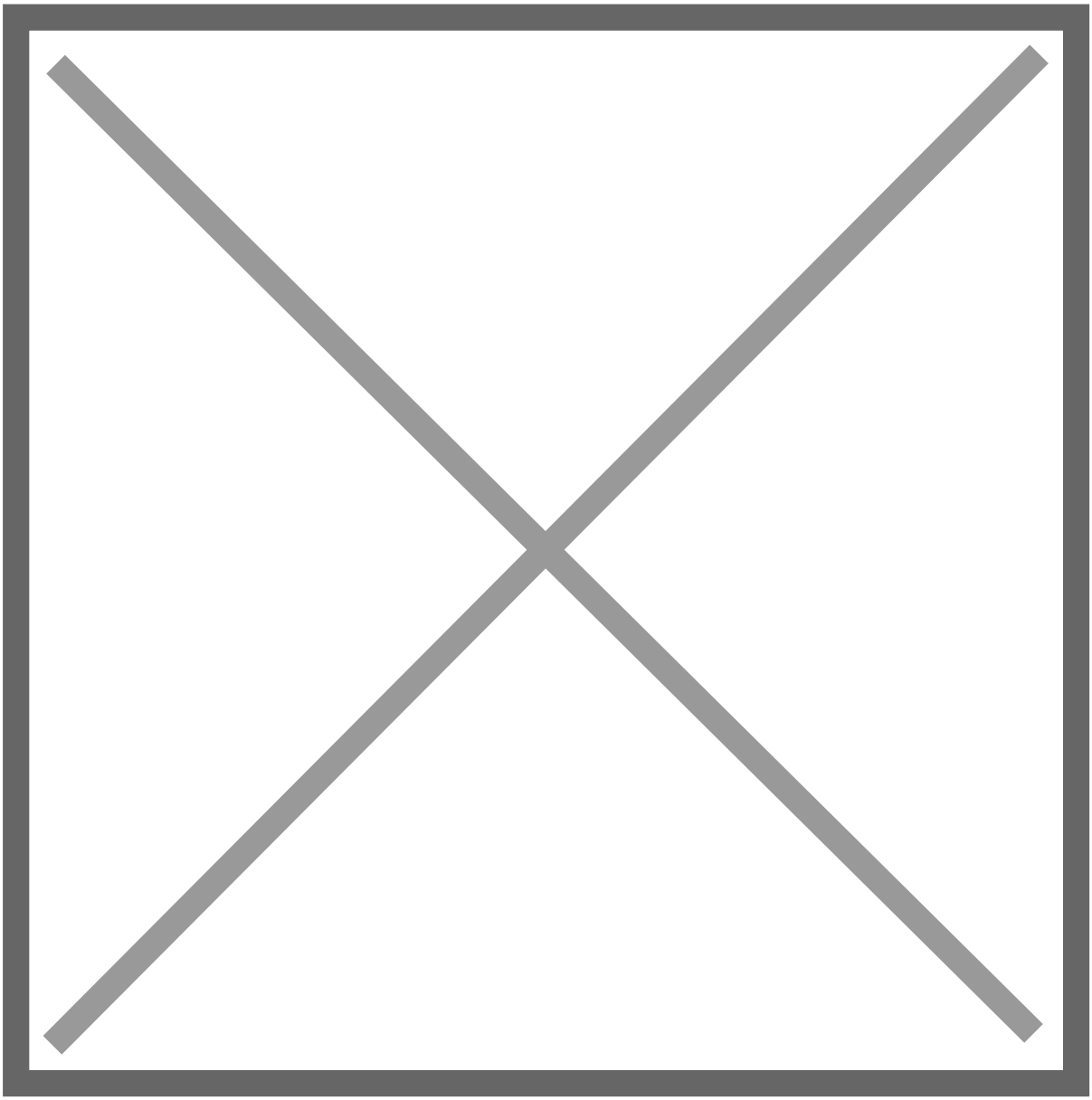


Lets complete this entry verifying the status of the CM Connection and the TSAPI CTI link:

Status -> Status and Control -> Switch Conn Summary



Status -> Status and Control -> TSAPI Service Summary



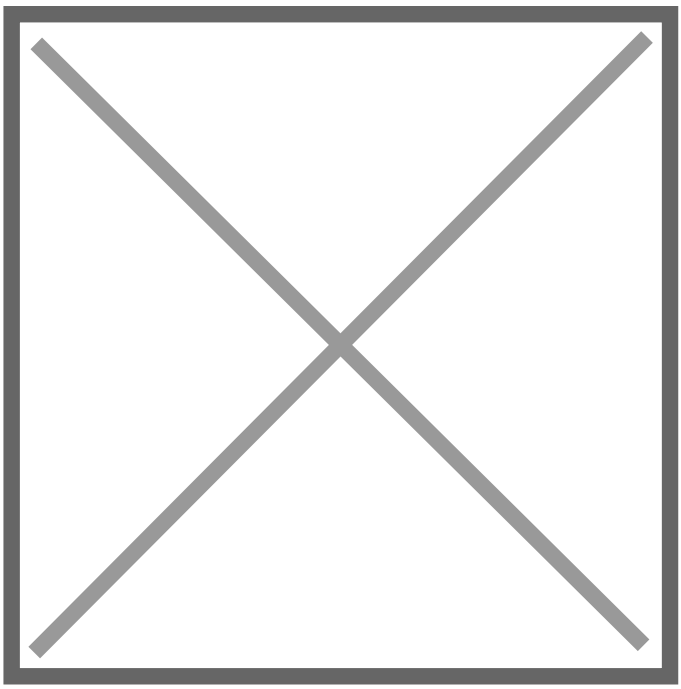
Source: https://whereismyvoicepacket.com/avaya-aes-admin-task-aes-tsapi-cti-link-integration/

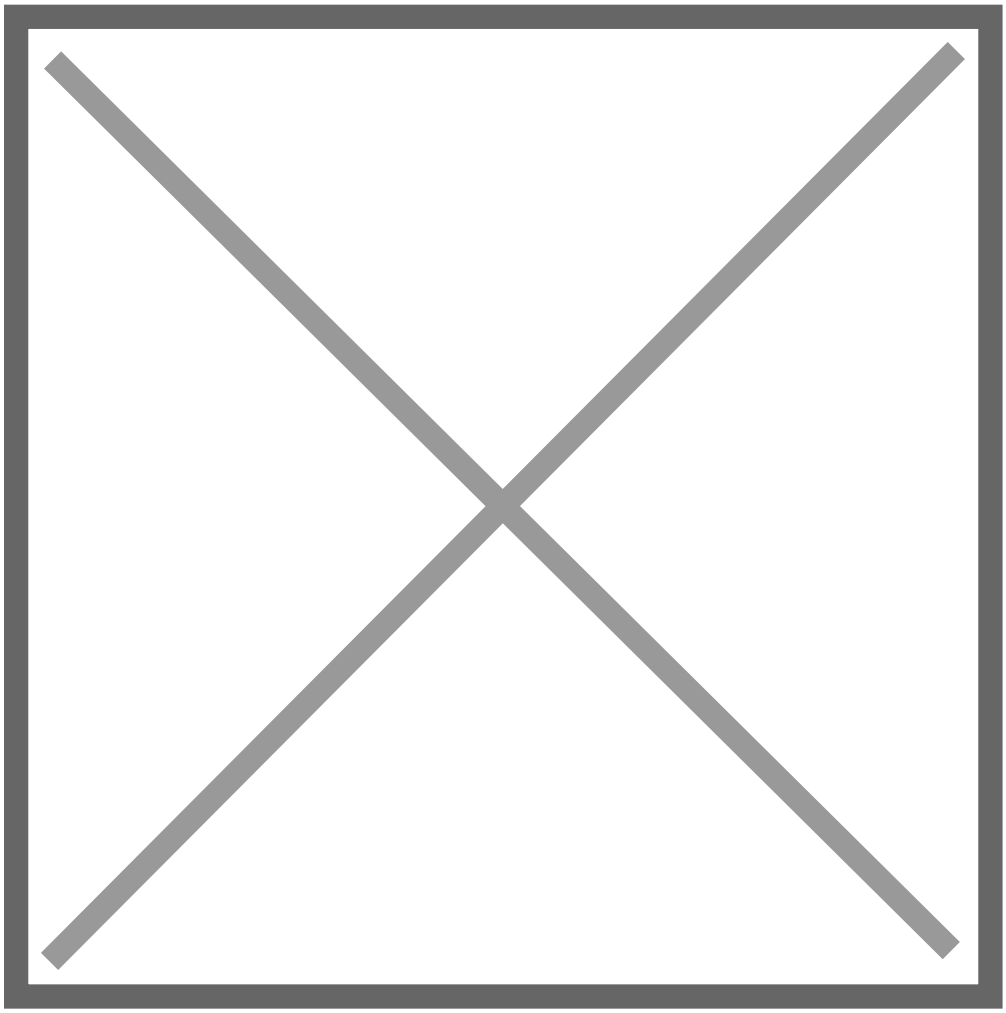
AES - Upgrade 8.0.1 to 8.1.3

In this entry we will focus in upgrading an AES version 8.1.2 to 8.1.3, to accomplish this we will fist 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

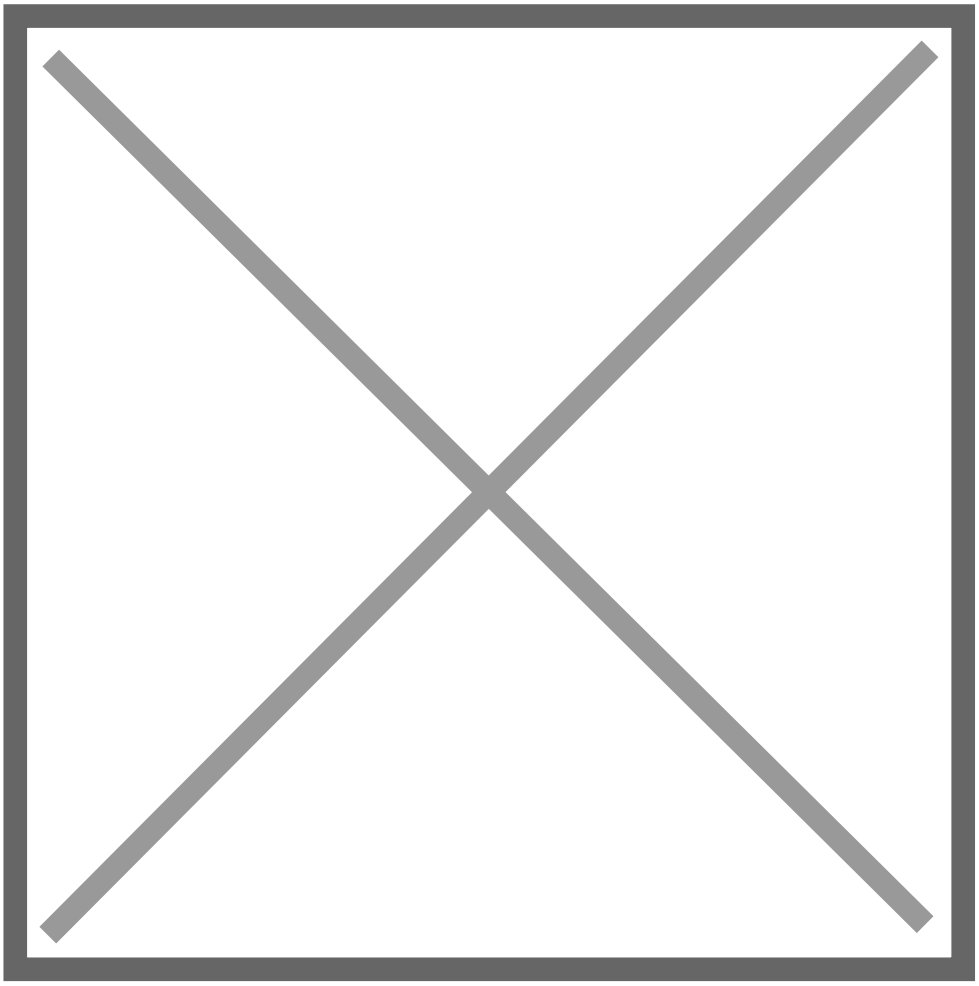


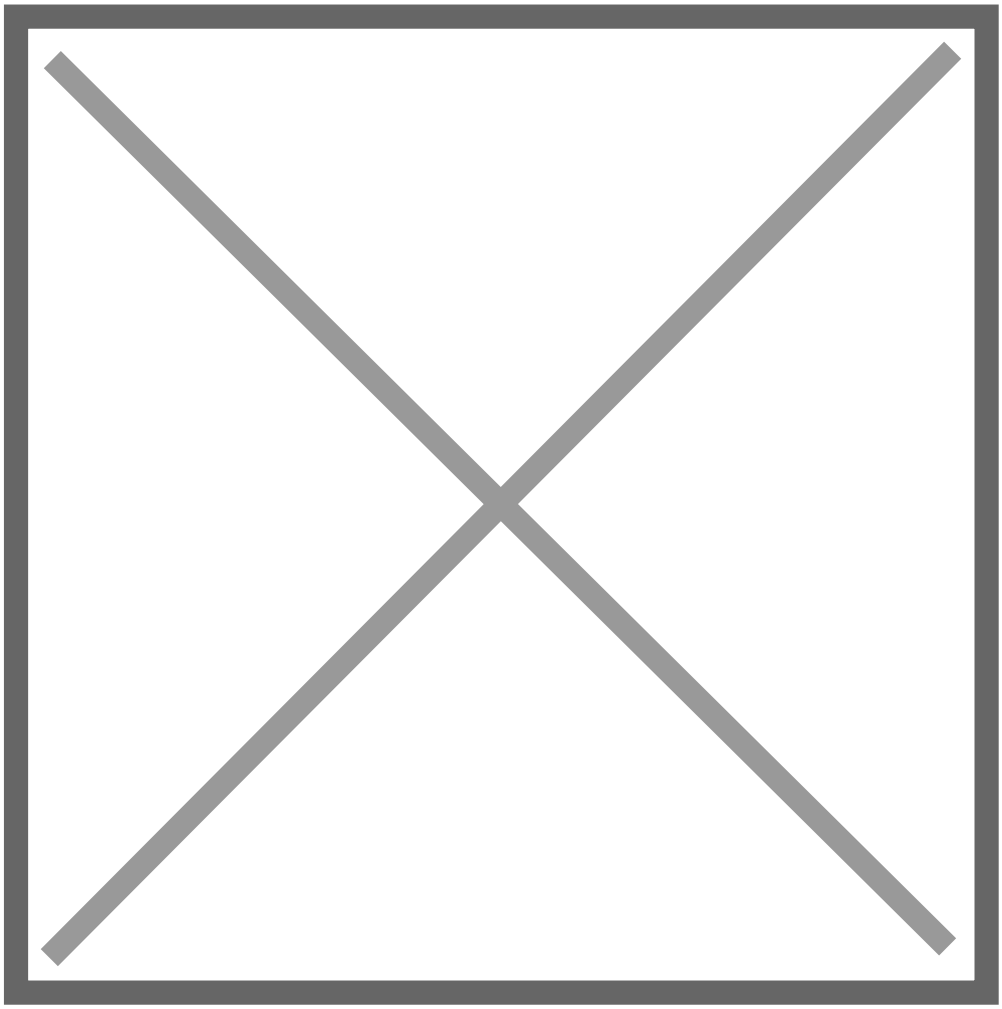


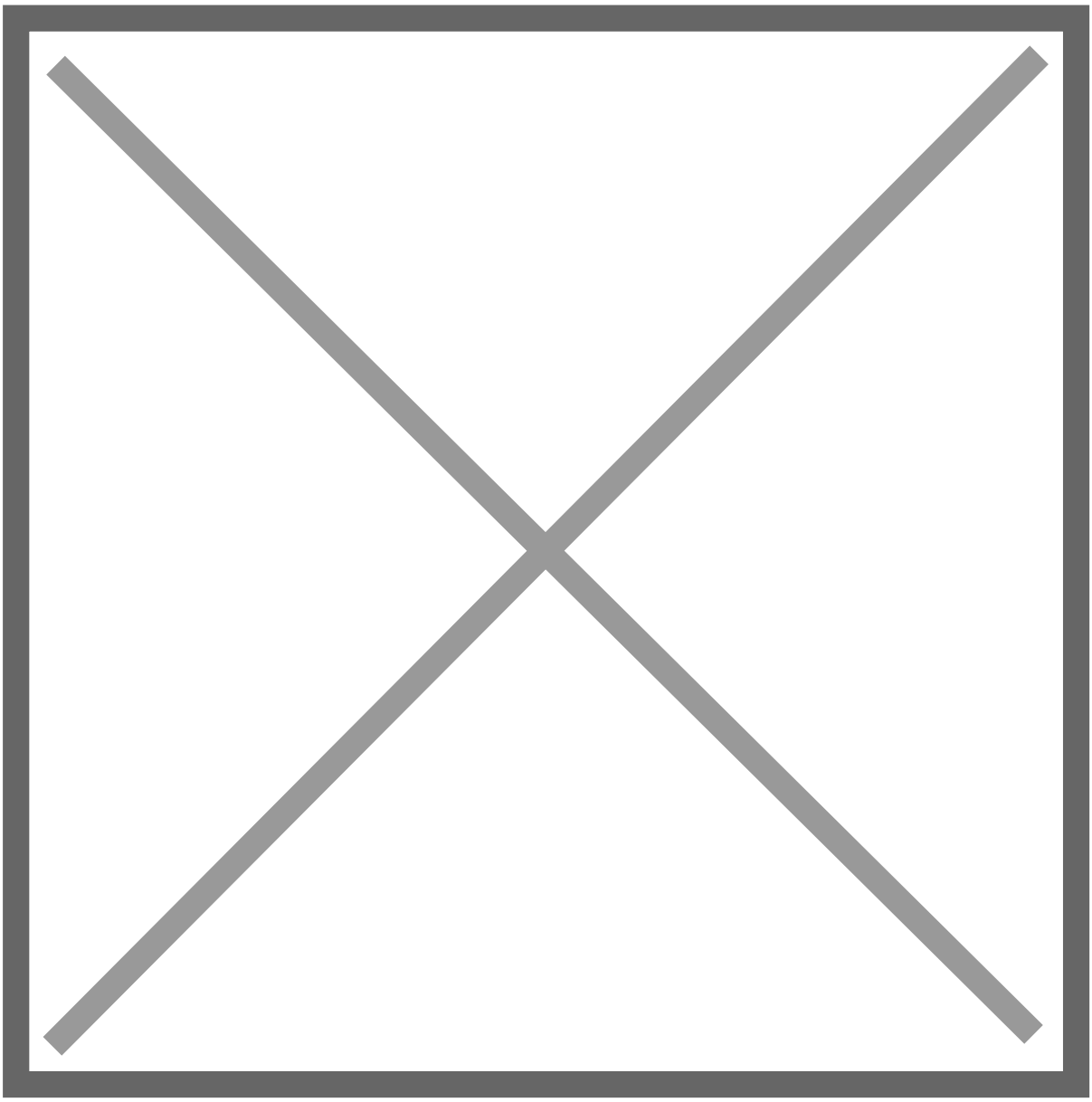
We will use the previous command later in this entry.

