



# **Avaya Aura<sup>®</sup> Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide**

Release 10.2.x  
Issue 1  
December 2023

© 2015-2023, Avaya LLC  
All Rights Reserved.

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

## Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

## Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

## Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

## Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

## Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

## Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

## Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

## Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

# Contents

<b>Chapter 1: Introduction</b> .....	5
Purpose.....	5
TSAPI and CVLAN backward compatibility.....	5
<b>Chapter 2: Installation Prerequisites</b> .....	7
Download location for clients and SDKs.....	7
Checklist for downloading client and SDKs.....	7
Downloading software from Avaya PLDS.....	7
Downloading TSAPI clients.....	8
Downloading clients and SDKs from Avaya Support.....	8
Downloading clients from Avaya DevConnect.....	9
Checklist for installing the TSAPI client.....	10
<b>Chapter 3: AE Services TSAPI clients and SDKs installation</b> .....	11
TSAPI client and SDK system requirements and compatibility matrix.....	12
Installing the TSAPI Windows client.....	13
Accessing the TSAPI Windows client desktop components.....	16
Verifying the TSAPI Windows client installation.....	17
Using TSAPI Spy while running TSAPI Test.....	18
Removing the TSAPI Windows client.....	18
Removing the TSAPI Windows client.....	18
Installing and configuring the TSAPI Linux Client.....	28
Installing the TSAPI Linux client.....	28
Customizing the Linux client configuration file.....	30
TSAPI Links (Tlinks).....	40
Port settings for a firewall administration.....	41
Installing and managing the TSAPI Windows SDK.....	41
AE Services TSAPI SDK and the programming environment.....	41
Installing the TSAPI Windows SDK.....	41
Viewing the TSAPI Windows SDK Components.....	43
Removing the TSAPI Windows SDK.....	43
Removing the TSAPI Windows SDK from a Windows system.....	43
TSAPI Windows SDK upgradation.....	44
Installing and managing the TSAPI Linux SDK.....	44
Installing the TSAPI Linux SDK.....	44
Removing the TSAPI Linux SDK.....	45
Upgrading the TSAPI Linux SDK.....	45
<b>Chapter 4: AE Services CVLAN Client installation</b> .....	46
The CVLAN Client.....	46
CVLAN client and certificate management.....	47
CVLAN client system requirements and compatibility matrix.....	48

Installing and managing CVLAN Windows client.....	49
Installing the CVLAN Windows Client.....	49
Upgrading the CVLAN Windows Client.....	50
Removing the CVLAN Windows Client.....	50
Installing and managing CVLAN Linux Client.....	50
Installing the CVLAN Linux Client.....	50
Upgrading the CVLAN Linux Client.....	51
Removing the CVLAN Linux Client.....	51
The ASAI test utility.....	52
Using the ASAI test utility.....	52
<b>Chapter 5: Resources</b> .....	54
Application Enablement Services documentation.....	54
Finding documents on the Avaya Support website.....	55
Accessing the port matrix document.....	55
Avaya Documentation Center navigation.....	56
Training.....	57
Viewing Avaya Mentor videos.....	57
Support.....	58
Using the Avaya InSite Knowledge Base.....	58
<b>Appendix A: Certificate management</b> .....	60
Server certificate authentication.....	60
Location and usage of Avaya-installed certificate.....	62
Location of your own certificates.....	62
Usage of your own certificate.....	63
AE Services certificate administration.....	64
Checklist for setting up TSAPI and CVLAN - if you use your own certificates.....	65
Client certificate authentication.....	65
Usage of default client keystore location.....	66
Client keystore location and password configuration.....	67
<b>Appendix B: TSAPI Client Message Tracing</b> .....	69
TSAPI Spy - a Windows client message tracing tool.....	69
Overview of the TSAPI Spy for Windows interface.....	69
Creating a trace file.....	72
Trace output.....	74
Client message tracing for Linux-based TSAPI clients.....	75
Enabling message tracing.....	75
About Message Tracing feature.....	75
Trace file examination.....	76
<b>Appendix C: File naming conventions</b> .....	78
File naming conventions.....	78
<b>Glossary</b> .....	80

# Chapter 1: Introduction

---

## Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is intended for people who want to gain a high-level understanding of the product features, functions, capacities, and limitations.

---

## TSAPI and CVLAN backward compatibility

From Release 10.1, AE Services supports the Transport Layer Security (TLS) version 1.3. From AE Services Release 10.1 and later, both TLS 1.2 and TLS 1.3 protocols are enabled by default. The lower level TLS protocols 1.0 and 1.1 are disabled by default and not recommended for use.

### Note:

- TLS version 1.0 and 1.1 are deprecated according to the National Institute of Standards and Technology (NIST) Special Publication 800-52. So, it is recommended to use TLS version 1.2 and/or 1.3 for added security.

This change may cause the older AE Services 8.x clients who are using TLS 1.0 or 1.1 to fail to establish a secure socket connection to the AE Services 10.2 server. To achieve a more secure client or server socket connection, we encourage current client applications to use AE Services 10.2 Client and SDK, where the TLS 1.2 and 1.3 protocols are supported. If upgrading to AE Services 10.2 SDK is not a viable option, an AE Services administrator can enable the TLS 1.1 and/or 1.0 protocol versions using the AE Services management console web interface.

- All four TLS protocol versions can be active at the same time. This allows a gradual migration of current client applications to move towards a more secure TLS protocol over a period of time.

### TSAPI Service

The Telephony Services Application Programming Interface (TSAPI) Server, Release 10.2 is compatible with the following server releases:

- AE Services Release 8.x 32-bit

- AE Services Release 8.x 64-bit

## **CVLAN**

The Call Visor Local Area Network (CVLAN) Client, Release 10.2 is compatible with the following server releases:

- AE Services Release 8.x CVLAN Client

# Chapter 2: Installation Prerequisites

---

## Download location for clients and SDKs

- Avaya Product Licensing and Delivery System (PLDS) website  
<https://plds.avaya.com>
- Avaya Support website (for Avaya customers with maintenance agreements)  
<http://support.avaya.com>
- Avaya DevConnect website (for DevConnect members)  
<http://www.avaya.com/devconnect>

 **Note:**

A fresh install does not have an Avaya signed default certificate.

---

## Checklist for downloading client and SDKs

No.	Task	Notes	✓
1.	Download software from Avaya PLDS.	<a href="#">Downloading software from PLDS</a> on page 7	
2.	Download the CVLAN client, TSAPI client and SDKs.	<a href="#">Downloading clients and SDKs from Avaya Support</a> on page 8	

---

## Downloading software from Avaya PLDS

### Before you begin

Ensure that you are an Avaya customer and you have registered on the Avaya PLDS website at <https://plds.avaya.com>.

### About this task

Use the following procedure to download the TSAPI client and the CVLAN client from the Avaya Product Licensing and Delivery System (Avaya PLDS) website .

The TSAPI client and CVLAN client are available at the Avaya PLDS website , but the TSAPI SDK is not. To get the TSAPI SDK, contact an authorized Avaya Business Partner or an Avaya Account Executive.