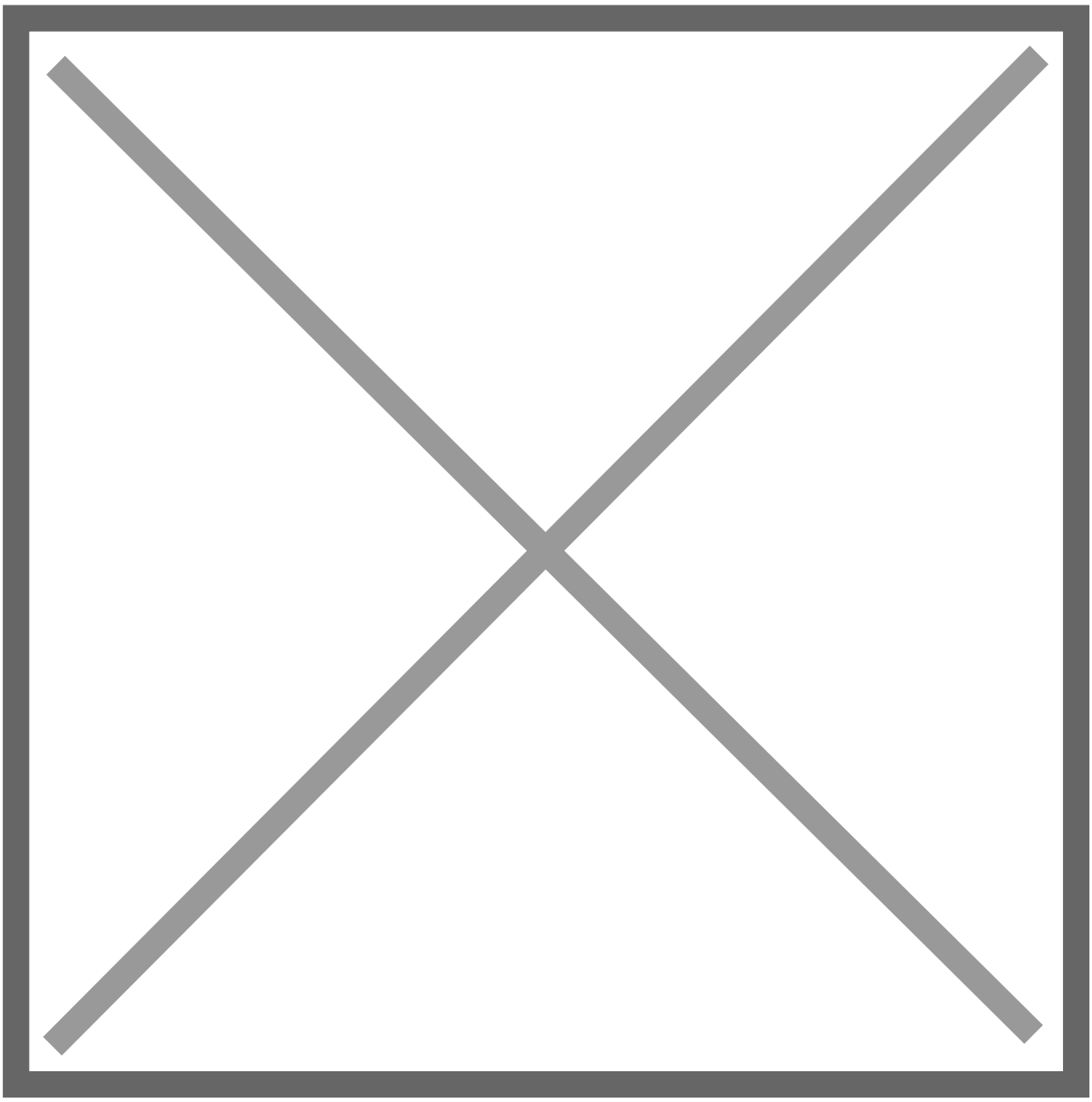
Here is the process to follow:

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)



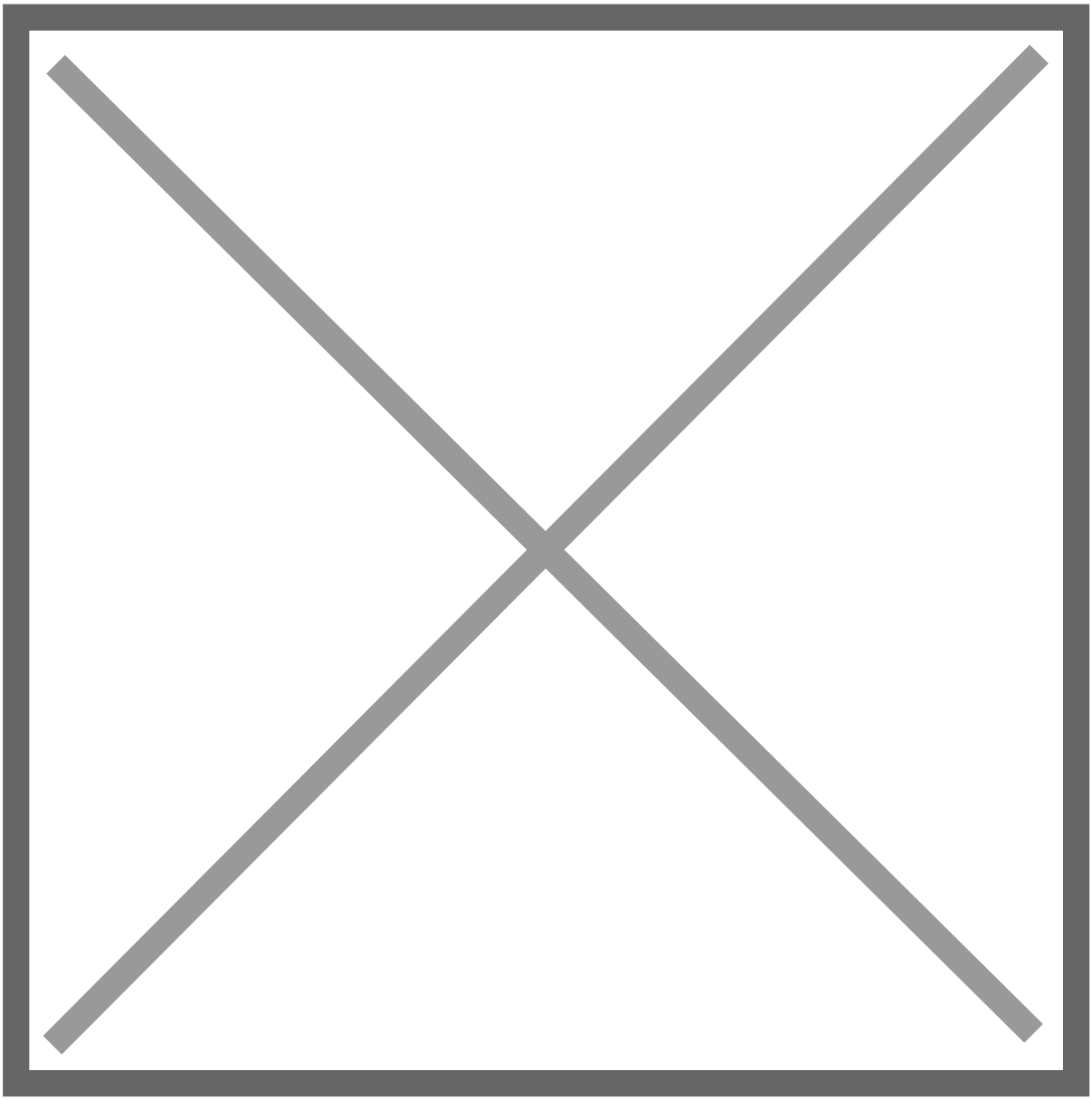




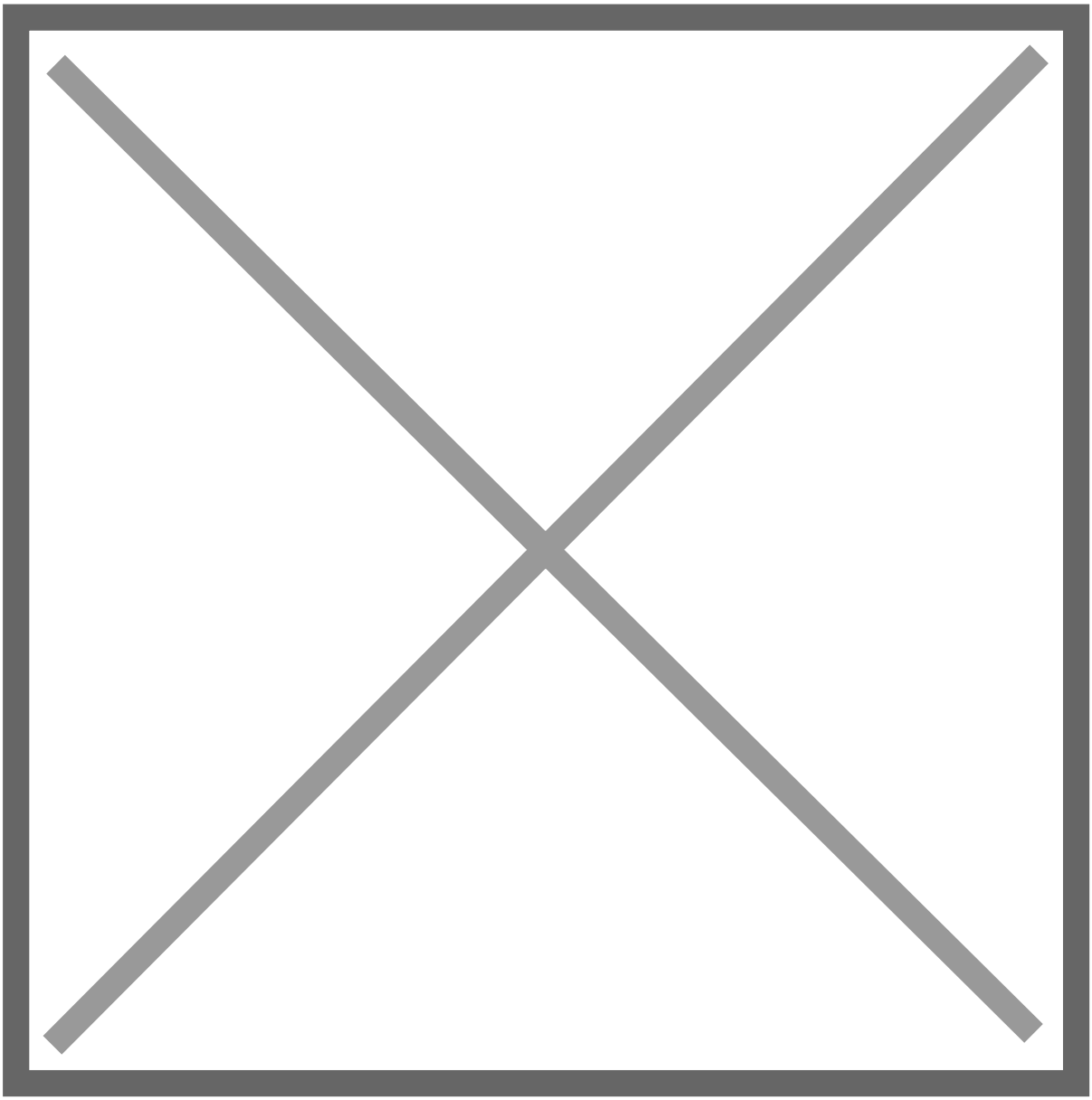


2. Keep track of the current configuration Backup configuration (Screenshoots)

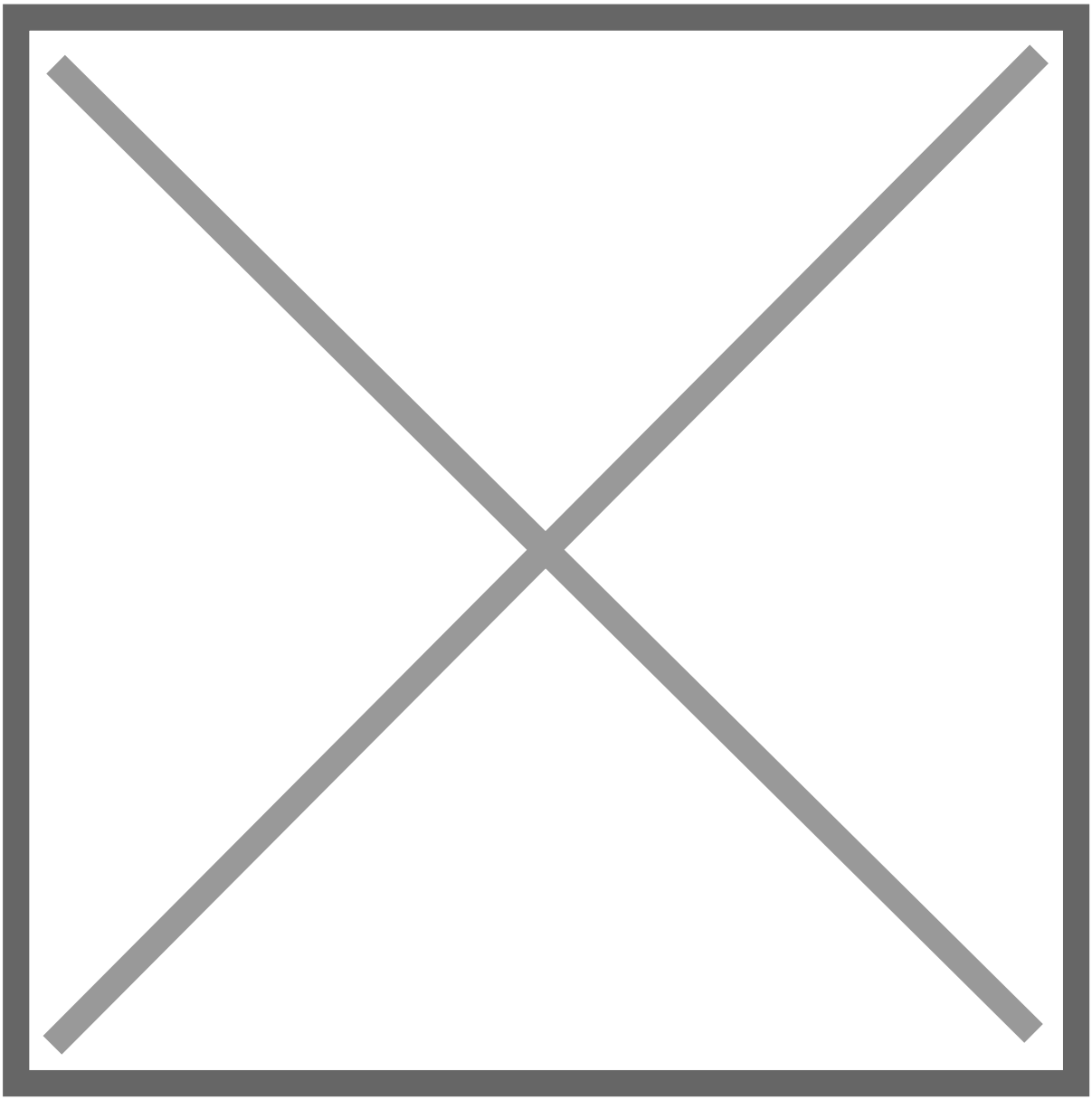
AE Services



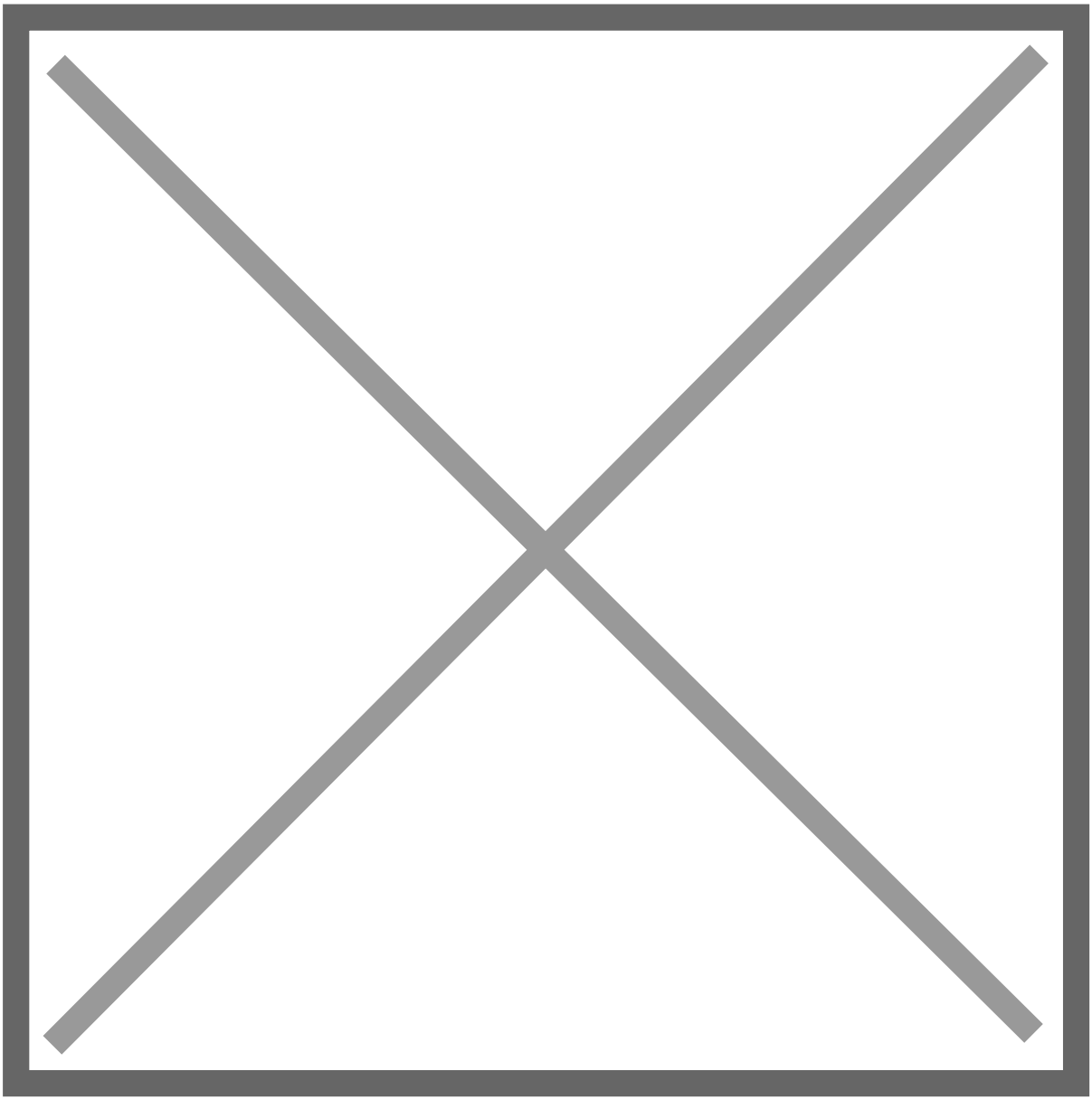
AES Services -> CVLAN -> CVLAN Links



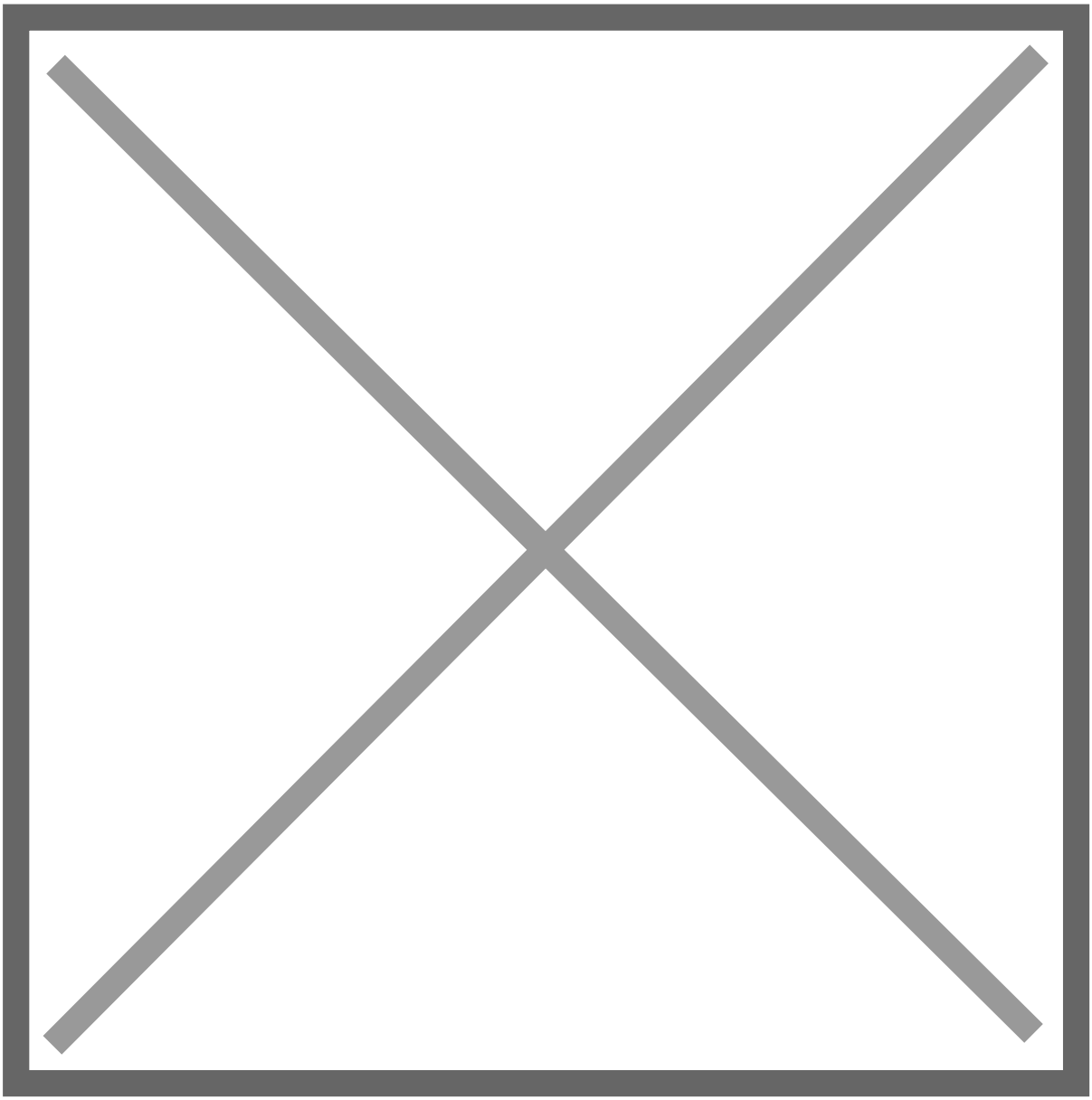
AES Services -> TSAPI -> TSAPI Links



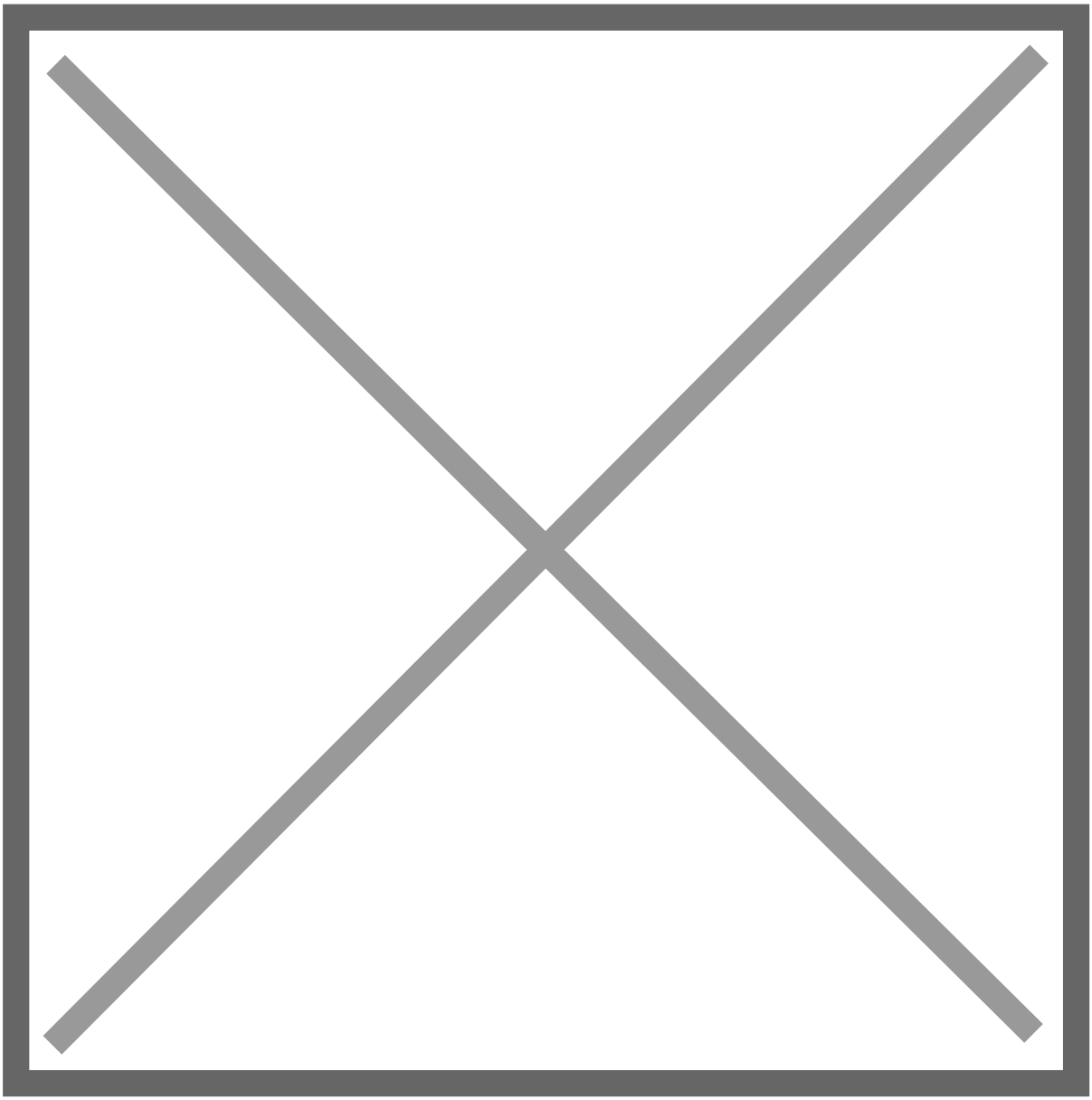
Communication Manager Interface -> Switch Connections



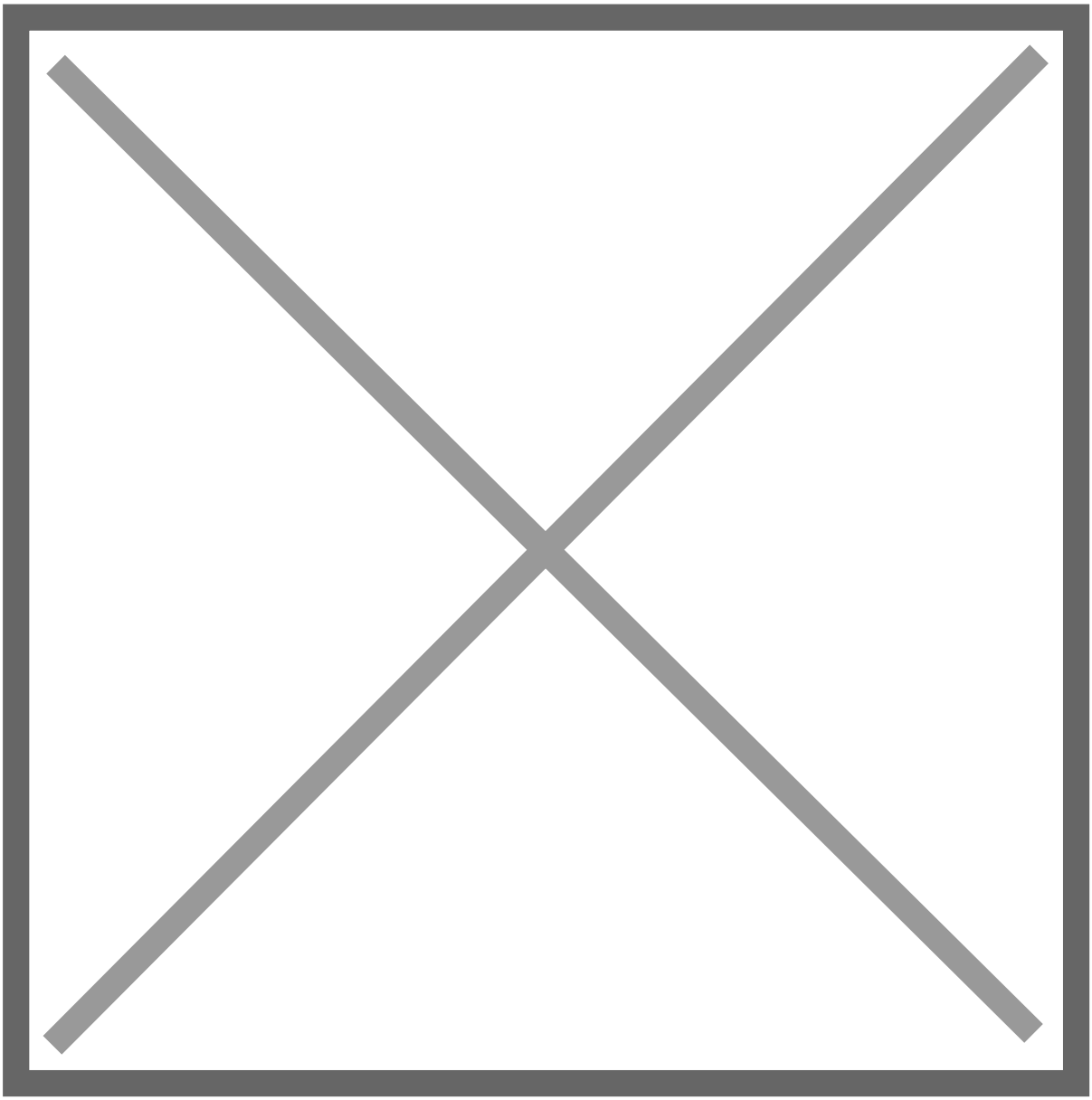
Communication Manager Interface -> Switch Connections -> Edit Connection



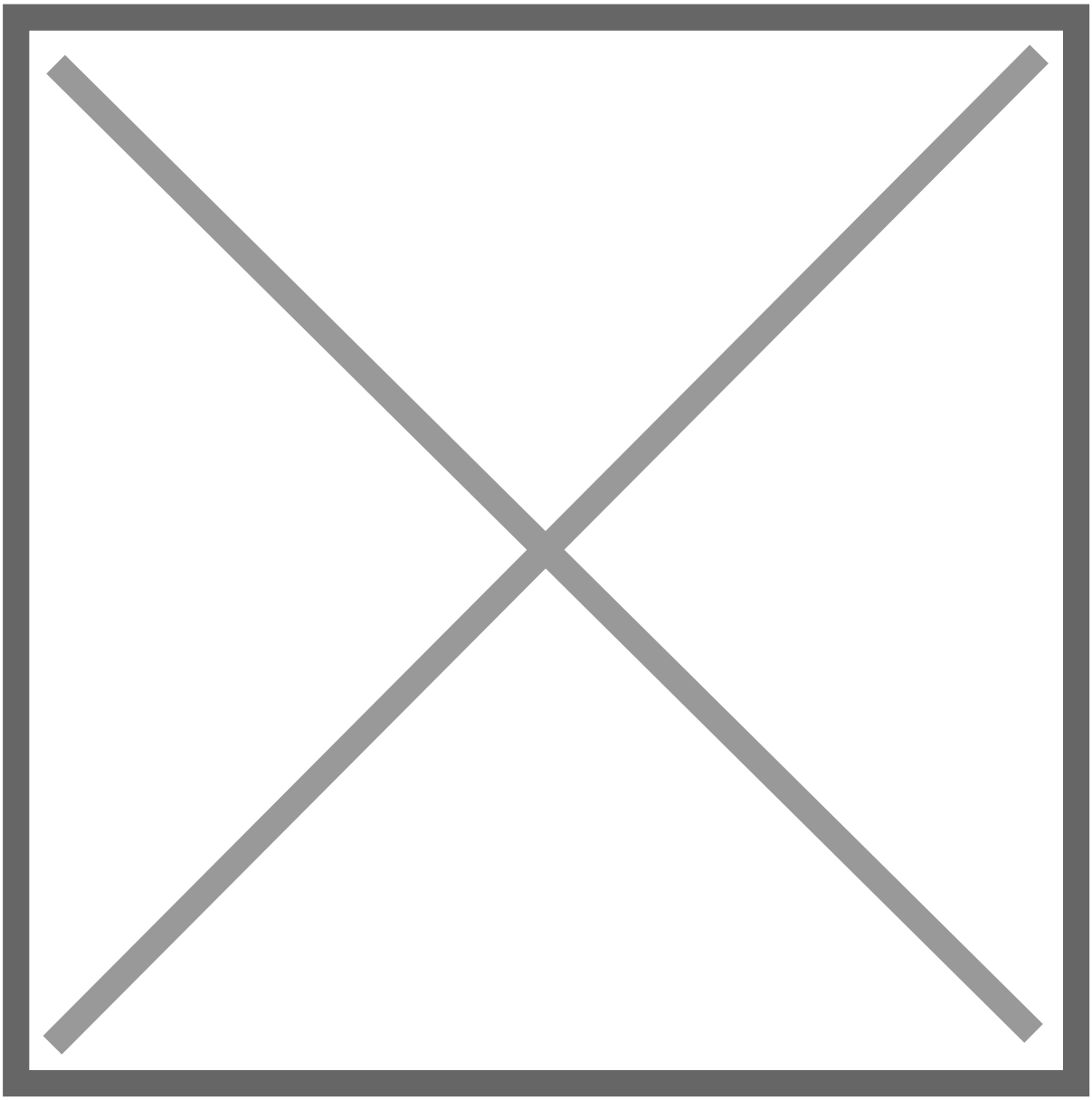
Communication Manager Interface -> Switch Connections -> Edit PE/CLAN IPs



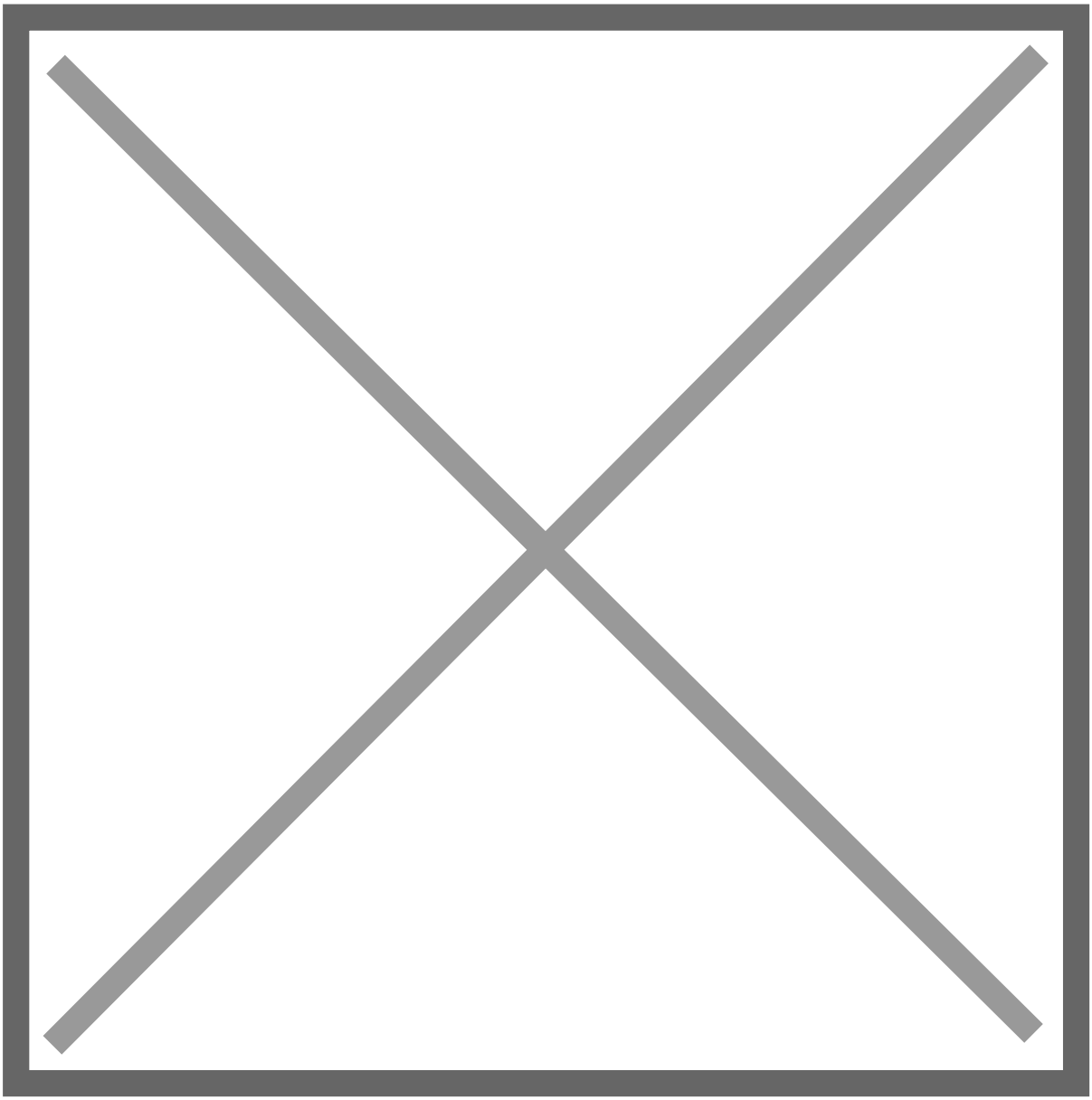
Communication Manager Interface -> Switch Connections -> Survivability Hierarchy