### Procedure

1. In your web browser, type <https://plds.avaya.com> .
2. On the LOGIN NOW page, type your email address and password, and click **SUBMIT** .
3. On the Home page, click **Assets > View Downloads** .
4. On the **Search by Download** tab, do the following:
  - a. In the **Company name** field, enter the name of your company.
  - b. In the **Application** field, click **Application Enablement Services** .
  - c. In the **Download Type** field, click **Software Downloads** .
  - d. In the **Version** field, click the current release.
5. Click **Search Downloads** .
6. In the **Software Downloads** list, find the appropriate download, and click **Download** .
7. On the About Download Manager page, click **Click to download your file now** .

#### **Note:**

The first time that you use the Download Manager, the browser prompts you to install Download Manager. Click **Install** and complete the procedure to install Download Manager.

8. Click **Exit** to exit Avaya Download Manager. Your browser displays the PLDS Downloads page. The system displays a check mark next to the software that you downloaded.
9. Click **Log out** .
10. Close your browser.
11. For Windows clients, go to the folder that you specified in the Save as dialog box, and extract from the zip file.

---

## Downloading TSAPI clients

### Downloading clients and SDKs from Avaya Support

#### About this task

Use the following procedure to download the TSAPI client from the Avaya Support Web site at <http://support.avaya.com>. This procedure considers that you are an Avaya customer and you have registered on the Avaya Support Web site.

**\* Note:**

The TSAPI client is available from the Avaya Support Site, <http://support.avaya.com>, but the TSAPI SDK is not. To get the TSAPI SDK, contact an authorized Avaya Business Partner or an Avaya Account Executive.

## Procedure

1. Log in to the Avaya Support Web site, <http://support.avaya.com>
2. On the Welcome to Avaya Support page, click **Support by Product > Downloads**.
3. In the **Enter Your Product** field type Application Enablement Services
4. In the **Choose Release** menu, select 10.2.
5. In the **Downloads** list, click one of the following:
  - Avaya Aura® Application Enablement Services TSAPI 32-bit Client Windows 10.2.x
  - Avaya Aura® Application Enablement Services TSAPI 64-bit Client Windows 10.2.x
  - Avaya Aura® Application Enablement Services TSAPI 32-bit Client Linux for RHEL 7.x, 8.x
  - Avaya Aura® Application Enablement Services TSAPI 64-bit Client Linux for RHEL 7.x, 8.x
  - Avaya Aura® Application Enablement Services CVLAN Client Windows 10.2.x
  - Avaya Aura® Application Enablement Services CVLAN Client Linux for RHEL 7.x, 8.x
6. On the Downloads page, click the file name, for example `tsapi-client-win32-10.2-xx.zip` for TSAPI 32-bit Client or `tsapi-client-x86_64-10.2-xx.zip` for TSAPI 64-bit Client, where xx represents the build number.
7. Save the file to your computer.

For Windows clients, extract the .zip file in a separate folder on your computer.

## Next steps

Start the installation

## Downloading clients from Avaya DevConnect

### Before you begin

The following procedure considers that you are an Avaya DevConnect member and that you have registered on the Avaya DevConnect website, <http://www.avaya.com/devconnect>

### About this task

Use the following procedure to download the TSAPI clients from the Avaya DevConnect website, <http://www.avaya.com/devconnect>.

**!** **Important:**

The TSAPI client is available from the Avaya DevConnect website, <http://www.avaya.com/devconnect>, but the TSAPI SDK is not. If you are a Gold or Platinum DevConnect member, you can order the TSAPI SDK through DevConnect. For more information, contact an authorized Avaya Business Partner or an Avaya Account Executive.

**Procedure**

1. Log in to the Avaya DevConnect website, <http://www.avaya.com/devconnect>
2. Click **Downloads**.
3. Click **Telephony Services API (TSAPI)**.
4. Click the arrow after **Programming Resources**, and then select the **Software Development Kits** check box.
5. From the list of results, click one of the following:
  - Avaya Aura® Application Enablement Services TSAPI 32-bit Client Windows 10.2.x
  - Avaya Aura® Application Enablement Services TSAPI 64-bit Client Windows 10.2.x
  - Avaya Aura® Application Enablement Services TSAPI 32-bit Client Linux for RHEL 7.x, 8.x.
  - Avaya Aura® Application Enablement Services TSAPI 64-bit Client Linux for RHEL 7.x, 8.x.
6. Read and accept the license agreement, and then click **Download** .
7. Save the file to your computer. For example `tsapi-client-win32-10.2-xx.zip` for TSAPI 32-bit Client or `tsapi-client-x86_64-10.2-xx.zip` for TSAPI 64-bit Client, where `xx` represents the build number.
8. For Windows clients, extract the `.zip` file in a separate folder on your computer.

**Checklist for installing the TSAPI client**

#	Task	✓
1	Obtain the IP address or Host Name of the AE Services server from the AE Services administrator.	
2	Check whether the TSAPI links are encrypted.	
3	Check whether the default CA certificate is being used for encryption.	
4	Check whether alternate TSAPI links are administered. If alternate TSAPI links are administered, you should configure the alternate Tlinks after the installation.	

**\* Note:**

If the TSAPI links are encrypted, and the default CA certificate is not being used, you will need to supply and configure the appropriate CA certificate on the client.

# Chapter 3: AE Services TSAPI clients and SDKs installation

This chapter describes the installation process for Avaya Aura® Application Enablement Services (AE Services) Telephony Services Application Programming Interface (TSAPI) clients and software development kits (SDKs). For TSAPI applications to run in AE Services or Communication Manager environment, you must install the TSAPI client.

A fresh install does not have an Avaya signed default certificate. A self-signed certificate is created during install time that can be used as a default certificate for testing purposes. AE Services servers upgraded to version 10.2.x will retain the default certificate for backward compatibility.

The AE Services 10.2.x TSAPI client installation continues to install the default certificate. This is so that 10.2.x clients can connect to AE Services servers 7.x and older, as well as servers that have been upgraded to 10.2.x.