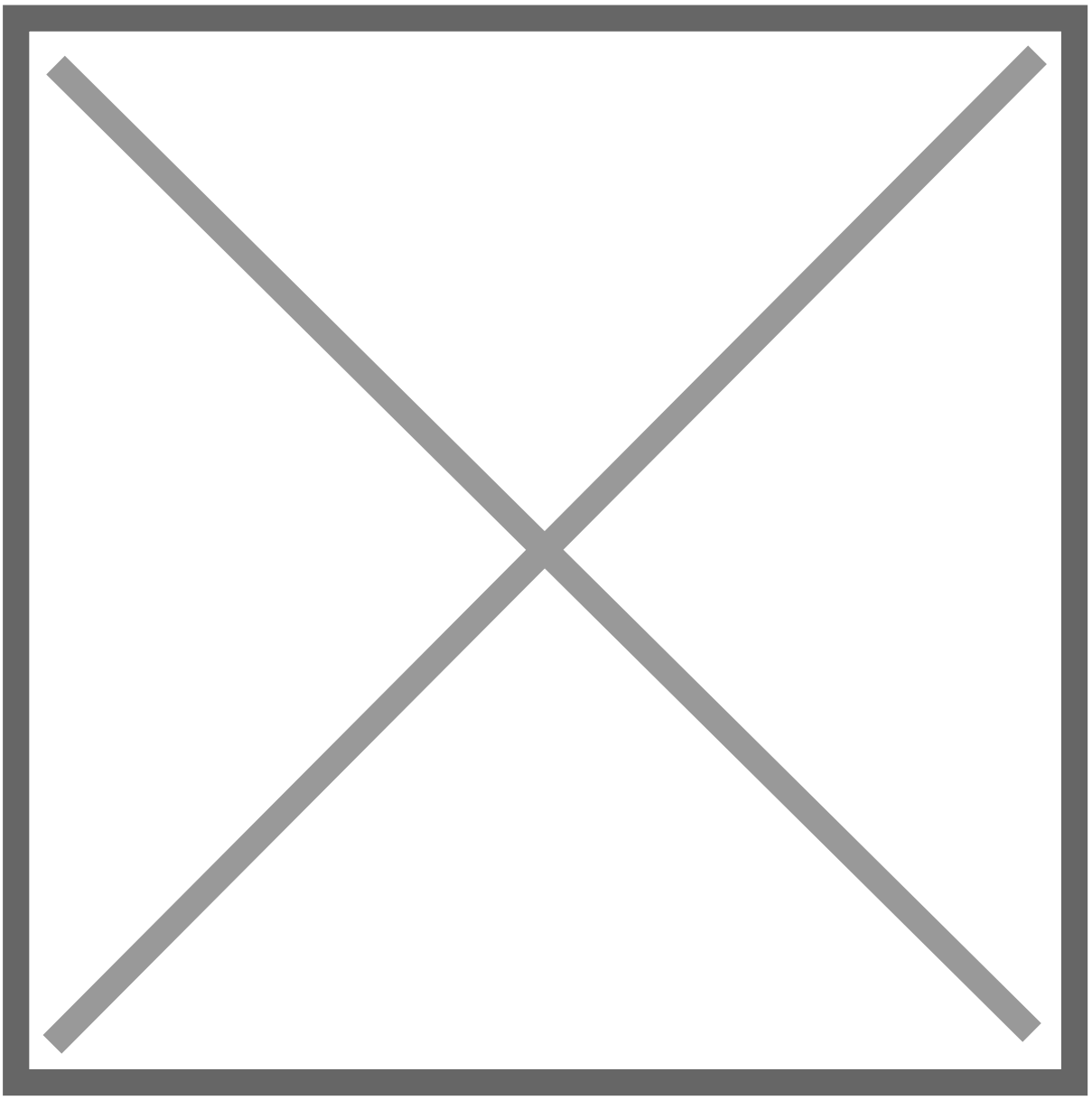


Maintenance -> Date Time/NTP Server

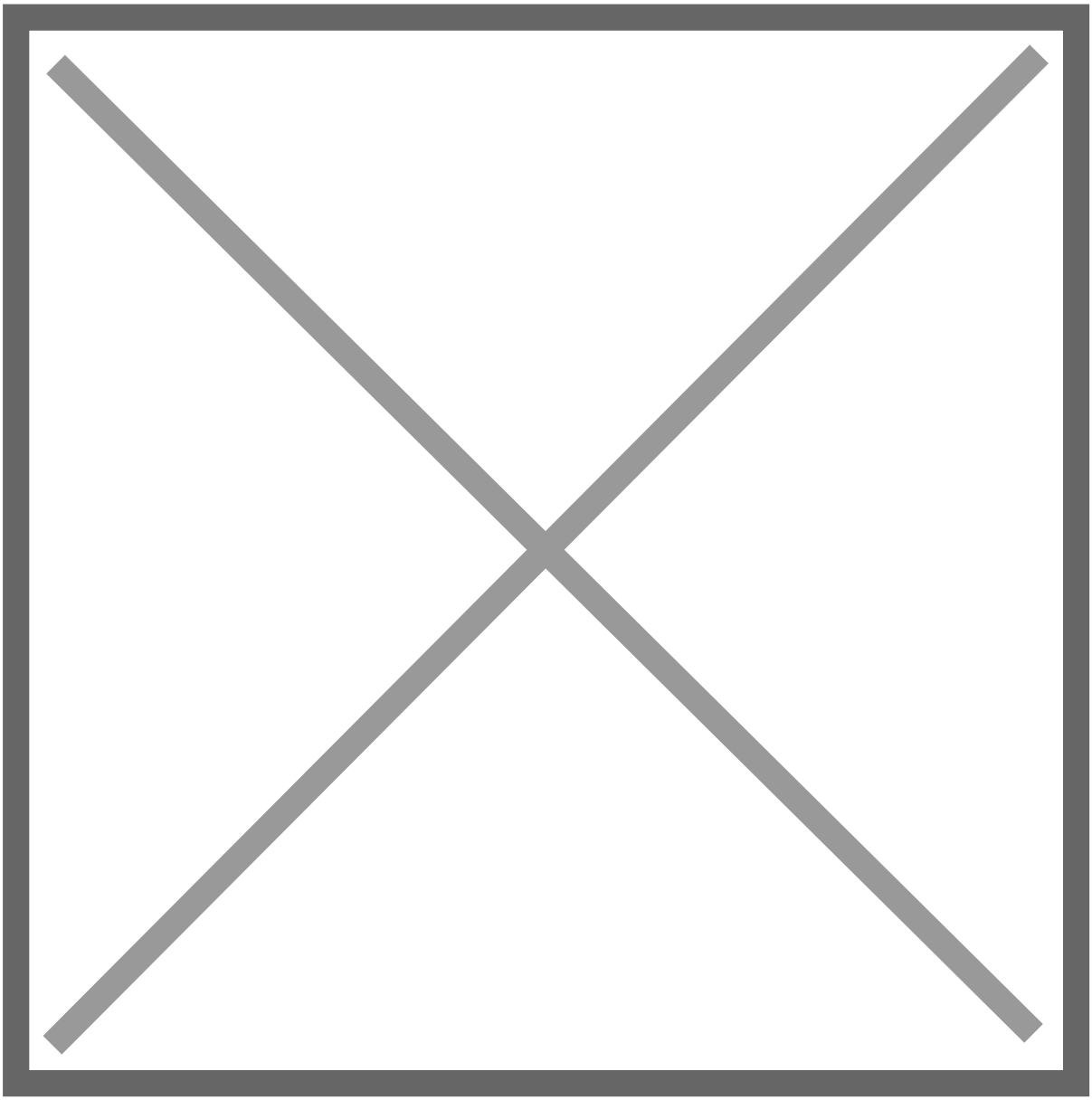


Networking -> Network Configure

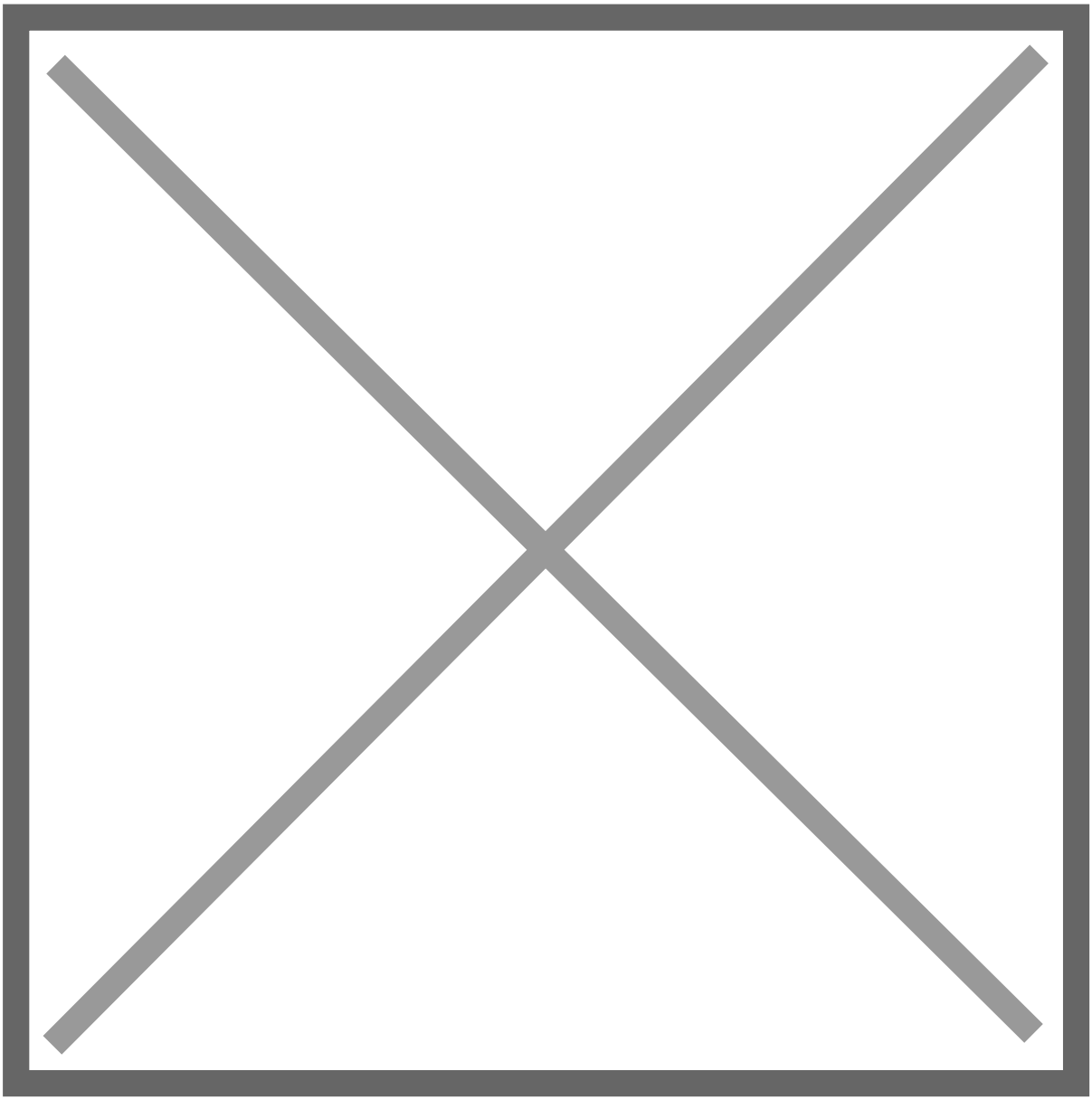




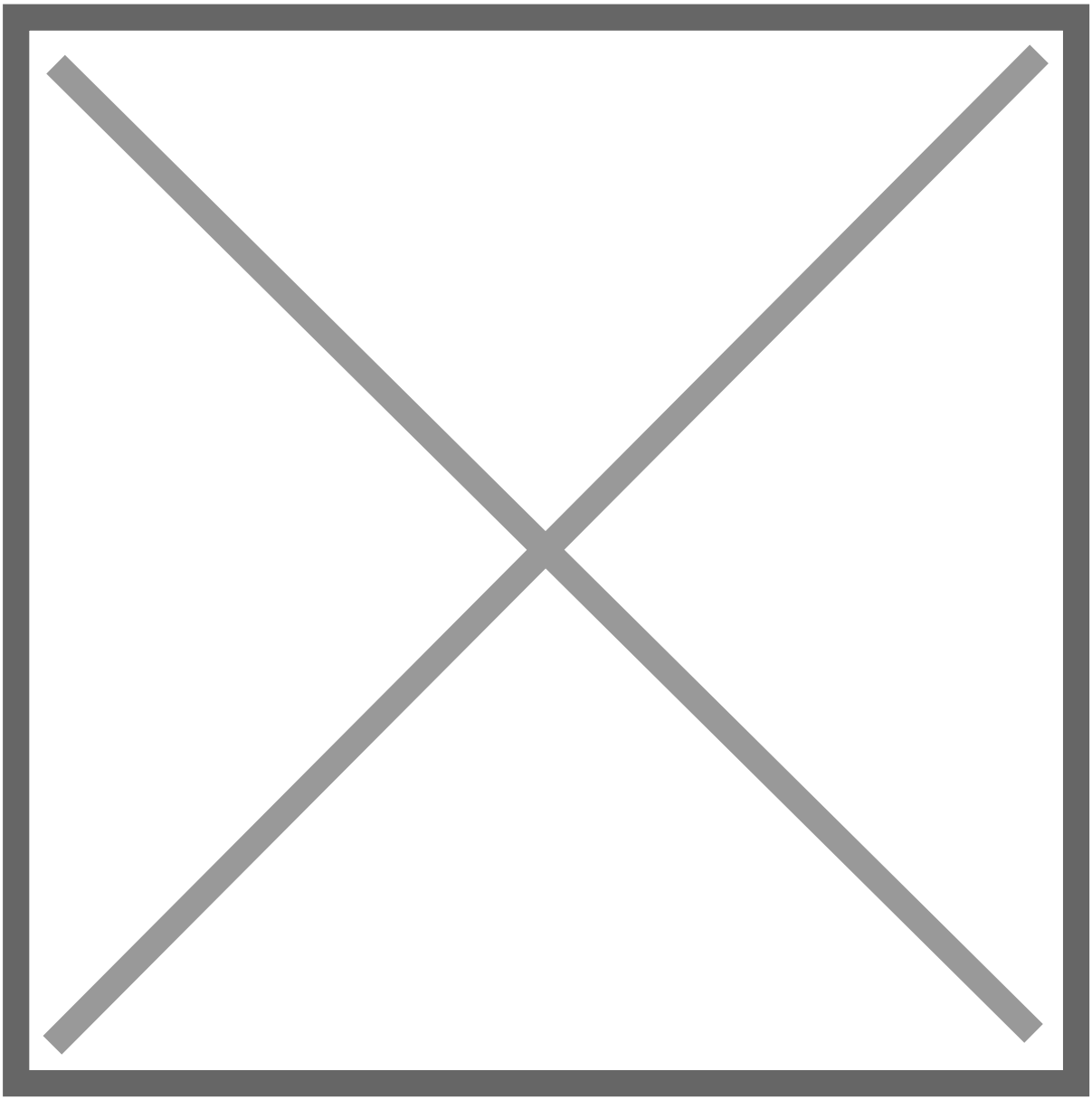
Security -> Security Database -> Tlinks



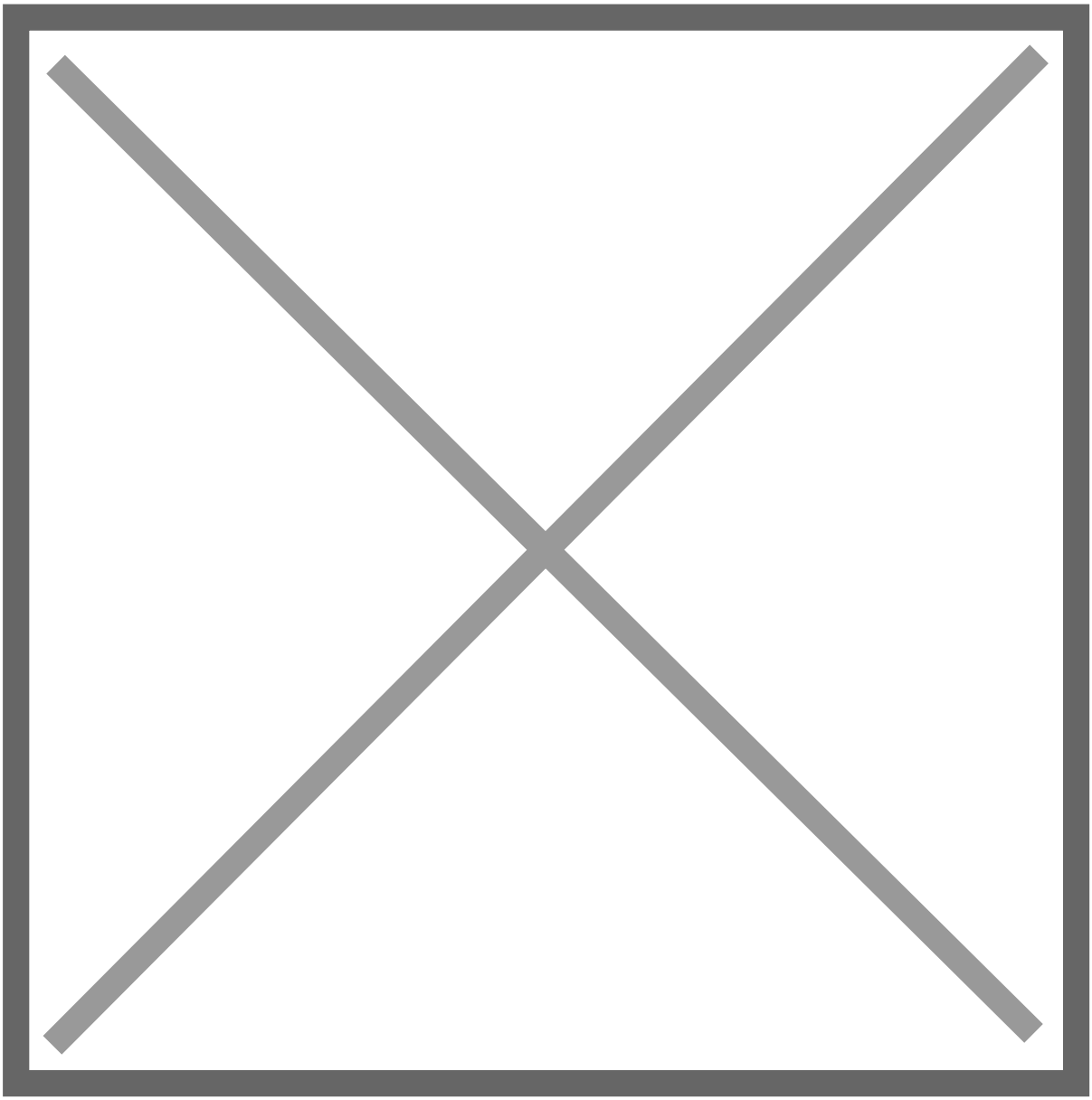
Status -> Switch Conn Summary



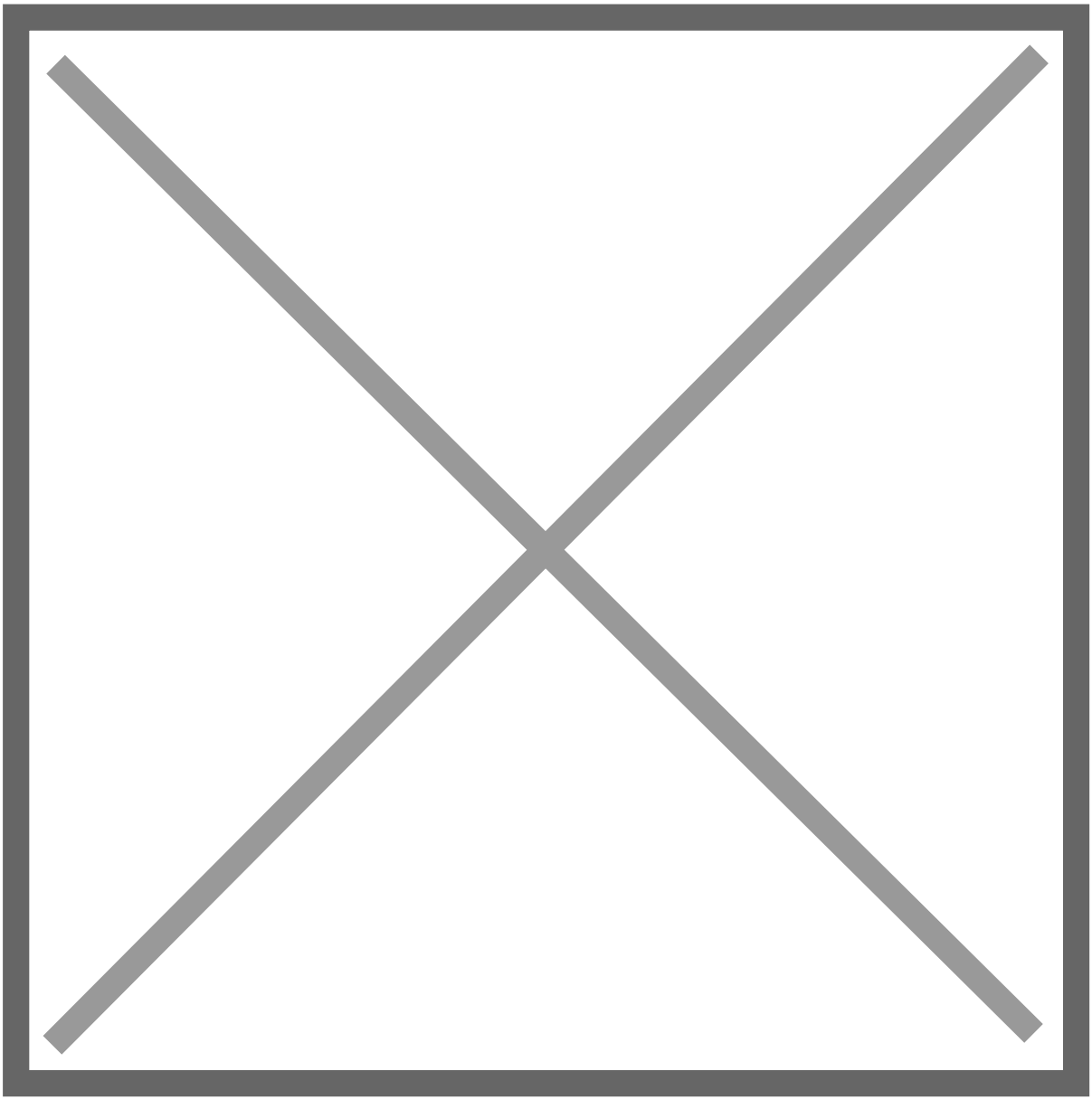
Status -> TSAPI Service Summary



Utilities -> SNMP -> SNMP Agent

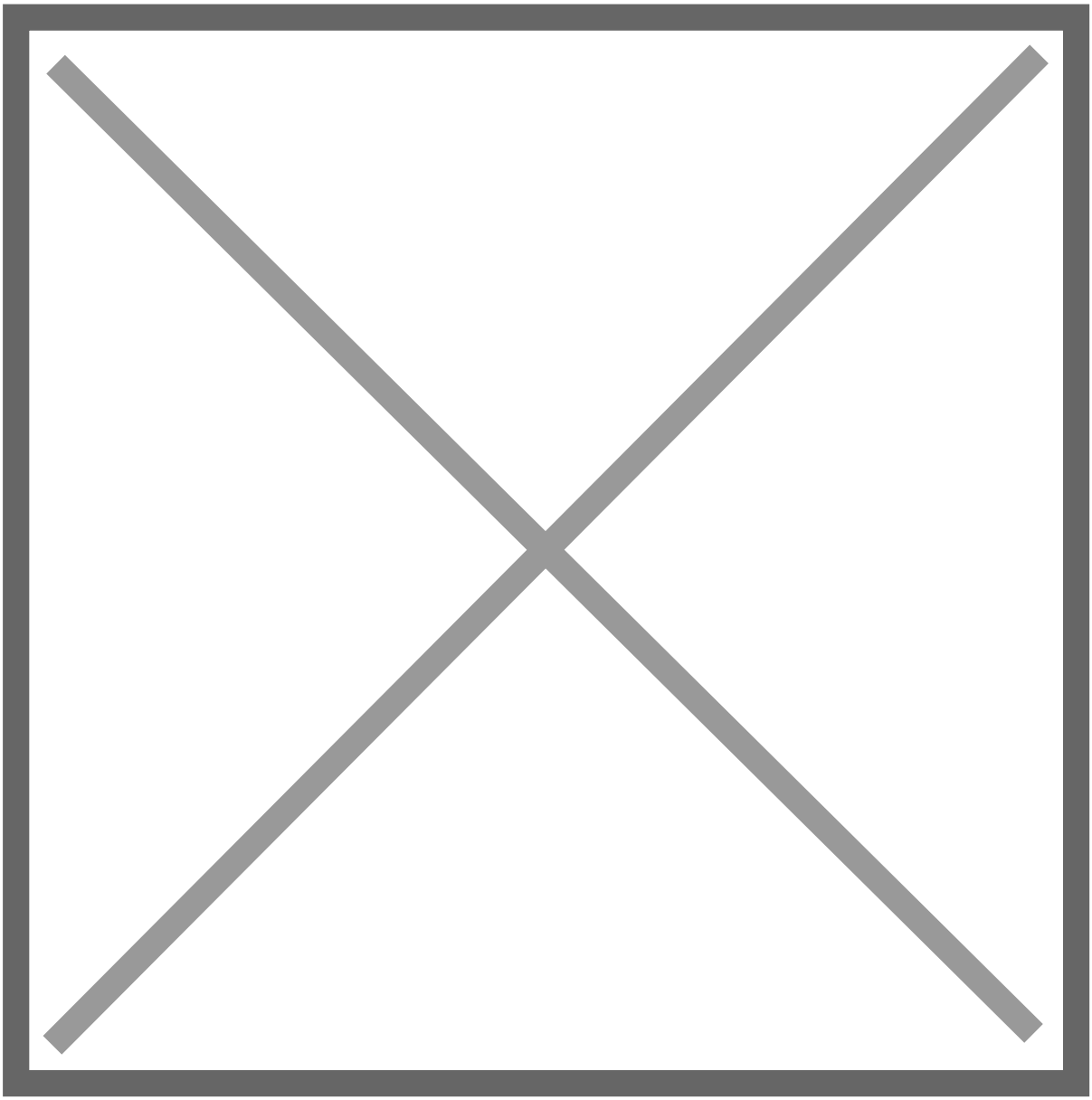


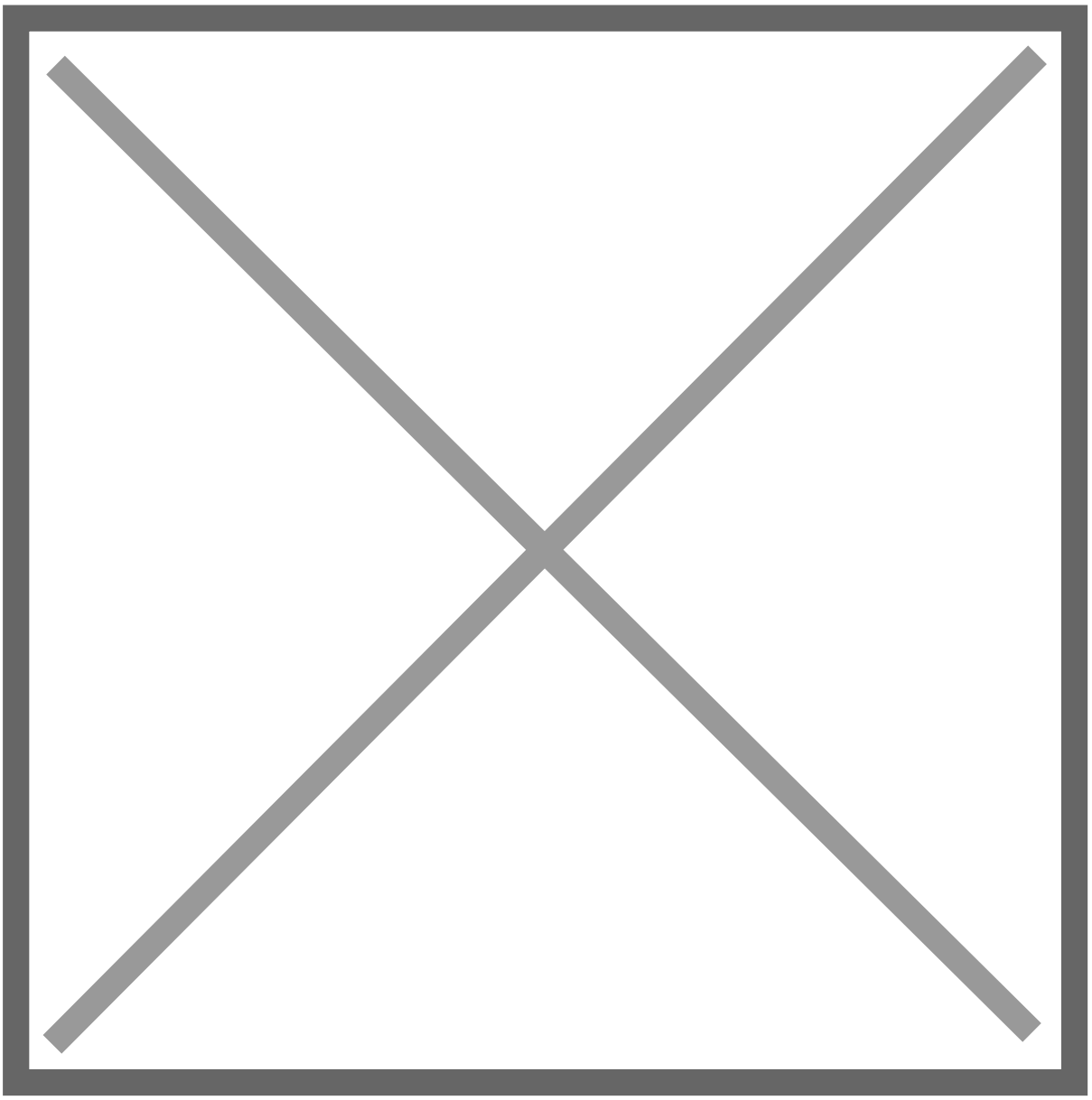
Utilities -> SNMP -> SNMP Trap Receivers