 **Note:**

AE Services does not support the following operating systems as Microsoft has ended its support for the following operating systems from January 2020:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2 Standard Edition (applicable for Release 8.1.3 and later)
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Ultimate

# TSAPI client and SDK system requirements and compatibility matrix

**Table 1: TSAPI client and SDK system requirements and compatibility matrix**

TSAPI client and SDK version (file system)	Microsoft Windows version (file system)	Linux Version (file system)	AES Version
10.2 (64-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows 11 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2022 Standard Edition (64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux version 8.4 and later (64-bits)</li> <li>• Red Hat Enterprise Linux version 7.6 and later 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• 10.x</li> <li>• 8.x</li> </ul>
10.2 (32-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows 11 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2022 Standard Edition (64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux version 8.4 and later (64-bits)</li> <li>• Red Hat Enterprise Linux version 7.6 and later 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• 10.x</li> <li>• 8.x</li> </ul>
10.1 (64-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows 11 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2022 Standard Edition (64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux version 8.4 and later (64-bits)</li> <li>• Red Hat Enterprise Linux version 7.6 and later 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>• 10.x</li> <li>• 8.x</li> </ul>

*Table continues...*

TSAPI client and SDK version (file system)	Microsoft Windows version (file system)	Linux Version (file system)	AES Version
10.1 (32-bits)	<ul style="list-style-type: none"> <li>Microsoft Windows 10 Professional Edition (64-bits)</li> <li>Microsoft Windows 11 Professional Edition (64-bits)</li> <li>Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>Microsoft Windows Server 2019 Standard Edition (64-bits)</li> <li>Microsoft Windows Server 2022 Standard Edition (64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux version 8.4 and later (64-bits)</li> <li>Red Hat Enterprise Linux version 7.6 and later 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>10.x</li> <li>8.x</li> </ul>
8.1.3 and later (64-bits)	<ul style="list-style-type: none"> <li>Microsoft Windows 10 Professional Edition (64-bits)</li> <li>Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>Microsoft Windows Server 2019 Standard Edition (64-bits)</li> </ul>	Red Hat Enterprise Linux version 7.6 and later 64-bits)	<ul style="list-style-type: none"> <li>8.x</li> </ul>
8.1.3 and later (32-bits)	<ul style="list-style-type: none"> <li>Microsoft Windows 10 Professional Edition (32-bits and 64-bits)</li> <li>Microsoft Windows Server 2012 R2 Standard Edition (32-bits and 64-bits)</li> <li>Microsoft Windows Server 2016 Standard Edition (32-bits and 64-bits)</li> <li>Microsoft Windows Server 2019 Standard Edition (32-bits and 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux version 7.6 and later (64-bits)</li> <li>Red Hat Enterprise Linux version 6.10 (32-bits and 64-bits)</li> </ul>	<ul style="list-style-type: none"> <li>8.x</li> </ul>

**\* Note:**

TSAPI client and SDK 32-bit and 64-bit version supports Visual Studio 2015. For more information about the compatibility matrix with the binary and library files, refer Microsoft documentation.

## Installing the TSAPI Windows client

### Before you begin

If you are upgrading from the Avaya Computer Telephony (Avaya CT) TSAPI Windows (TS Win32) client to the Avaya Aura® Application Enablement Services TSAPI Windows 32-bit or 64-bit client, you must remove the Avaya CT TS Win32 client before you install the Avaya Aura® Application Enablement Services TSAPI Windows client.

 **Note:**

You must uninstall the previous version of the Avaya Computer Telephony (Avaya CT) TSAPI Windows client from your system before installing the new version.

### About this task

Use the following procedure to install the TSAPI Windows client.

 **Note:**

Use the network drive-based installation procedure to install a significant number of TSAPI Windows clients. For information about network-based installation and setting up configuration files (`tslib.ini`), see [Customizing the `tslib.ini` file before installation](#).

 **Important:**

Ensure you complete the instructions for downloading and saving the installation files to your computer. For more information, see [Downloading software from PLDS](#).

### Procedure

1. Log on to your computer as a user with administrator permission or any equivalent permissions.
2. Go to the directory containing the TSAPI Windows client files you downloaded, and double-click **setup.exe**.

Setup displays the Welcome dialog box.

3. Click **Next**.

Setup searches for any older versions of the TSAPI client.

- If setup detects the Avaya CT TS Win32 client, it issues the following warning:

```
The Avaya CT Win 32 Client needs to be uninstalled before the
installation can continue.
```

Click **OK**, to exit the installation program.

- If setup detects an earlier, incompatible version of the Avaya Aura® Application Enablement Services TSAPI client, it displays a dialog box with the message:

```
Setup has detected an older version of the Avaya Aura
Application Enablement Services TSAPI Client on your system.
This version needs to be removed before the installation can
continue. Would you like Setup to remove this version for you
now?
```

Click **Yes** to remove the earlier version of the TSAPI client software automatically. Your existing TSAPI client configuration settings is preserved.

After completing the search, the setup displays the License Agreement dialog box.

4. Carefully review the license agreement. Select **I accept the terms of the license agreement**, and then click **Next**. Setup displays the Choose Destination Location dialog box.

5. Click **Next** to accept the default destination folder. The default destination folder for TSAPI 32-bit client is C:\Program Files (x86)\Avaya\AE Services\TSAPI Client and the default destination folder for TSAPI 64-bit client is C:\Program Files\Avaya\AE Services\TSAPI Client.

Setup displays the AE Services Server Configuration dialog box.

6. Complete the AE Services Server Configuration dialog box.

The information you specify in this dialog box is saved in the `tslib.ini` file. If you do not have this information, see [Installing the TSAPI Windows client without the hostname and the IP address](#).

- a. In the **Host Name or IP Address** field, type a valid hostname or IP address of the AE Services Server, for example:

192.168.123.44 (IP address)

aeserver1 or aeserver.company.com (host name)

- b. In the **Port Number** field, select the required port among the available ports (450 for unencrypted and 453 for encrypted) from the dropdown. By default, unencrypted port 450 is disabled and encrypted port 453 is enabled. If your installation uses multiple AE Services Server, click **Add to List**.
- c. You can repeat substeps a and b to add multiple host names or IP addresses to the **Configured AE Services Servers** list box.

 **Note:**

If Setup detects a previously installed TSAPI client or a previous `tslib.ini` file, it will display the list of previously configured AE Services Servers (along with the default port) in the Configured AE Services Servers dialog box. If you reuse any of the same AE Services Servers from the list, you can click **Next** to proceed. Otherwise, you can delete the AE Services Servers that are not required.

- d. Click **Next**.

Setup displays the Ready to Install the Program dialog box.

7. Click **Install** to begin the installation.

Setup displays the Setup Status dialog box as it installs files, and then displays the Installation Wizard Complete dialog box.

8. From the Installation Wizard Complete dialog box, click **Finish** to exit the Setup.

## Next steps

Verify that the components in your configuration can communicate. For more information, see [Verifying the TSAPI Windows client installation](#).

## Related links

[Customizing the `tslib.ini` file prior to installation](#) on page 26

[Downloading software from Avaya PLDS](#) on page 7

[Verifying the TSAPI Windows client installation](#) on page 17

## Accessing the TSAPI Windows client desktop components

### Before you begin

Ensure that the TSAPI Windows client is installed.

### About this task

Use this procedure to access AE Services TSAPI Windows client components.

### Procedure

1. On the **Start** menu, click **All Programs > Avaya AE Services > TSAPI Client > TSAPI Test**.
2. Select one of the following:
  - **Edit TSLIB.INI** - The `tslib.ini` file contains configuration information for the TSAPI client. The file is installed with the TSAPI Client installation folder. For Windows-based clients, the configuration file is `TSLIB.INI`. Select **Edit TSLIB.INI** to open the `tslib.ini` file. See, [Editing the TSAPI Windows client configuration file \(tslib.ini\)](#).
  - **TSAPI Spy** - The TSAPI Spy (`TSSPY32.EXE` or `TSSPY64.EXE`) program may be used to obtain a trace of messages flowing between programs and the TSAPI Service. Select the TSAPI Spy to open the TSAPI Spy application. For more information, see [TSAPI Spy - a Windows client message tracing tool](#).
  - **TSAPI Test** - The TSAPI Test program allows you to test your TSAPI Client installation by opening a stream and making a call. Select **TSAPI Test** to open the TSAPI Test program.
  - **TSAPI Client Readme** - `TSAPI Client Readme` file provides information about TSAPI Client installation and TSAPI SDK Client Compatibility. Select `TSAPI Client Readme` to open the `TSAPI Windows Client Readme` file.
  - **OpenSSL License** - Open the `OpenSSL License` file to review the terms of the license. Select **OpenSSL License** to open the `OpenSSL License` file.
  - **Apache Software Foundation License** - The TSAPI Spy program includes software developed by the Apache Software Foundation. Select **Apache Software Foundation License** to open the `Apache Software Foundation License` file.
  - **Apache Software Foundation Notice** - This file describes the software components developed by the Apache Software Foundation that are included with the TSAPI Spy application. Select **Apache Software Foundation Notice** to open the `Apache Software Foundation Notice` file.

### Related links

[Editing the TSAPI Windows client configuration file](#) on page 19

[TSAPI Spy - a Windows client message tracing tool](#) on page 69

## Verifying the TSAPI Windows client installation

### About this task

After you have installed the TSAPI Windows client, use **TSAPI Test** to verify that the components in your configuration can communicate. Use this procedure to run the TSAPI Test application.

### Procedure

1. Click on **Start > All Programs>Avaya AE Services>TSAPI Client>TSAPI Test** Windows opens the TSAPI Test application.
2. Complete the TSAPI Test Application dialog box as follows:
  - a. In the **Server** field, select the tlink that corresponds to the AE Services Server and Avaya Aura<sup>®</sup> Communication Manager that you want to test. Tlinks are names that the TSAPI Service assigns to the TSAPI CTI links between the AE Services Server and Avaya Aura<sup>®</sup> Communication Manager.
  - b. In the **User** field, type your CT User user ID.

 **Note:**

A CT User is a person or an application administered in the AE Services User database with the CT User field set to yes. CT User authorization is controlled by the AE Services Security Database.

- c. In the **Password** field, type your CT User password.
- d. In the **From** field, under **Make Telephone Call**, type a phone number that is administered in Avaya Aura<sup>®</sup> Communication Manager.

 **Note:**

If the Security Database is enabled for the TSAPI Service, the CT User entered in step 2b must have permission in the AE Services Security Database to control this phone number.

- e. In the **To** field, under Make Telephone Call, type a second phone number that is administered in Avaya Aura<sup>®</sup> Communication Manager.
- f. Click **Dial**. If the call is successful TSAPI Test displays a message box with the message: Call successfully originated. Dismiss this message box to terminate call.

 **Note:**

- If the call fails, TSAPI Test displays a message box with the message:  
acsOpenStream() failed: Unable to make secure connection to server (-15). This error can occur when connecting to an AE Services 10.2.x server with TLS 1.2 or 1.3 enabled, and the version of TSAPI client does not support TLS 1.2 or 1.3.

- If a call is not successful, TSAPI Test displays a message box with a message that indicates the reason for failure. See [Using TSAPI Spy while running TSAPI Test](#).

g. Click **Close** to exit TSAPI Test.

#### Related links

[Using TSAPI Spy while running TSAPI Test](#) on page 18

## Using TSAPI Spy while running TSAPI Test

### About this task

If your call fails while you are running TSAPI Test, use TSAPI Spy to monitor the activity between the AE Services Server and the client running TSAPI Test. For more information about TSAPI Spy, see Appendix B TSAPI Client Message Tracing. Use this procedure to monitor your call with TSAPI Spy.

### Procedure

1. On the **Start** menu click **All Programs > Avaya AE Services > TSAPI Client > >TSAPI Spy** Windows opens the TSAPI Spy application.
2. See [Verifying the TSAPI Windows client installation](#) to perform the procedure and monitor the activity between the AE Services TSAPI Service and TSAPI Test.

#### Related links

[Verifying the TSAPI Windows client installation](#) on page 17

---

## Removing the TSAPI Windows client

### Removing the TSAPI Windows client

#### Procedure

1. Click **Start > Control Panel**.
2. From the Control Panel, click **Programs and Features**.  
The system displays the Uninstall or change a program window.
3. Select **Avaya Application Enablement Services TSAPI Client** and click **Remove**.  
The system displays a confirmation dialog box.
4. Click **Yes**.  
Setup uninstalls the software and displays the Uninstall Complete dialog box.
5. Click **Finish**.

**Note:**

The `tslib.ini` file is not removed from the TSAPI Client installation folder.

## Editing the TSAPI Windows client configuration file

### About this task

You can customize the behavior of TSAPI Windows clients by editing the TSAPI client configuration files. The `tslib.ini` file contains configuration information for the TSAPI client. It is installed with the TSAPI Client installation folder.

### Procedure

1. On the **Start** menu, click **All Programs > Avaya AE Services > TSAPI Client > Edit TSLIB.INI**.
2. Edit the configuration file.

For more information, see TSAPI Windows client configuration file field description.

### Related links

[TSAPI Windows client configuration file field description](#) on page 19

### TSAPI Windows client configuration file field description

Name	Description
<b>Telephony Servers</b>	Use this section to edit the [Telephony Servers] to change the Host Name or IP address of the AE Services Server or to create entries for additional AE Services Servers. Each entry must be in the following format (spaces are not valid in host names): <code>hostname=port_number</code> or <code>IPAddress=port_number</code> . For example: <ul style="list-style-type: none"> <li>• Unencrypted: <code>aeserver.domain.com=450</code> or <code>192.168.123.44=450</code></li> <li>• Encrypted: <code>aeserver.domain.com=453</code> or <code>192.168.123.44=453</code></li> </ul>
<b>Config</b>	Use this section to configure settings for server certificate and client certificate authentication if you are using secure (encrypted) TSAPI links. If you are not sure whether you need to use this section, please refer, TSAPI Windows client certificate authentication.  If you do plan to set up the Config section, see Server certificate authentication using your own certificate.
<b>Alternate Tlinks</b>	Use this section if you want your TSAPI Windows clients to use the Alternate Tlinks feature. See, Specifying Alternate Tlinks for the TSAPI Windows client.
<b>Shared Admin</b>	Use this section when you want to use a pointer to a server-based <code>tslib.ini</code> file. See Installing the next client by sharing a single <code>tslib.ini</code> file among clients.

 **Note:**

If a firewall is present between the AE Services Server and the TSAPI client machine, make sure that the address in the `TSLIB.INI` or `tslibrc` configuration file uses the externally facing IP address of your firewall instead of the IP address of the AE Services Server.