3. Maintenance window

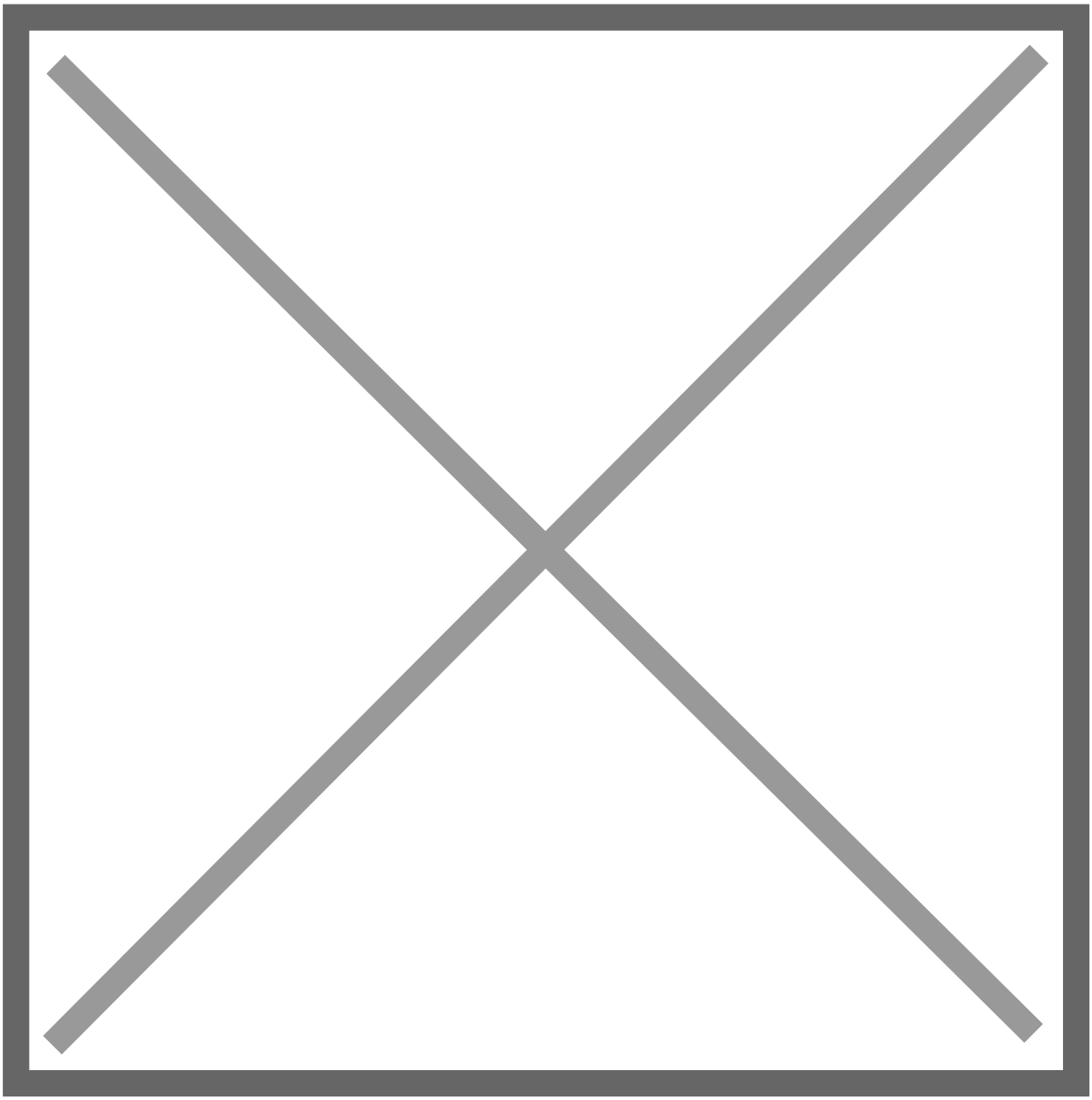
Create a backup file **Maintenance -> Server Data -> Backup** and download

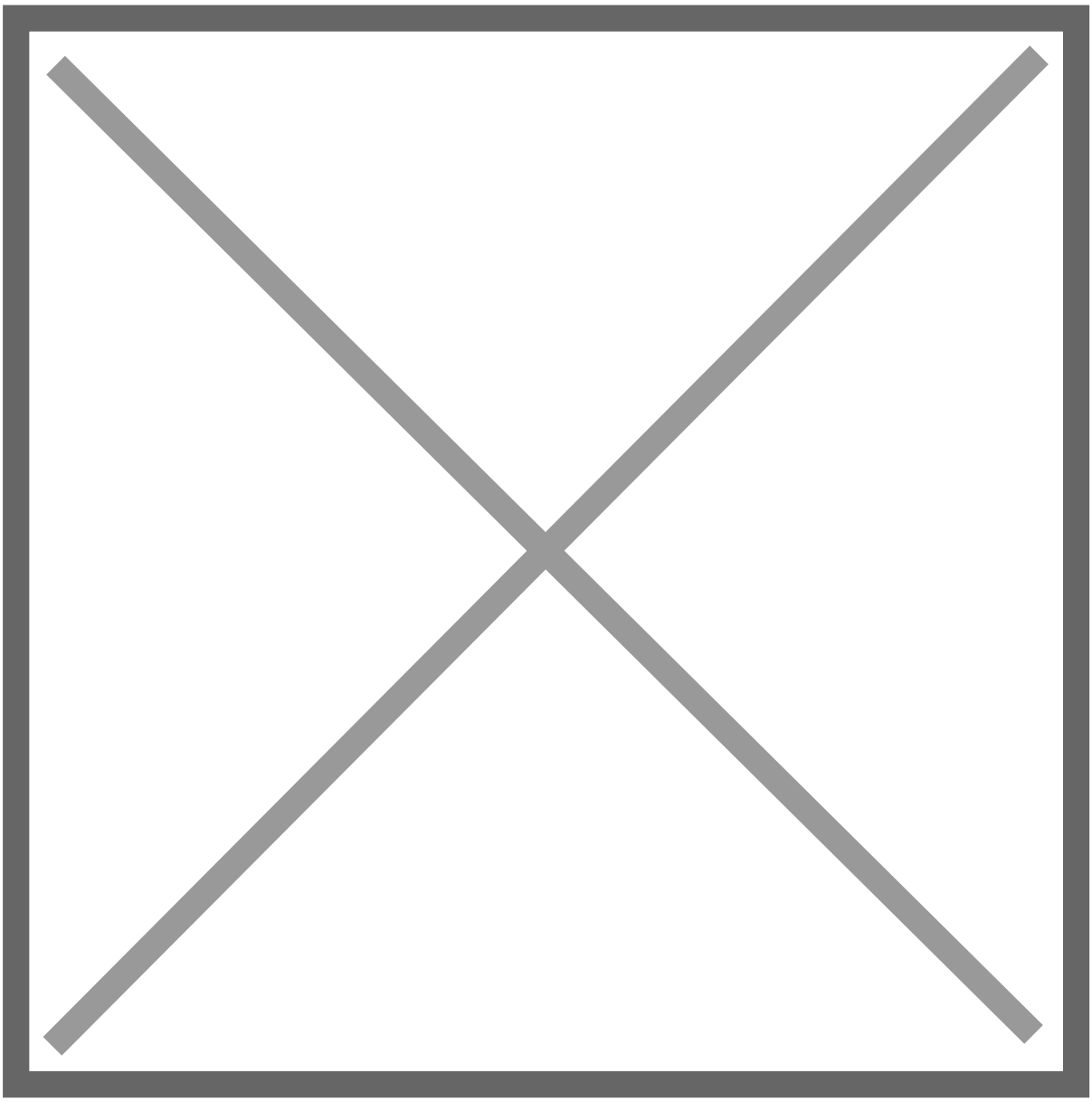




Shutdown production server

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/

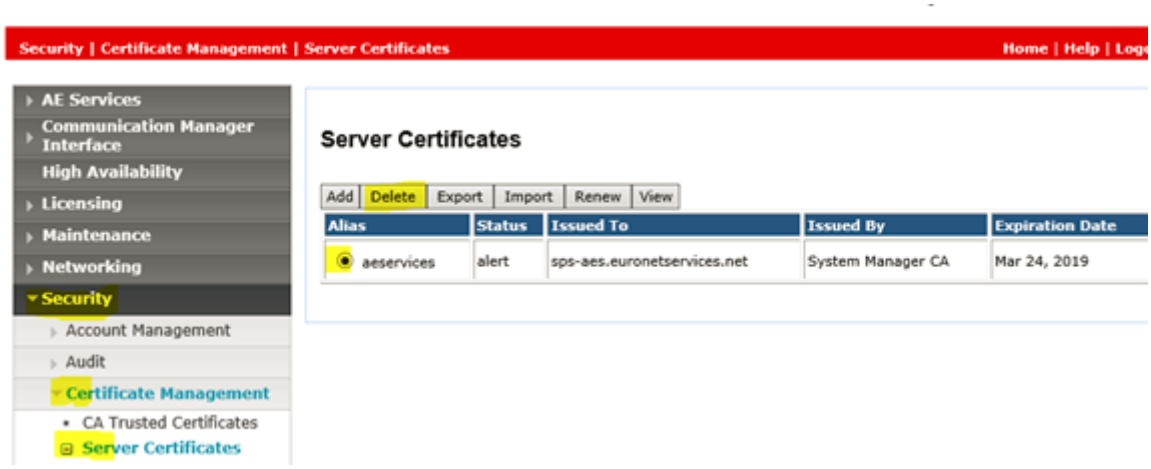
Administration, upgrades and maintenances

AES - Renew AES Cert using System Manager

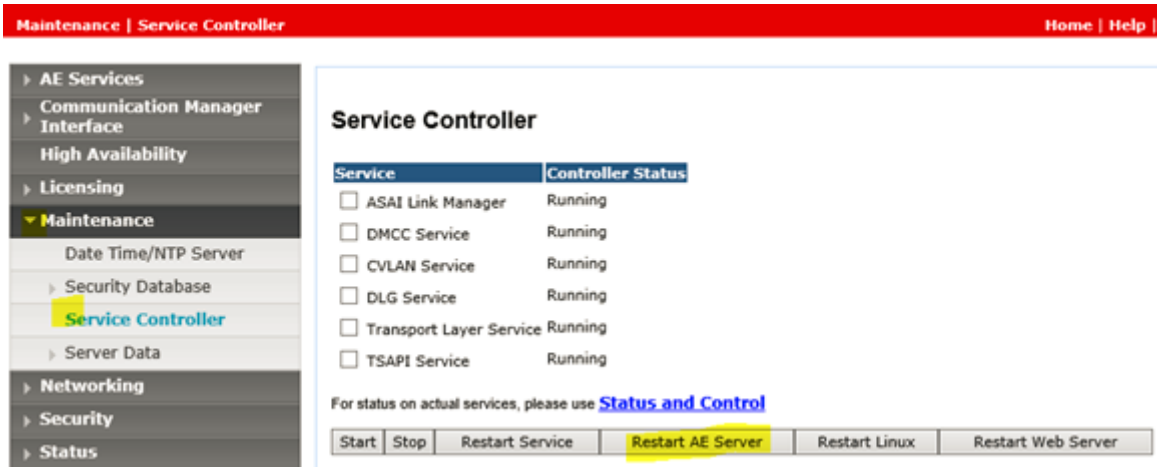
AES certificate renewal if using SMGR certificate with CA Certificate and End Entity in place.

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

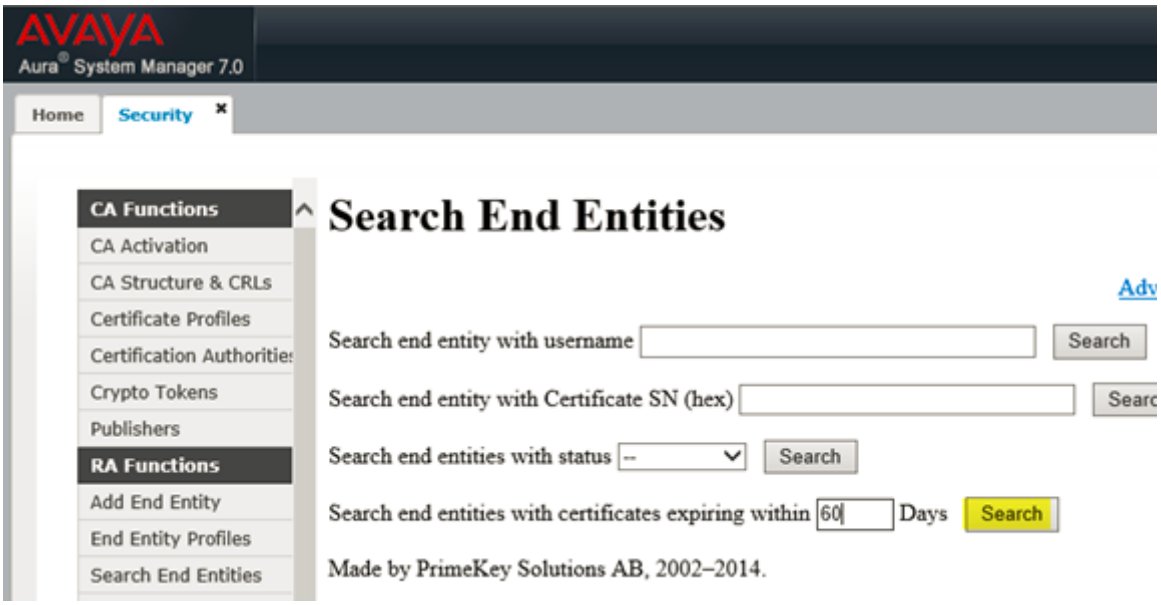
1. Remove Certificate that is about to expire from AES.



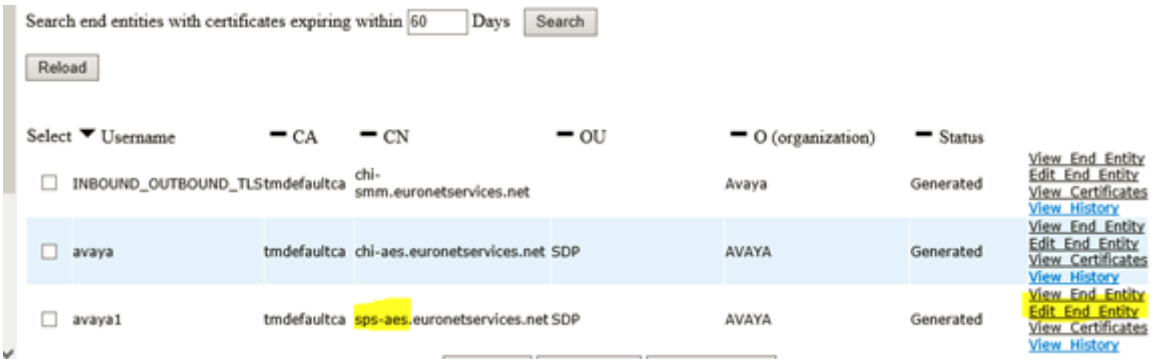
2. Restart AE Server



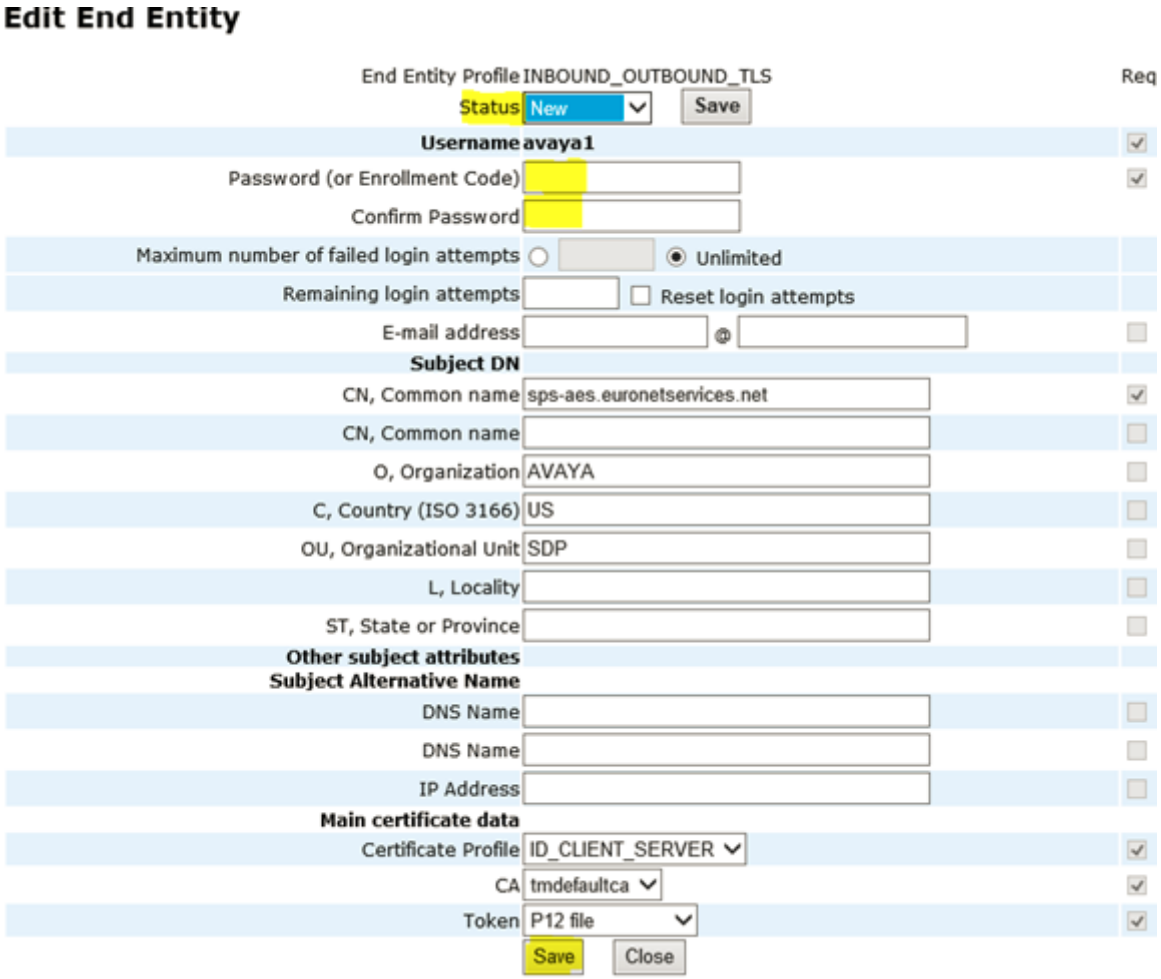
3. Go to the System Manager> Security> Certificates> Authority> Search End Entities



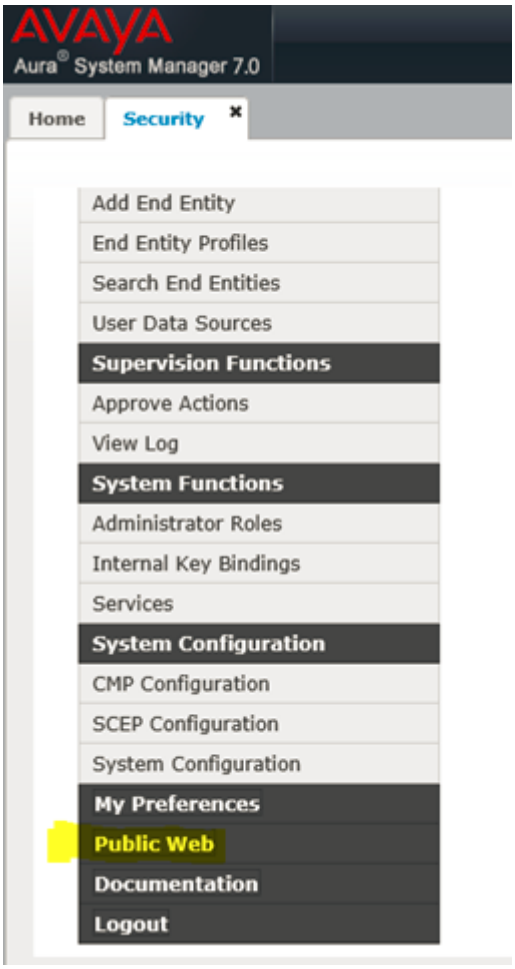
4. Verify the certificate for your AES by the CN and select *Edity End Entity*



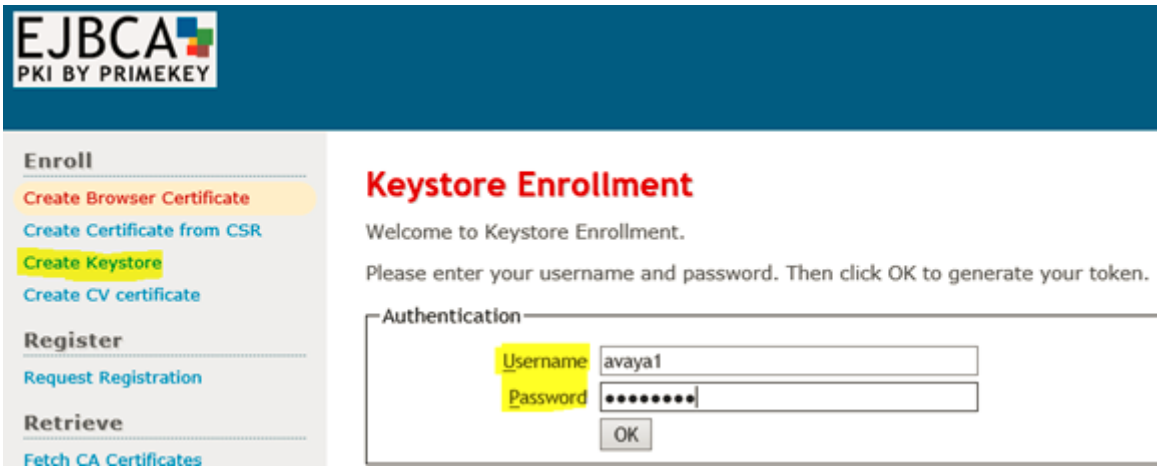
5. Change the status to New, enter the passwords and then Save



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.

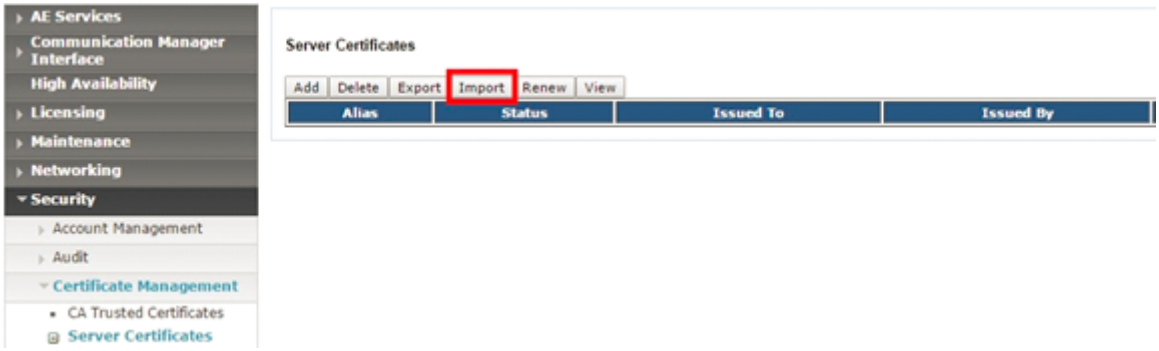
Once you click enroll the certificate will be downloaded (depending on your browser you can select where it is saved or find it in downloads from windows explorer.