**Related links**

[Specifying Alternate Tlinks for the TSAPI Windows client](#) on page 20

[Installing the next client by sharing a single tslib.ini file among clients](#) on page 28

[TSAPI Windows client certificate authentication](#) on page 21

[Server certificate authentication using your own certificate](#) on page 22

## Specifying Alternate Tlinks for the TSAPI Windows client

### About this task

The Alternate Tlinks feature enables the TSAPI client library to select an alternate Tlink if the preferred Tlink is unavailable when trying to establish a session. To enable the usage of this feature, specify the alternate Tlinks in the TSAPI Configuration file. For more information, see TSAPI Links (Tlinks).

 **Important:**

When multiple AE Services Servers are used as alternates, the CT User user ID, and password used by the application must be configured identically on each AE Services Server.

Use this procedure to set up a list of alternate Tlinks in the `tslib.ini` file. You are typically adding statements that specify a list of alternate Tlinks for the TSAPI Service.

### Procedure

1. Click on **Start > All Programs > Avaya AE Services > TSAPI Client > Edit TSLIB.INI** to open the `tslib.ini` file.
2. Locate the line `[Alternate Tlinks]` in the `tslib.ini` file, or add this line to the end of the file if it is not present.

This line is required if you want your TSAPI Windows clients to use the Alternate Tlinks feature.

3. After the `[Alternate Tlinks]` line, add a list of alternate Tlink entries.

```
Alternates (TLINK) =TLINK1 : TLINK2 : TLINK3 : TLINK4
```

Where

See [Alternate Tlinks for the TSAPI Windows client](#) for a detailed explanation on the alternate tlink entry.

**Related links**

[TSAPI Links \(Tlinks\)](#) on page 40

## TSAPI Windows client certificate authentication

The TSAPI Service may be configured to use Transport Layer Security (TLS) for encrypting TSAPI client connections to the AE Services Server. When the TSAPI client requests a secure connection to the AE Services Server, the TSAPI service sends a certificate to the TSAPI client that allows the client to verify the identity of the server. This process is known as server certificate authentication.

You can configure the TSAPI Service to request a certificate from the client so that the AE Services Server can verify the identity of the client. This process is known as client certificate authentication.

For server certificate authentication, you may use the Avaya Product Root Certificate Authority (CA) certificate as the server certificate which is default at AE Services 7.x and older and servers upgraded to AE Services 10.2.x, the self-signed certificate created during 10.2.x fresh installation, or a CA certificate issued by a trusted in-house or third-party certificate authority or your own certificate.

### \* Note:

For self-signed certificate, **TLS Hostname Validation** must be disabled that is the value of **Verify Server FQDN** field must be set to zero.

For client certificate authentication, AE Services does not provide a default certificate. You must provide and install your own certificates for client certificate authentication.

For more information about certificates, see Appendix A: Certificates management.

### \* Note:

The `tslib.ini` configuration file provides several configuration settings to control the behavior of the TSAPI client during server certificate and client certificate authentication.

You do not have to add any certificate configuration settings under the following conditions:

- You do not need to add any certificate configuration settings to the `tslib.ini` file if you do not use secure client connections, and hence, certificates.
- If you use secure client connections, you do not need to add any server certificate authentication settings to the `tslib.ini` file for either of the following situations:
  - You use the default AE Services certificate for server certificate authentication.
  - You use your own certificates and the trusted CA certificate is installed on the client computer in the file `<installation-directory>\certs\ca\aesCerts.cer`.
- If you use secure client connections, you do not need to add any client certificate authentication settings to the `tslib.ini` file for either of the following situations:
  - The TSAPI Service is not configured to perform client certificate authentication.
  - The client keystore containing the client certificate is installed on the client computer in the file `<installation-directory>\certs\tsapiClient.pfx` and does not have a password.

## Related links

[Certificate management](#) on page 60

### Server certificate authentication using your own certificate

You must add statements to the `tslib.ini` file that specifies the location of your certificate only if you are:

- Using your own certificates for server certificate authentication
- Not using the predefined location for storing certificates that is, the `aesCerts.cer` file

For example:

[Config]

Trusted CA File=<*certificate\_location*>

Verify Server FQDN= 0

where:

- The trusted CA File is the label for the file specification. The equal sign (=) is a separator between the label and the file specification.

`certificate_location` is the full pathname of a file containing the certificates for your trusted CA in Privacy Enhanced Mail (PEM) format. For example,

```
C:\Program Files\Avaya\AE Services\TSAPI  
Client\certs\ca\ExampleCorpServCert.cer
```

**\* Note:**

The specified file might contain several certificates.

- Verify Server FQDN is a setting that determines whether the TSAPI client verifies the Fully Qualified Domain Name (FQDN) in the Server Certificate for added security.

**\* Note:**

This setting must be set to 0 when the AE Services Server is using the Avaya self-signed certificate.

If you want the client to check the certificate for the FQDN, you can use the Verify Server FQDN=1 setting. Otherwise, you can use the Verify Server FQDN=0 setting.

You must add statements to the `tslib.ini` file that specify the location and or password of the client keystore only if:

- The TSAPI Service is configured to perform client certificate authentication
- You are not using the predefined location for the client keystore that is, the `tsapiClient.pfx` file
- If the client keystore is password protected

[Config]

Client KeyStore=<*keystore-location*>

KeyStore Password=<*keystore-password*>

where:

- The Client KeyStore setting specifies the full pathname of a PKCS12 (Public-Key Cryptography Standards #12) keystore containing the client certificate that the TSAPI client must send to the TSAPI Service. For example: Client KeyStore=C:\Program Files (x86)\Avaya\AE Services\TSAPI Client\certs\myKeystore.pfx
- The KeyStore Password setting specifies the password of the client keystore. For example: KeyStore Password=p@ssWord!

If the client keystore does not have a password, then this configuration setting is not needed.

TSLIB.INI

The [Telephony Servers] section specifies the AE Services servers that your installation uses.

[Telephony Servers]

```

; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
; Each entry must have the following format:
; host_name=port_number
; where:
; - host_name is either the domain name or IP address of the
; AE Services server.
; - port_number is the TSAPI Service port number. The port numbers used
; by AE Services are 450 for unsecure connection and 453 for secure connection.
; Note: In order to use secure connection, you need to install Trusted CA on your
; client and configure Trusted CA File parameter under [Config];

;For example:
; For using Unsecure connection:
; aeserver.mydomain.com=450           # host name example
; 192.168.123.45=450                 # IPv4 address example
; 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=450 # IPv6 address example
; For using Secure connection:
; aeserver.mydomain.com=453           # host name example
; 192.168.123.45=453                 # IPv4 address example
; 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=453 # IPv6 address example
    
```