Next Import the new AE Services server certificate into the AES

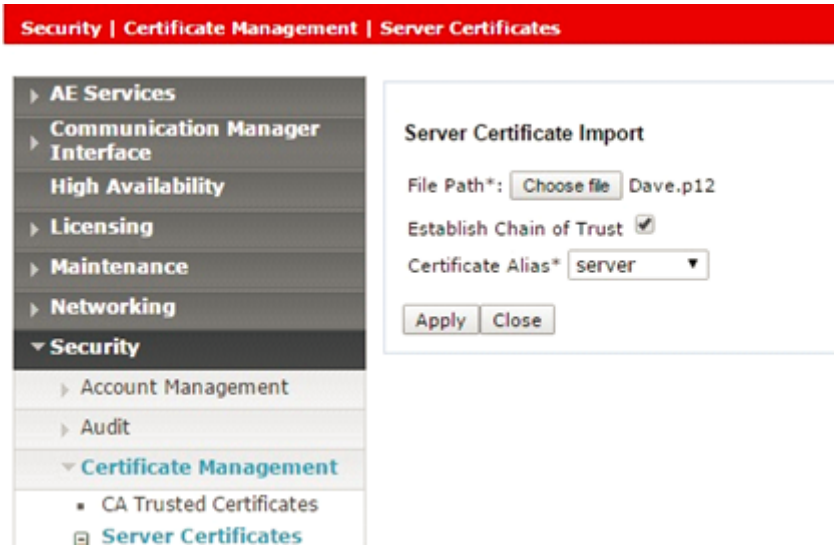
1. Using the AE Services Management Console navigate to "Security > Certificate Management > Server Certificates"

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

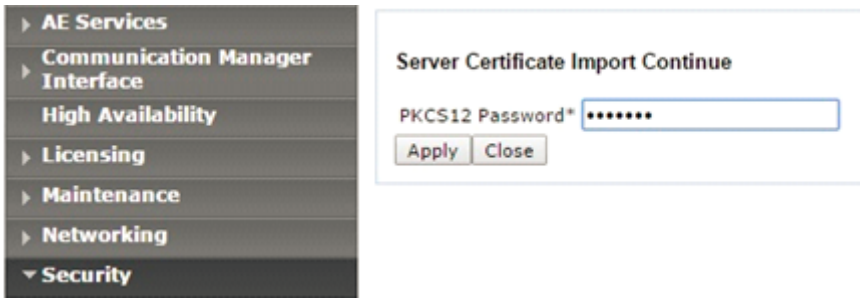
3. Click the "Apply" button.

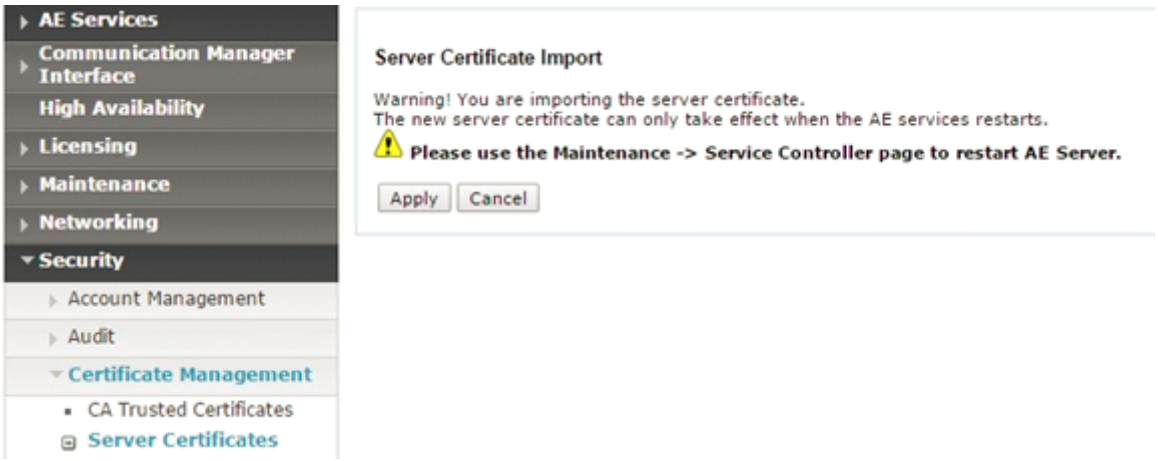


4. Select Choose file, Establish Chain of Trust and Certificate Alias.

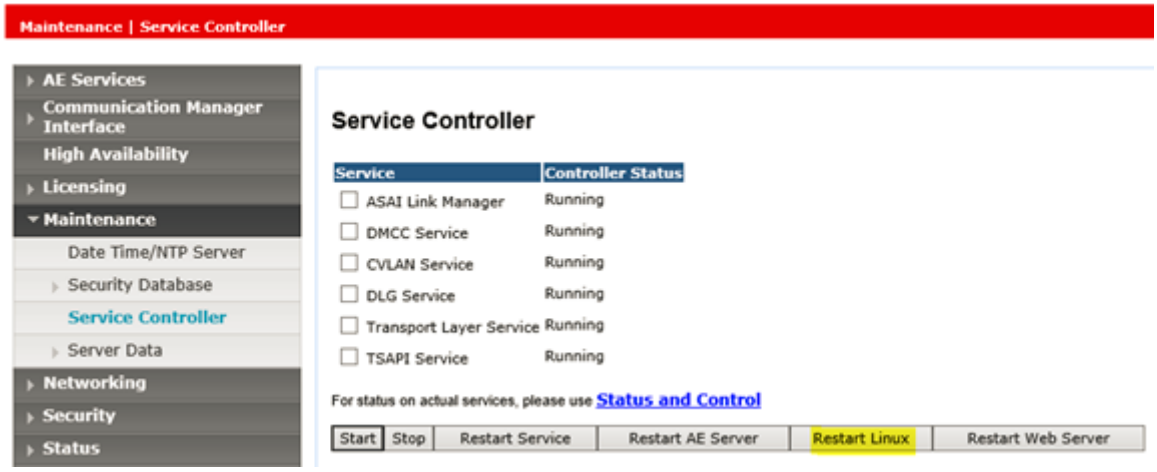


5. Enter the PKCS12 password (from the End Entity) and select Apply and then on the next page Apply again.





6. Restart the Linux server.



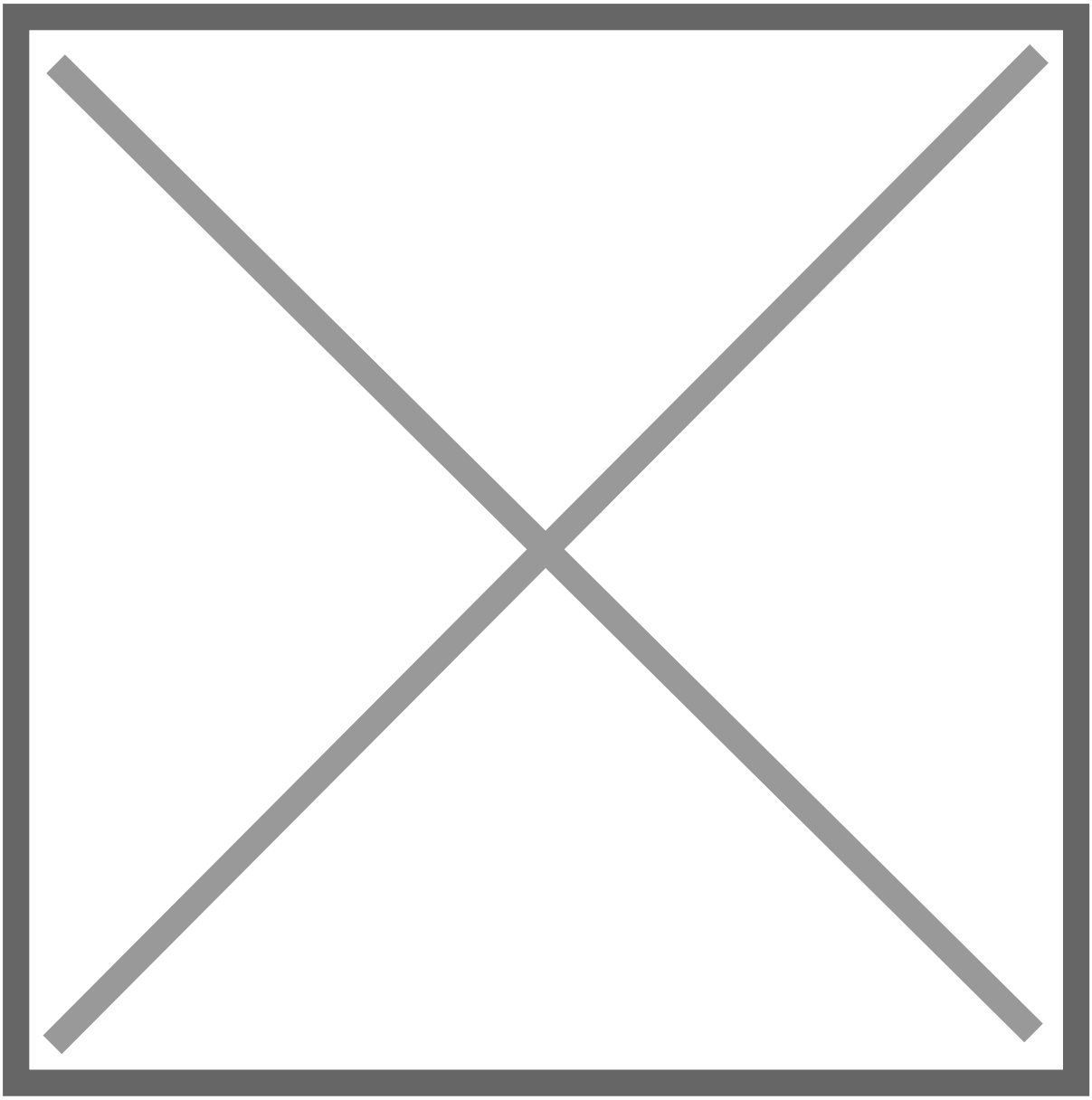
Troubleshooting

Troubleshooting

AES - TSAPI logging

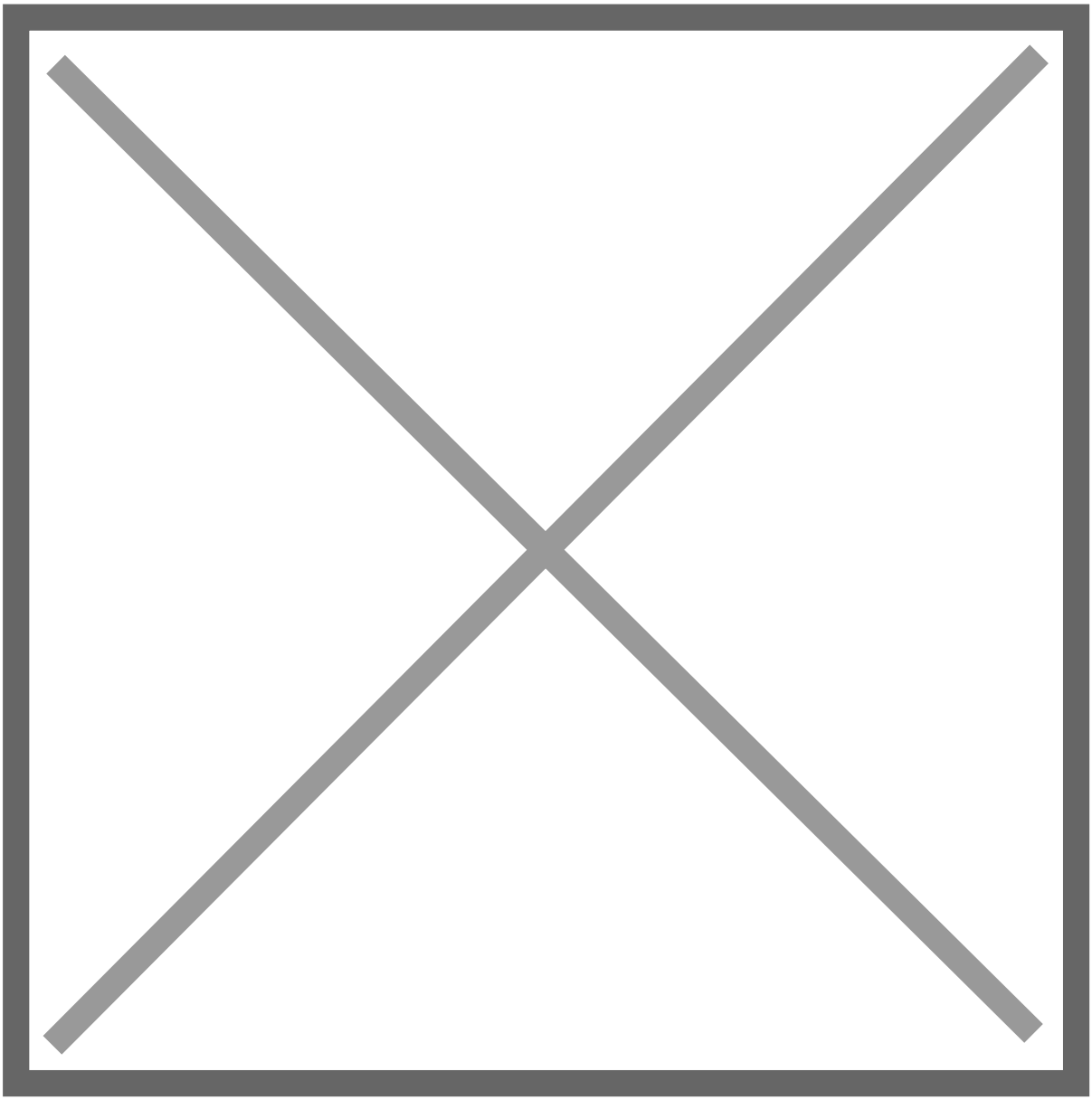
In the last entry we worked with AES, CM and TSAPI cti links, this entry will be short but we will show how to locate AES logs and how to enable TSAPI debugging.

Logs can be seen using the web page navigate to **Status -> Logs -> Error Logs**:



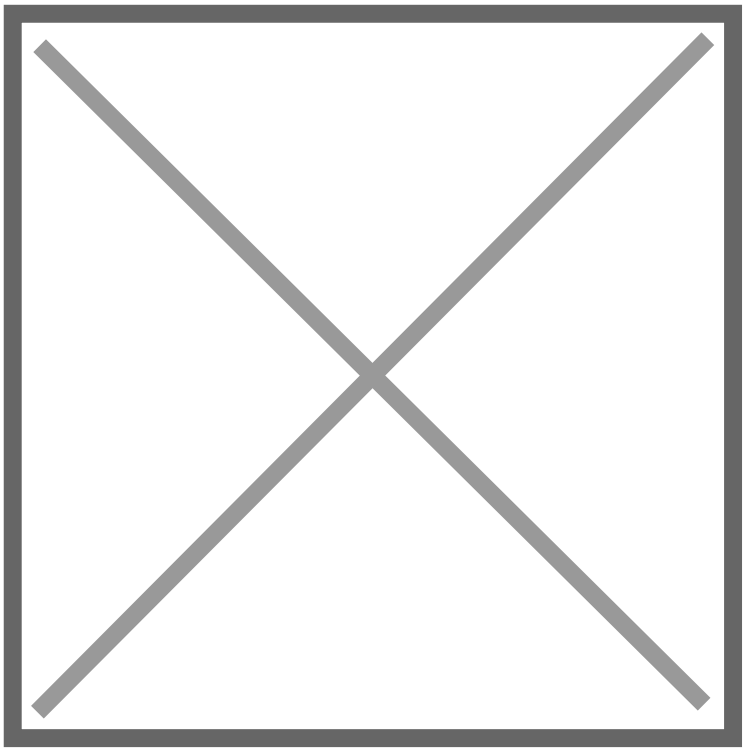
They can be checked one by one or do a download to your PC, but logs can also be located in:

/var/log/avaya/aes/

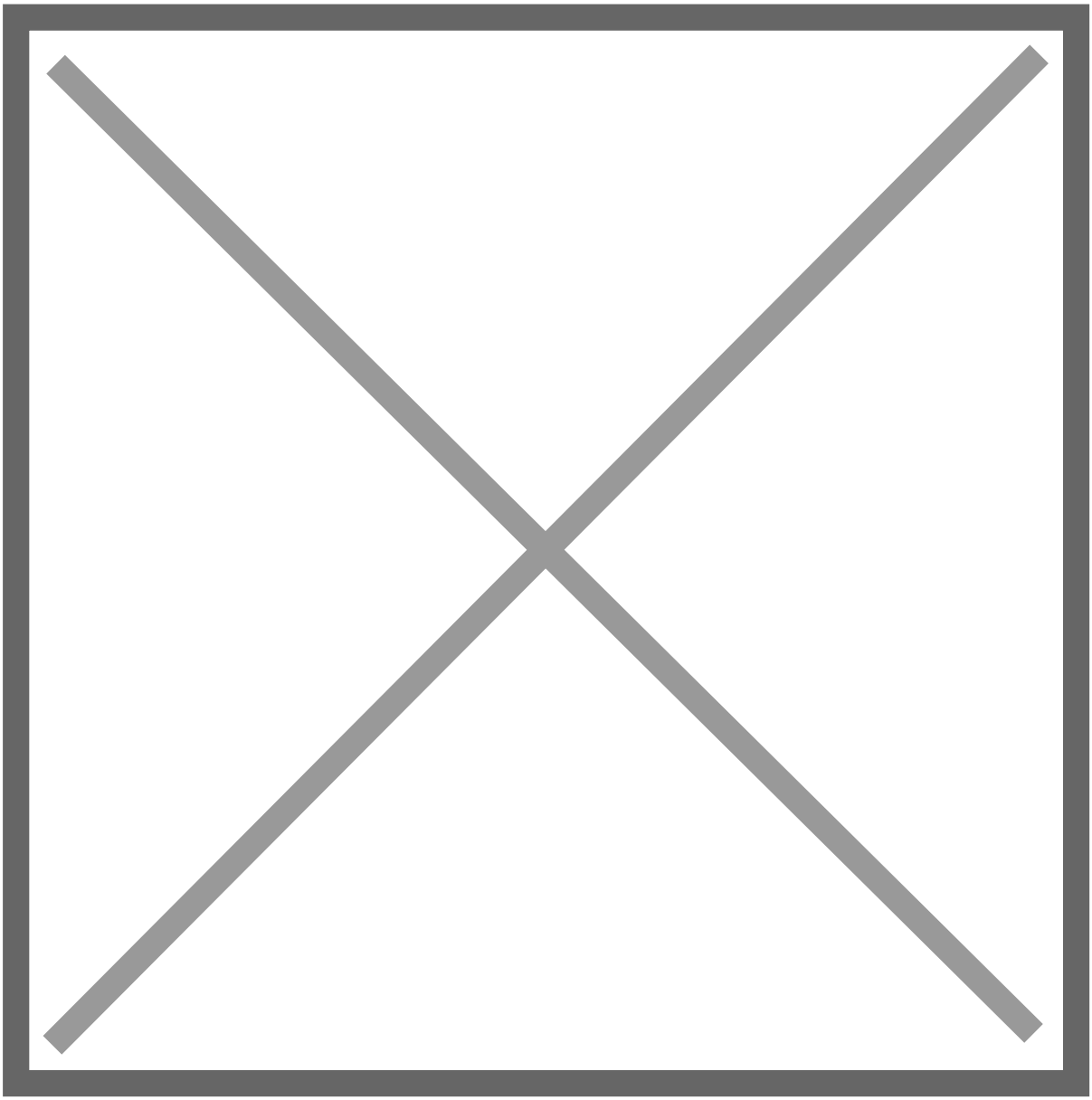


Sometimes it’s useful enabling debugging for TSAPI, the best way to do it is:

Status -> Log Manager -> Trace Logging Levels -> TSAPI Service -> Everything on

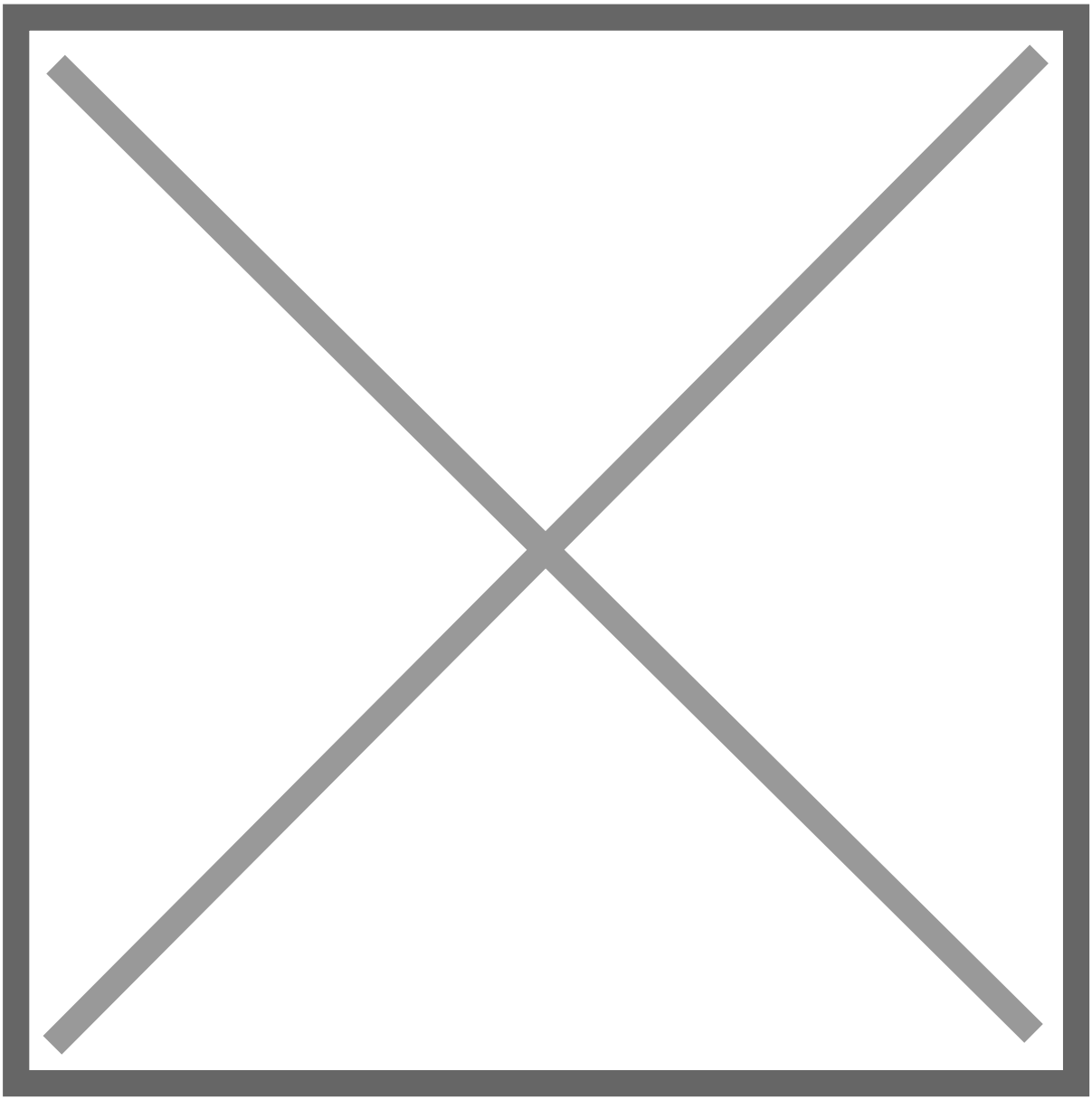


When enabled a new folder is created in the path ***/var/log/avaya/aes/TSAPI*** lets make a TSAPI Test using the web page but typing the wrong password:

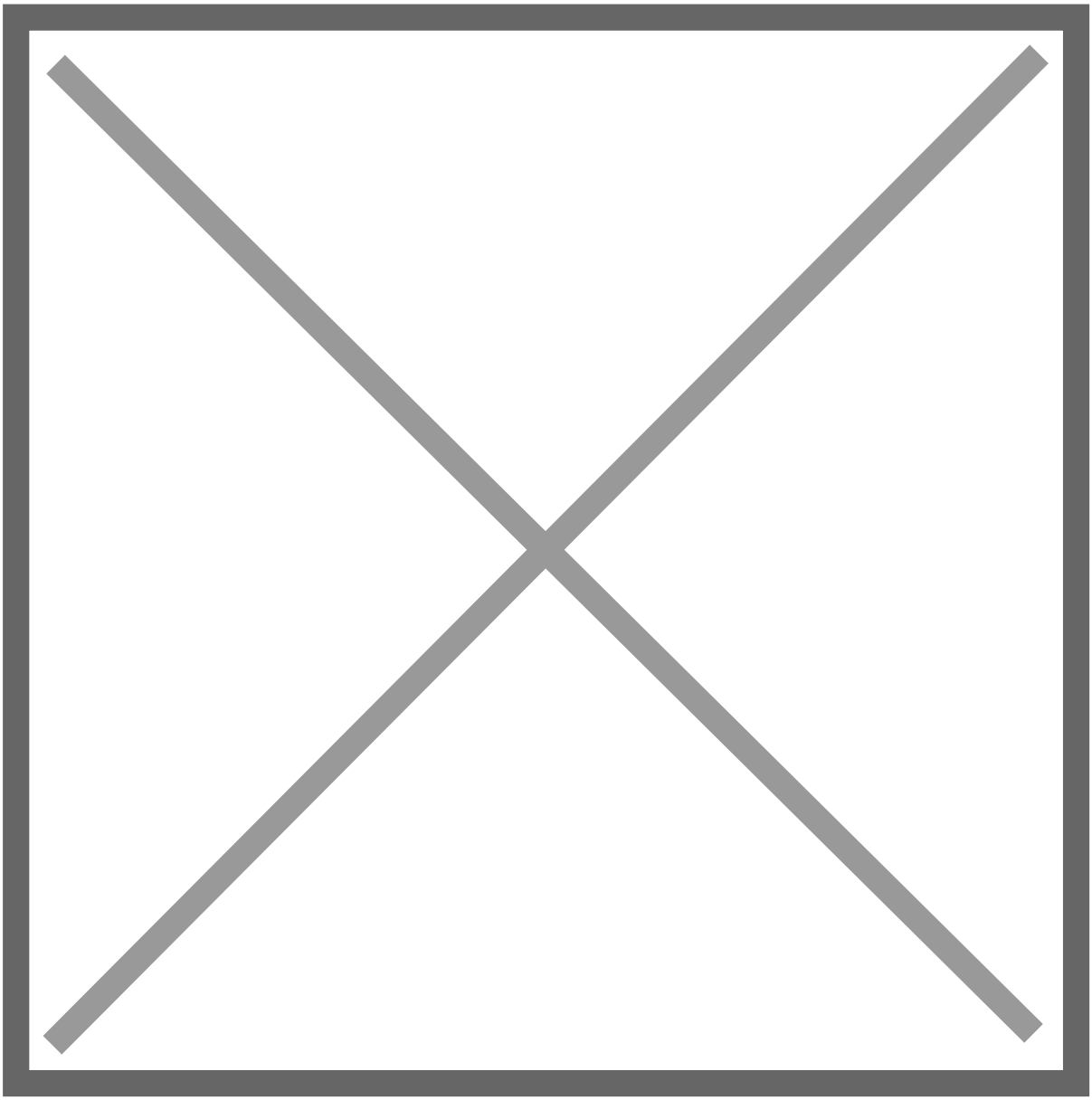


Now lets verify the logs (TSAPI Service log is set to disabled now):

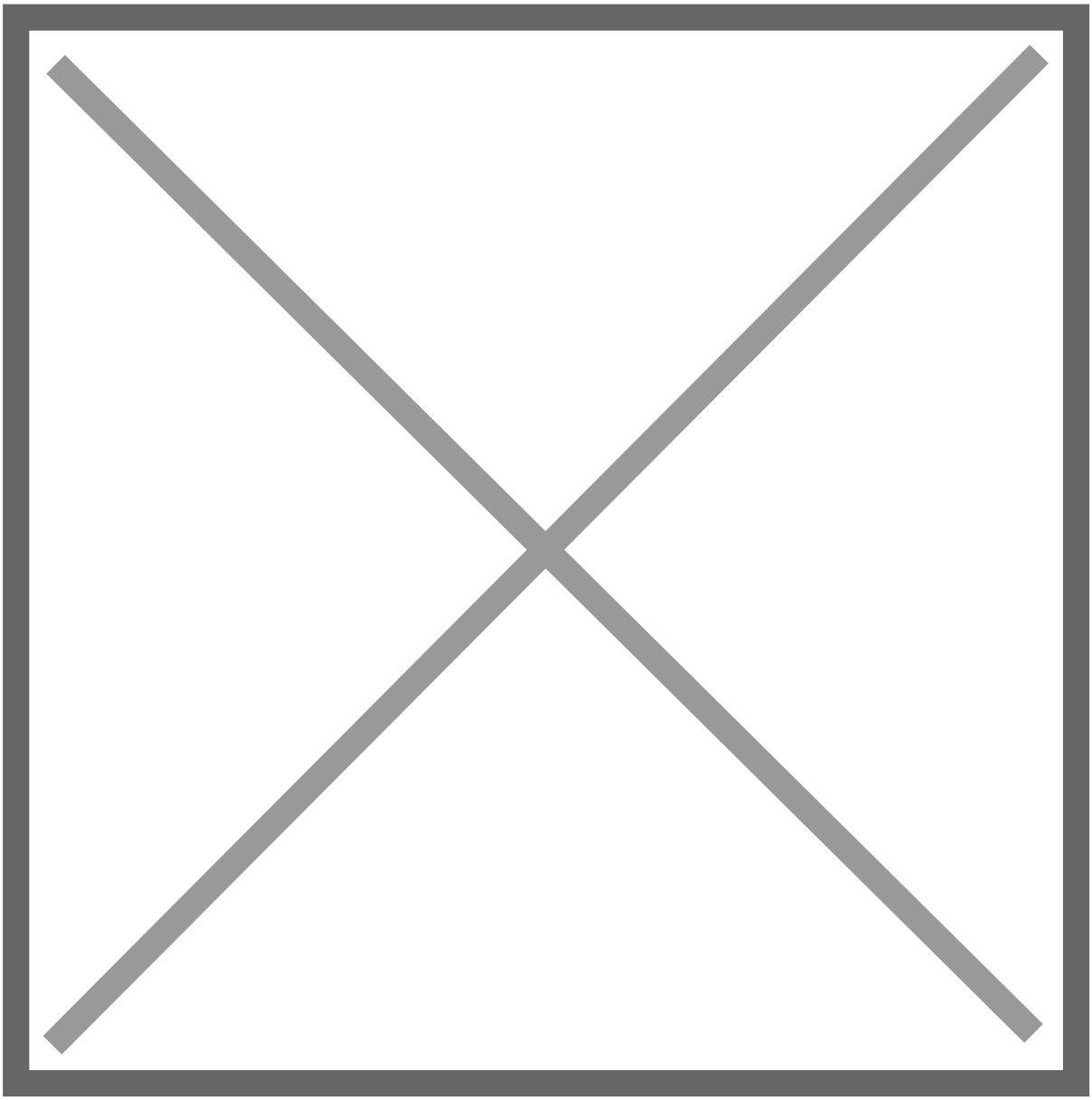
The first thing to notice is that there is a new folder



There are two types of logs generated one for the communication to the CM and a different one for the 3rd party application:



As the password was set incorrectly lets verify the csta_trace.out log and look for that error:



Source: https://whereismyvoicepacket.com/aes-logging/

Troubleshooting

AES - useful commands

Here is a list of useful commands in Avaya AES.

Checking services

```
service aesvcsSpiritAgent status
service subagent1 status
service subagent2 status
service snmpd status

systemctl status aesvcsSpiritAgent
systemctl status subagent1
systemctl status subagent2
systemctl status snmpd
```

Information

```
swversion
cat /etc/os-release
uname -r
df -h
hostname
who
reboot
shutdown -r now
```

Networking info

```
ifconfig
route -n
iptables -L --line-numbers
netstat -nao | grep 8443
netstat -plnt | grep 0.0.0.0
/opt/mvap/bin/netconfig
```

Administration

```
wget https://x.x.x.x:8443
cat /etc/hosts
cat /etc/hosts.allow
cat /etc/hosts.deny
find / -iname sms_test.php
```

Important file/folders

```
ls /var/log/avaya/aes/
cat /var/lib/net-snmp/snmpd.conf
vi /opt/mvap/conf/javaManager.properties
ls /opt/coreservices/avaya/certs/ -ltr
cat /opt/coreservices/certmgmt/conf/certmgmt.conf
```

IP Table administration

```
iptables -S | grep 8443
iptables -L --line-numbers
iptables -D INPUT 1
sudo iptables -I INPUT 1 -p tcp -s 10.191.33.168 --dport 8443 -j ACCEPT
```

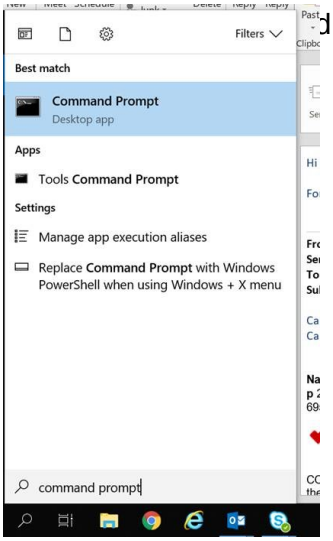
Source: https://whereismyvoicepacket.com/avaya-aes-admin-task-useful-commands/

Troubleshooting

Retrieve CTI desktop log from agent machine

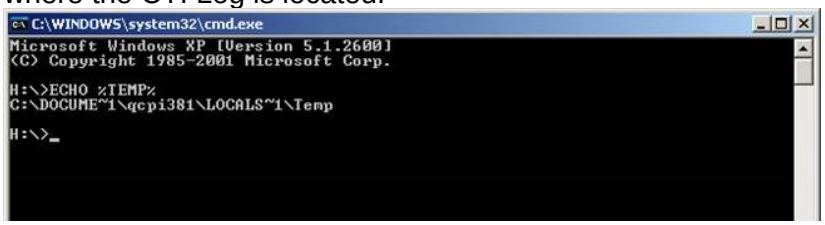
“Retrieve the CTI desktop log from agent machine.”

There is a CTI log that gets saved on the Agent’s machine that dumps a trace of CTI activity.? This log can help in determining login issues or connection issues and may explain why the agent either cannot login or does not see the CTI pop-up.



d Prompt and select it.

When you get the black screen, enter “ECHO %TEMP%”. This will provide the path to the temporary folder where the CTI Log is located.



Open Windows Explorer and follow the path shown in the black screen to find the file “JavaCTIClient.log”

NOTE: The App Data folder may be a hidden folder and the rep may not be able to see it. If they can't see it, see instructions below.

To view hidden files and?folders in Windows 7

1.????? Select the Start button, then select Control Panel > Appearance and Personalization.?
2.????? Select?**Folder**?Options, then select the View tab.?
3.??????? Under Advanced settings, select Show hidden files,?**folders**, and drives, and then select OK.

To view hidden files and?folders?in?Windows 10

1.????? Open File Explorer from the taskbar.?
2.????? Select View > Options > Change?**folder**?and search options.?
3.??????? Select the View tab and, in Advanced settings, select?**Show**?hidden files,?**folders**, and drives and OK.

Lab

Lab

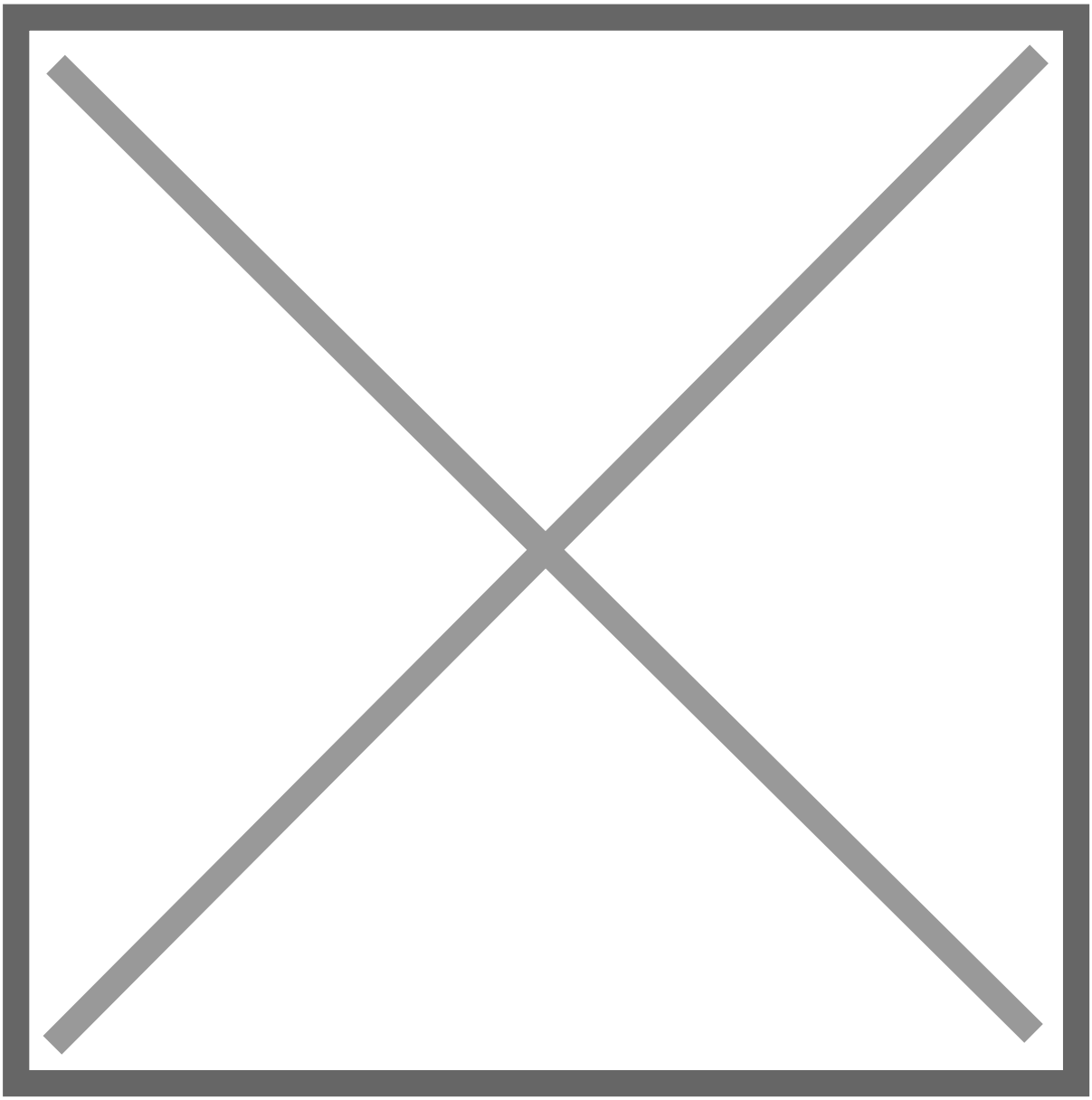
Avaya AES - TSAPI CTI link basic testing

In a previous entry we integrated Application Enablement Services and Communication Manager setting up a TSAPI CTI link to be used by a 3rd party software.

In this entry we will work creating a new TSAPI user that will be used for external applications (we will integrate Verint application in a future entry), but in the meantime we will test that user using 2 methods.

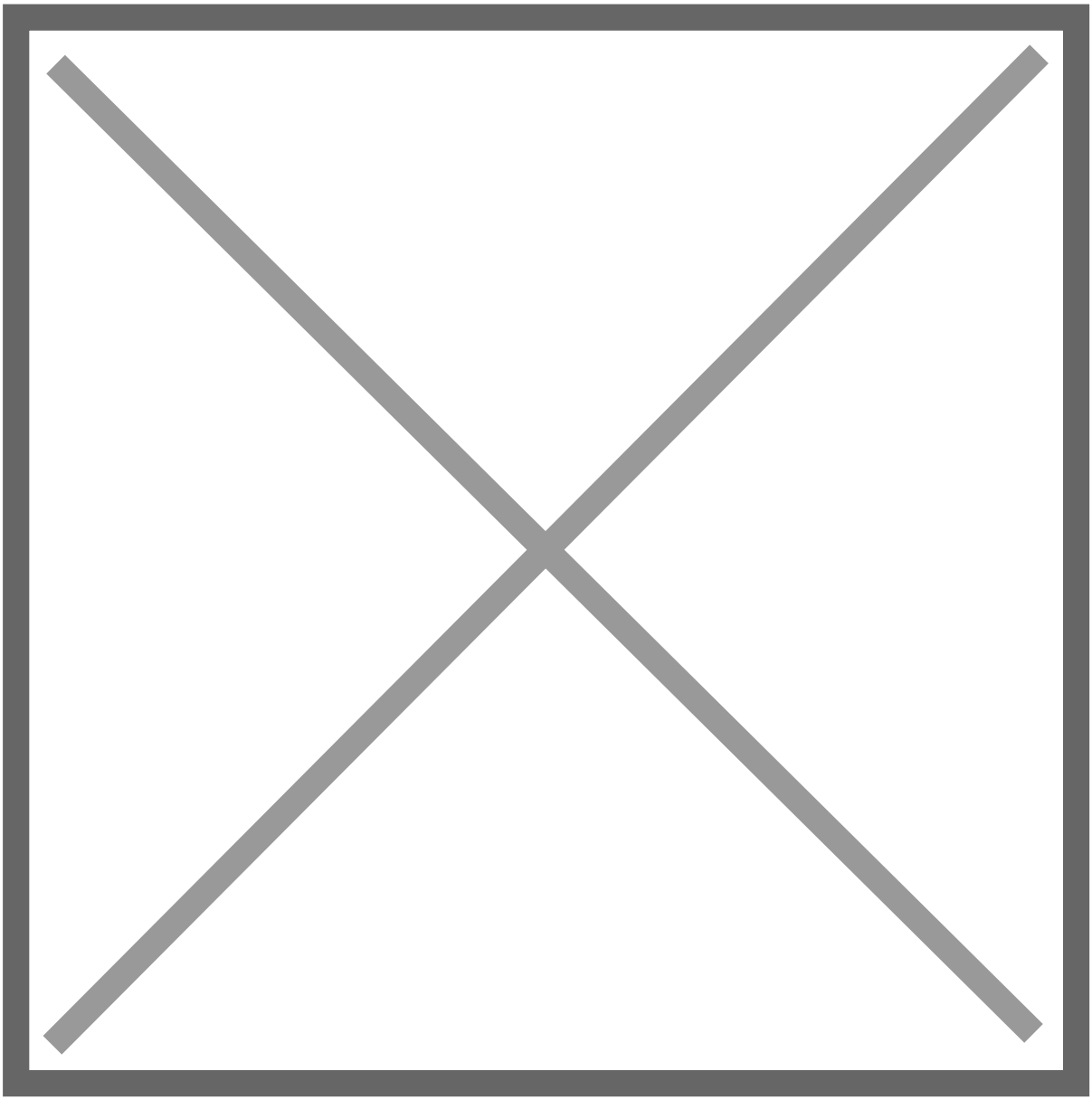
Log in into the AES server and navigate to:

User Management -> User Admin -> Add user

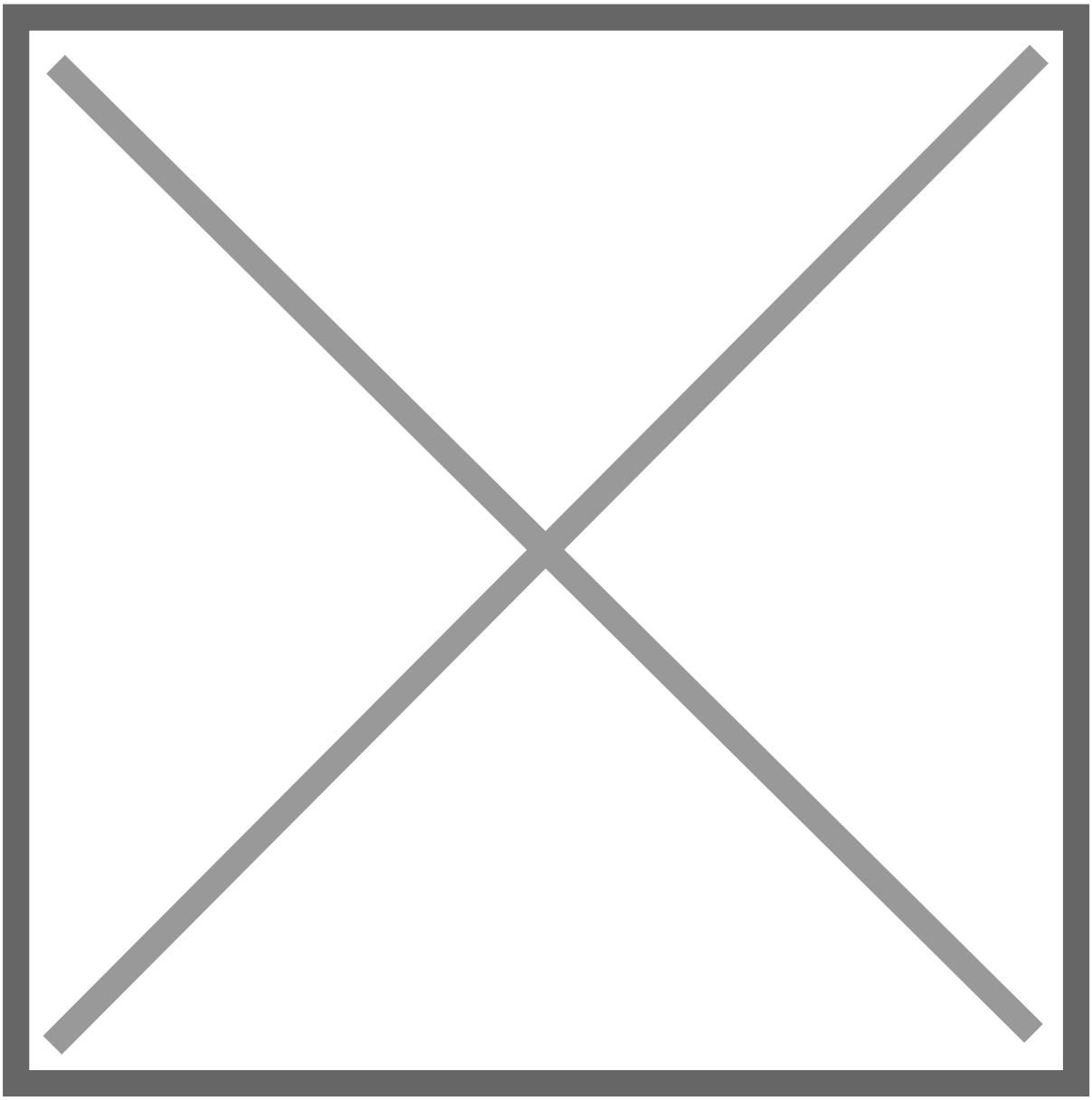


Make sure the *CT User* option is set to Yes.