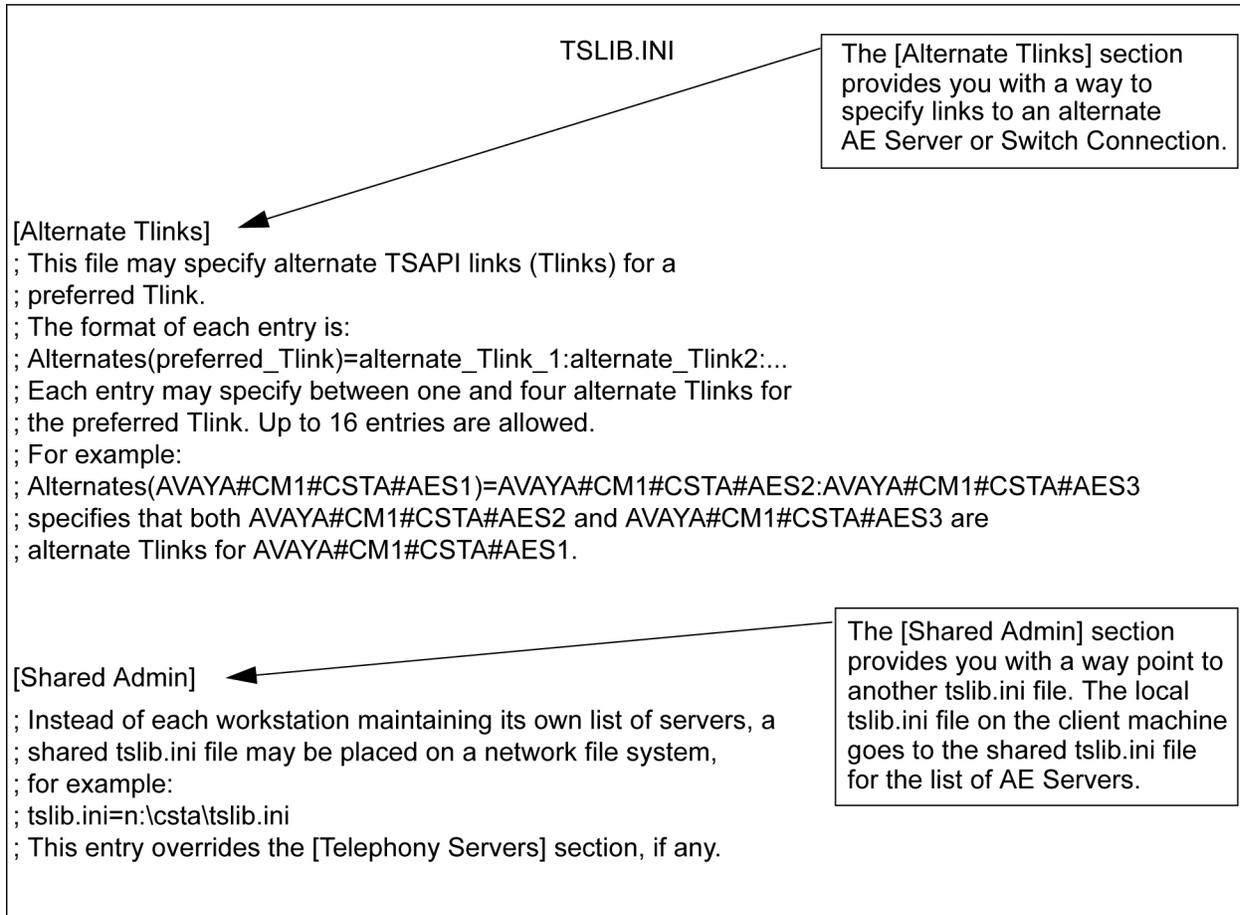
The [Config] section allows you to specify where your Trusted CA certificates for server certificate authentication are stored, and where your client certificates for client certificate authentication are stored. You do not need to edit this section if you do not use secure client connections

[Config]

```

; When accessing Telephony Services via a secure,
; encrypted
; connection, the Application Enablement (AE) Services
; server
; sends its certificate to the TSAPI client, and the TSAPI
; client
; verifies that the certificate is signed by a trusted
; Certificate
; Authority (CA).
; If your organization has installed its own certificate on the AE
; server, then the TSAPI client must have access to the trusted
; CA certificate(s) for the AE Services server certificate. Provide
; the location of a file containing the trusted CA certificate(s) here.
    
```

**Figure 1: Sample tslib.ini file - Part 1**



**Figure 2: Sample tslib.ini file - Part 2**

**\* Note:**

The client's shared certificate must have the following values to establish a secure connection from a TSAPI client to the AE Services server:

- **Key Usage:** Digital Signature, Non-repudiation, Key encipherment
- **Extended Key Usage:** clientAuth

**\* Note:**

**Extended Key Usage** is an optional field, it must have the mentioned value only if it is present in the certificate configuration.

The connection will be dropped if the certificate does not meet the above criteria.

## Network-based installations for the TSAPI Windows client

This section provides two installation scenarios for network-based installation. Use this section as your guide for the installation scenario that you want to use.

## Customizing the tslib.ini file prior to installation

### About this task

Use this procedure to customize the `tslib.ini` file prior to installation.

### Procedure

1. Copy the software and install the first TSAPI client as described in Copying the TSAPI Windows client software.
2. Install the next TSAPI client and all subsequent clients as described in Installing the next client: customizing the `tslib.ini` file before installation.

### Related links

[Copying the TSAPI Windows client software](#) on page 26

[Installing the next client customizing the tslib.ini file prior to installation](#) on page 27

## Sharing a single tslib.ini file among clients

### About this task

Use this task to share a single `tslib.ini` file among clients.

### Warning:

Although this method allows you to maintain only one centrally-located configuration file, the drawback is that an outage of the file server where the configuration file resides could prevent all of your TSAPI clients from connecting to the AE Services Server.

### Procedure

1. Copy the software and install the first TSAPI client as described in Copying the TSAPI Windows client software.
2. Install the next TSAPI client using the [Shared Admin] settings in the `tslib.ini` file as described in Installing the next client by sharing a single `tslib.ini` file among clients.

### Related links

[Copying the TSAPI Windows client software](#) on page 26

[Installing the next client by sharing a single tslib.ini file among clients](#) on page 28

## Copying the TSAPI Windows client software

### About this task

To install the Windows client software from a network drive, you must first transfer the TSAPI Windows client installation software to the network drive. Then client computers can install from the file server.

Use this procedure to copy the TSAPI Windows client software to a network drive.

### Procedure

1. Create or locate a directory such as `\TSAPI\Client` on a network drive. You can do this remotely from a client computer, or directly from the file server.

2. Copy the files for the TSAPI Windows client installation software to the `\TSAPI\Client` directory on the network drive.
3. If the TSAPI Windows client installation software is provided as a `.zip` file, then extract the files from the `.zip` file to the `\TSAPI\Client` directory on the network file server.

## Installing the first TSAPI client

### About this task

Copy the TSAPI Windows client software to a network drive.

Use this procedure to install the first TSAPI client.

### Procedure

1. [Initial client installation] On the client computer, go to the `\TSAPI\Client` folder on the network drive, and double-click **setup.exe** to install the TSAPI Windows client.
2. At this point you can follow Steps 3 through 8 of the procedure to install the TSAPI Windows client, see Installing the TSAPI Windows client. Notice that in Step 6 of the TSAPI Windows client installation procedure you are providing the Host Name or IP Address of the AE Services Server that gets added to the `tslib.ini` file.
3. Make any other changes to the `tslib.ini` file, such as specifying alternate Tlinks or configuration settings for secure Tlinks.