Now with the user created, lets change the permissions to set ctitsapi to be able to access any element in the Avaya CM, navigate to **Security -> Security Database -> CTI Users -> List All Users** and click on the *Edit* button:

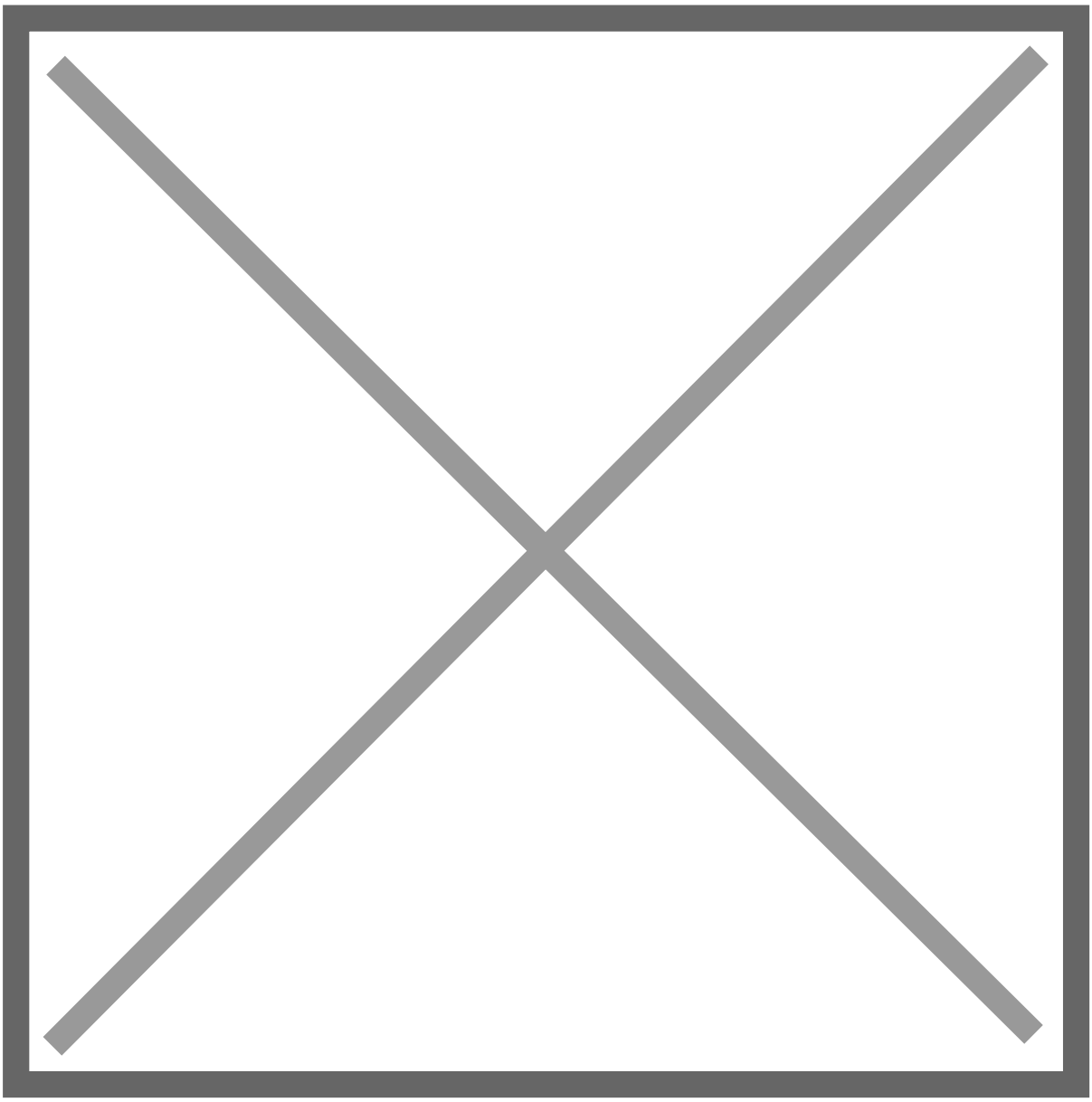


Enable Unrestricted Access option:

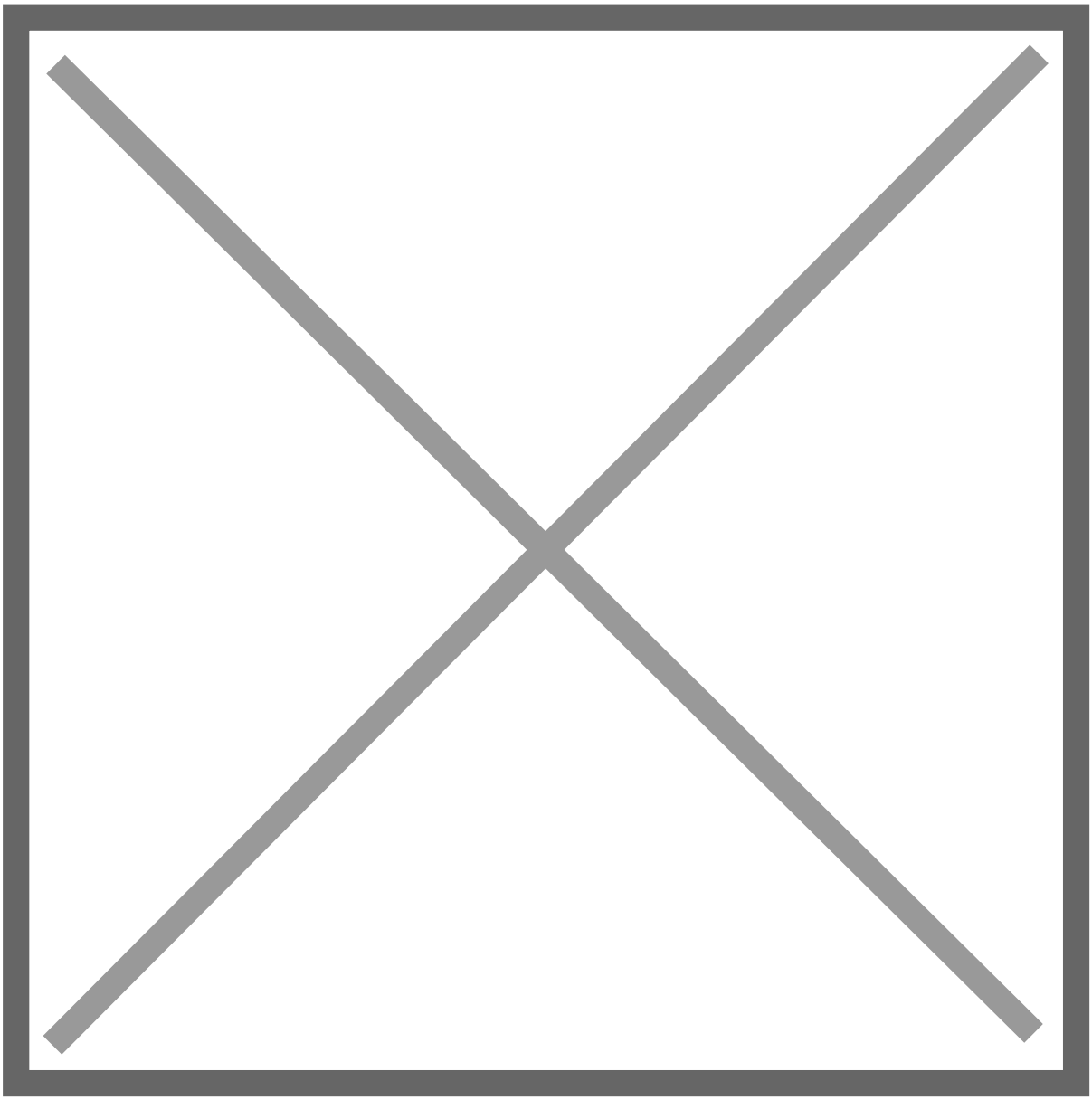


Its now time to test, as mentioned before, we will use 2 methods:

1. Testing locally using, navigate to Utilities -> Diagnostics -> TSAPI Test:

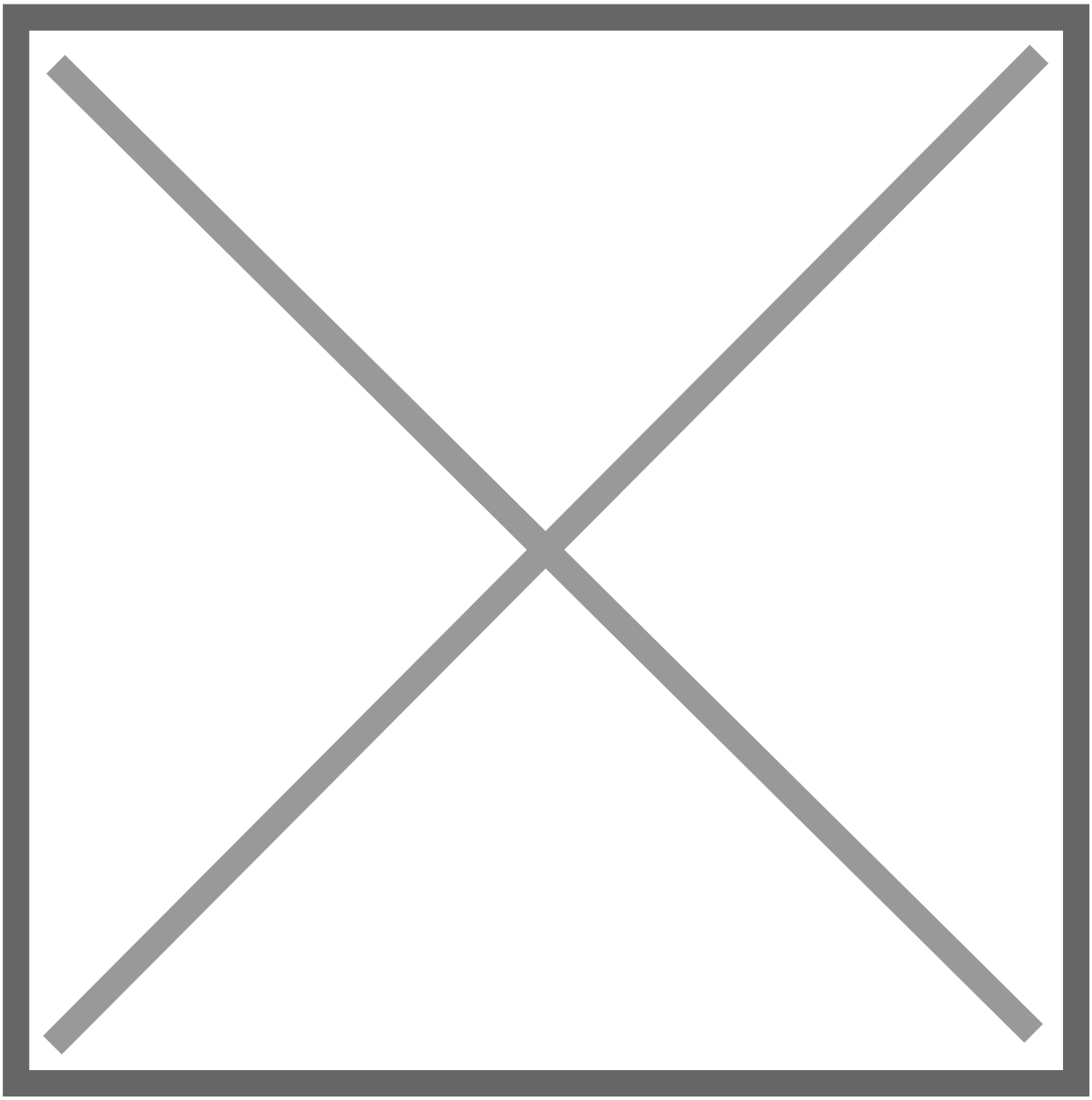


Type the user y password created in the previous step and fill out a valid and registered extension in the from field and use other station, VDN or hunt group (I used the voicemail hunt group), if everything is fine you will see a successful message like this one:

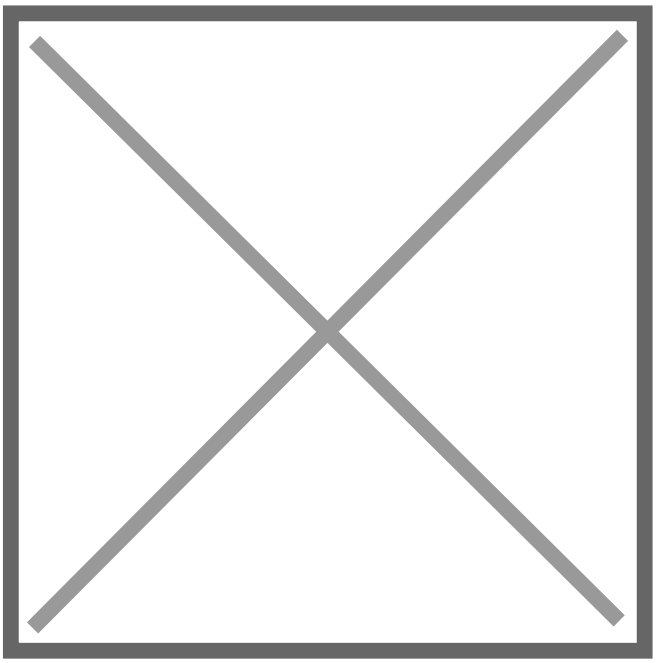


2. The second option to perform a test is using the official client provided by Avaya in the web portal:

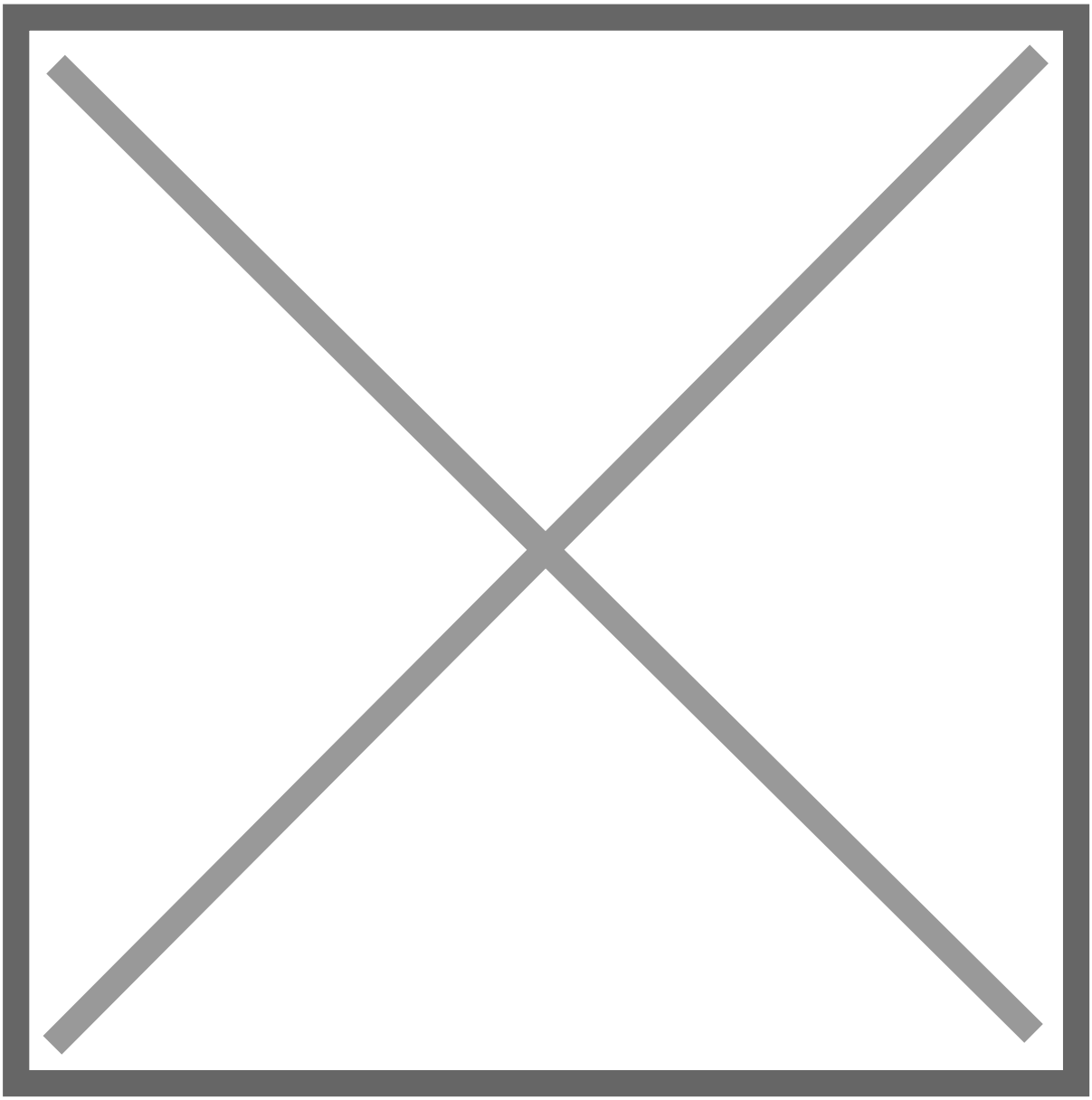
Download and install the TSAPI client application from Avaya Support.



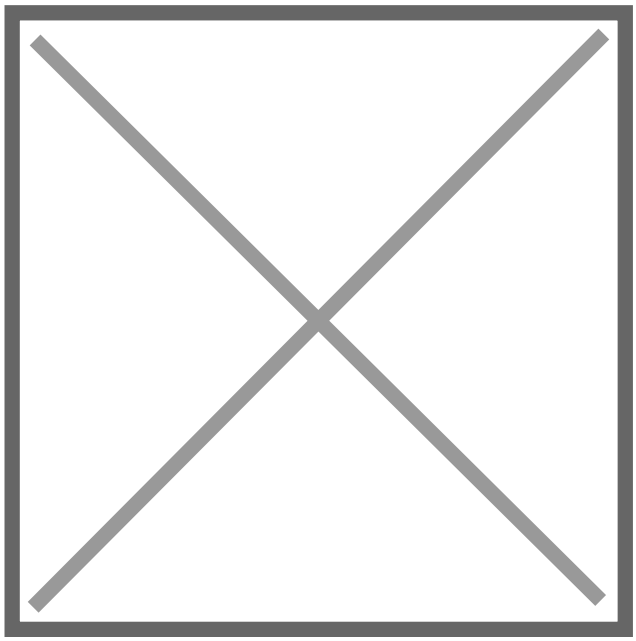
After the software is installed edit TSLIB.INI



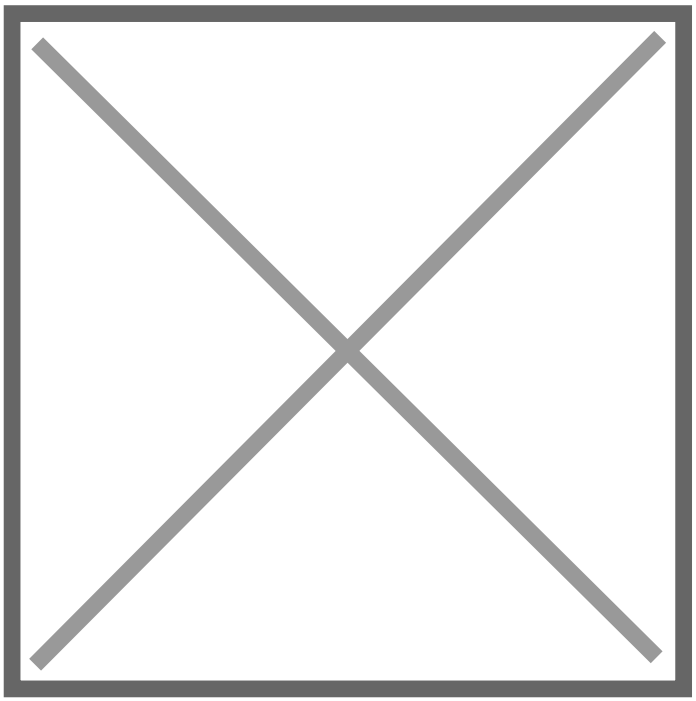
Add a new line/edit the following with the IP address of the AE Server:



After completed, open the TSAPI Test:



Fill out all the information again (server in the top is populated automatically) and click Dial, if successful you should get a message like the following:



Source: https://whereismyvoicepacket.com/aes-tsapi-test/