## Installing the next client customizing the `tslib.ini` file prior to installation

### About this task

Use this procedure if you want each client to have its own local copy of the `tslib.ini` file. Using this approach means that if there is a change that affects all of your clients for example, the IP address of the AE Services Server changes, you will need to update the `tslib.ini` files on all your client computers individually.

### Procedure

1. After you have installed the TSAPI Windows client on the first client computer, copy the client's local `tslib.ini` file to the `\TSAPI\Client` directory on the network server.

The purpose of this step is to make subsequent client installations easier. By copying the `tslib.ini` file to the network server, you are enabling setup to provide the contents of the updated `tslib.ini` file the next time a client computer runs the setup program.

2. For next client installation and all subsequent clients, from the next client computer, go to the `\TSAPI\Client` directory on the network drive and double-click **setup.exe** to install the TSAPI Windows client. This time you do not have to complete the AE Services Server Configuration dialog box. The setup will get this information from the `tslib.ini` file on the server. When the setup completes the installation, it will create a local `tslib.ini` file with the appropriate host name or IP address.

## Installing the next client by sharing a single `tslib.ini` file among clients

### Before you begin

Install the TSAPI Windows client on the first client computer.

### About this task

Follow these steps if you want all of your clients to share a single copy of the `tslib.ini` file. Using these settings means that the local `tslib.ini` file on each client will direct the TSAPI Windows client library to obtain the host name or IP address of the AE Services Server from the shared `TSLIB.INI` file.

### Caution:

This method allows you to maintain only one centrally-located configuration file and the drawback is that an outage of the file server where the configuration file resides could prevent all of your TSAPI clients from connecting to the AE Services Server.

### Procedure

1. Copy the client's local `TSLIB.INI` file to the network file server, for example, `h:\TSAPI\Client\sharedtslib.ini`. Do not overwrite the `TSLIB.INI` file in the `\TSAPI\Client` folder containing the TSAPI Windows client installation software.
2. Edit the [Shared Admin] section of the client's local `tslib.ini` file to contain the full pathname of the shared `TSLIB.INI` file on the network file server. For example: `tslib.ini=h:\TSAPI\Client\sharedtslib.ini` (where `h:\TSAPI\Client` specifies the network drive and path to the `tslib.ini` file on your server).
3. Now copy the client's local `TSLIB.INI` file to the `\TSAPI\Client` directory on the network file server, overwriting the `TSLIB.INI` file in the directory that contains the TSAPI Windows client installation software.
4. For next client installation and subsequent installations, from another client computer, go to the `\TSAPI\Client` directory on the network drive and double-click **setup.exe** to install the TSAPI Windows client. This time you do not have to complete the AE Services Server Configuration dialog box. Setup will install the updated `TSLIB.INI` file that points to the shared `TSLIB.INI` file.

---

## Installing and configuring the TSAPI Linux Client

### Installing the TSAPI Linux client

#### Before you begin

- Download the installation files and save them to your computer. For more information, see downloading software from PLDS.

- For 32 bit TSAPI client:
  - Ensure that you have 32 bit `glibc-2.28-127.el8.i686` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install glibc-2.28-127.el8.i686
```
  - Ensure that you have 32 bit `libstdc++-8.2.1-3.5.el8.i686` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install libstdc++-8.2.1-3.5.el8.i686
```
  - Ensure that you have 32 bit `openssl-libs-1:1.1.1-8.el8.i686` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install openssl-libs-1:1.1.1-8.el8.i686
```
- For 64 bit TSAPI client:
  - Ensure that you have 64 bit `glibc-2.28-127.el8_3.2.x86_64` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install glibc-2.28-127.el8_3.2.x86_64
```
  - Ensure that you have 64 bit `libstdc++-8.2.1-3.5.el8.x86_64` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install libstdc++-8.2.1-3.5.el8.x86_64
```
  - Ensure that you have 64 bit `openssl-libs-1:1.1.1-8.el8.x86_64` or higher version library installed on your computer. If not installed, you can run the following command to install the library. For example:
 

```
yum install openssl-libs-1:1.1.1-8.el8.x86_64
```

## Procedure

1. Log in to the client computer as `root`.
2. Go to the directory containing the TSAPI Linux Client installation program `tsapi-client-linux-arch-version-build.bin`.  
Where,
  - Version is the TSAPI Linux Client version number.
  - Build is the TSAPI Linux Client build number.
3. Use the `chmod` command to make the TSAPI Linux Client installation program executable. For example, `chmod +x tsapi-client-linux-arch-8.1-xxx.bin`.
4. Run the TSAPI Linux Client installation program to begin the installation. For example: `./tsapi-client-linux-arch-8.1-xxx.bin`
5. Press the `Enter` key to display the **End User License Agreement**.

6. Carefully review the license agreement. When the installation program asks if you agree to the license terms, enter `y`.
7. When the installation program asks you to enter a temporary directory for the installation RPM, enter a valid directory, or press the `Enter` key to accept the default directory (`/tmp`).
8. When the installation program prompts for confirmation, enter `y`.
9. Edit the `tslibrc` file. For more information, see Linux client configuration file customization.

### Related links

[Downloading software from Avaya PLDS](#) on page 7

[Customizing the Linux client configuration file](#) on page 30

## Customizing the Linux client configuration file

You can customize the behavior of TSAPI Linux clients by editing the TSAPI client configuration files. The TSAPI Linux client uses a configuration file called `tslibrc`, which, by default, is located at `/usr/lib/tslibrc` for 32-bit client and at `/usr/lib64/tslibrc` for 64-bit client.

TSAPI Linux clients rely on the `tslibrc` configuration file to identify the AE Services Servers that are available on the network. To provide TSAPI Linux clients with access to the AE Services Servers, you must edit the `tslibrc` configuration file.

You can specify an alternate location for this file by setting and exporting the shell environment variable `TSLIBRC`. If the `TSLIBRC` variable is not set, the client library searches your `$HOME` directory for a file named `.tslibrc`. If the client library cannot locate a configuration file after looking in both `TSLIBRC` and `.tslibrc`, it looks for the file `/usr/lib/tslibrc` for 32-bit client and at `/usr/lib64/tslibrc` for 64-bit client.

## Editing the `tslibrc` file

### About this task

Use this procedure to edit the `tslibrc` file.

### Procedure

1. Use your text editor to open the `/usr/lib/tslibrc` file for 32-bit client or `/usr/lib64/tslibrc` file for 64-bit client.
2. Replace `127.0.0.1` with either the fully qualified domain name or the IP address of the AE Services server to gain access and the port number you want to use.
  - The port number for the Unencrypted TSAPI Service is 450.
  - The port number for the Encrypted TSAPI Service is 453.

```
host_name port_number # comment
```

Where:

- `host_name` is an Internet domain name or IP address. Spaces are not valid in hostnames.
- `port_number` is the TCP port for the TSAPI Service name. If the port number is omitted, a default value of 450 is assumed.

 **Note:**

By default, TSAPI unencrypted port 450 is disabled from AE Services Release 10.2.

- `# comment` is the area to the right of the pound sign for comments.

If you use a firewall, for more information, see Port settings for firewall administration.

### Related links

[Port settings for a firewall administration](#) on page 41

## Specifying Alternate Tlinks for the Linux client

### About this task

The Alternate Tlinks feature allows the TSAPI client library to select an alternate Tlink if the preferred Tlink is unavailable when trying to establish a session. To put this feature into effect, you must specify the alternate Tlinks in the TSAPI Configuration file. For a brief description of Tlinks, see TSAPI Links (Tlinks).

 **Important:**

When multiple AE Services Servers are used as alternates, the CT User user id and password used by the application must be configured identically for each AE Services Server.

Use these steps to set up a list of alternate Tlinks in the `tslib.ini` file

### Procedure

1. Use your text editor to open the `/usr/lib/tslibrc` file for 32-bit client or `/usr/lib64/tslibrc` file for 64-bit client.
2. Add a list of alternate Tlink entries, using the following format.

Alternates(TLINK)=TLINK1:TLINK2:TLINK3:TLINK4

where:

- Alternates is the label for the first ordered list (you can have up to 16 lists)
- (TLINK) is the name of the preferred Tlink, for example (AVAYA#Avaya Aura<sup>®</sup> Communication Manager1#CSTA#AESRV1). Be sure to enclose the preferred Tlink name in parentheses.
- = The equal sign is a separator between the preferred Tlink, and the list of 1 to 4 alternate Tlinks. You must use the equal sign (=) to separate the preferred Tlink and the list of additional alternate Tlinks.

TLINK1:TLINK2:TLINK3:TLINK4 is an ordered list of Tlink names that are used as alternates if the preferred Tlink is not available. Be sure to separate each Tlink name with a colon. You can specify from 1 to 4 Tlinks for each list of alternates.

### Related links

[TSAPI Links \(Tlinks\)](#) on page 40

## Examples for specifying Alternate Tlinks for the Linux client

### Example 1

```
#[Alternate Tlinks]Alternates(AVAYA#CM1#CSTA#AESRV1)=AVAYA#CM1#CSTA#AESRV2
```

### Example 2

```
#[Alternate  
Tlinks]Alternates(AVAYA#CM1#CSTA#AESRV1)=AVAYA#CM1#CSTA#AESRV2:AVAYA#CM1#CS  
TA#AESRV3:AVAYA#CM1#CSTA#AESRV4
```

In Example 1, there are two AE Services Servers, AESRV1 and AESRV2, that each have a TSAPI link to the same switch, Avaya Aura<sup>®</sup> Communication Manager. When opening a stream, if AESERV1 is unavailable, the TSAPI client will attempt to use AESRV2 instead of AESRV1.

In Example 2, there are four AE Services Servers that each have a TSAPI link to the same switch, Avaya Aura<sup>®</sup> Communication Manager.

When opening a stream:

- If AESRV1 is unavailable, the TSAPI client will attempt to use AESRV2 instead of AESRV1.
- If AESRV2 is also unavailable, the TSAPI client will attempt to use AESRV3.
- If AESRV3 is also unavailable, the TSAPI client will attempt to use AESRV4.
- If AESRV4 is also unavailable, the TSAPI client will not be able to establish a connection with an AE Services server.

## TSAPI Linux client certificate authentication

The TSAPI Service may be configured to provide Transport Layer Security (TLS) for encrypting data exchanged between the TSAPI client and the AE Services server. If you plan to use encrypted links, you have the option of using the Avaya Product Root Certificate Authority (CA) certificate which is default, or using certificates issued by a trusted in-house or third-party certificate authority (also referred to as your own certificates). For more information about certificates, see Appendix A: Certificates management.

### Note:

You do not have to add any configuration settings for certificates under the following conditions:

- You do not use encrypted connections, and, hence, certificates.
- You use encrypted Tlinks with the default AE Services certificate. The default AE Services certificate is signed by the Avaya Product Root Certificate Authority (CA). The certificate for the Avaya Product Root CA is installed with the TSAPI Linux client in `/opt/mvap/tsapi/client/certs/CA/avayaprca.pem`.

- You use encrypted Tlinks with your own certificates, and you have copied the trusted CA certificate to the client computer as `/opt/mvap/tsapi/client/certs/CA/aesCerts.pem`. When establishing a secure connection, the TSAPI client checks to see if you have provided this file. If so, you do not need to configure the location of the Trusted CA File in the `tslibrc` file.

## Certificate configuration statements addition to the `tslibrc` file

If you are using your own certificates for server certificate authentication, and you are not using the predefined location for storing certificates (that is, `/opt/mvap/tsapi/client/certs/CA/aesCerts.pem`), you must add statements to the `tslibrc` file that specify where your certificates are located. For example:

```
Trusted CA File=<certificate_location>
```

```
Verify Server FQDN= 0
```

where:

- Trusted CA File is the label for the file specification. The equal sign (=) is a separator between the label and the file specification.

`certificate_location` is the full pathname of a file containing the certificate(s) for your trusted CA in Privacy Enhanced Mail (PEM) format. For example:

```
/opt/mvap/tsapi/clients/certs/CA/exampleCA.pem
```

Note that the specified file may contain several certificates.

- Verify Server FQDN is a setting that determines whether the TSAPI client verifies the Fully Qualified Domain Name (FQDN) in the Server Certificate (for added security).

### **Note:**

This setting should be set to 0 when the AE Services Server is using the Avaya Product Root CA Certificate.

- If you want the client to check the certificate for the FQDN, use this setting: Verify Server FQDN=1
- If you do not want the client to check the certificate for the FQDN, use this setting: Verify Server FQDN=0

Alternatively, you could just omit this line.

If the TSAPI Service is configured to perform client certificate authentication and you are not using the predefined location for the client keystore (that is, the `tsapiClient.pfx` file), or if the client keystore is password protected, then you must add statements to the `tslibrc` file that specify the location and/or password of the client keystore. For example:

```
Client KeyStore=<keystore-location>
```

```
KeyStore Password=<keystore-password>
```

where:

- The Client KeyStore setting specifies the full pathname of a PKCS12 (Public-Key Cryptography Standards #12) keystore containing the client certificate that the TSAPI client should send to the TSAPI Service. For example:

```
Client KeyStore=/home/ctiuser/certs/myKeystore.pfx
```

- The KeyStore Password setting specifies the password of the client keystore. For example:  
KeyStore Password=xxxxxxx

If the client keystore does not have a password, then this configuration setting is not needed.

```

# /usr/lib/tslibr or /usr/lib64/tslibr- Linux Telephony Services Library
Configuration File

# Blank lines and text beginning with "#" are ignored.

# -----
# [Telephony Servers]
#
# List your Telephony Servers and Application Enablement (AE) Services
# servers that offer TSAPI Telephony Services below.
#
# Each entry must have the following format:
#
# host_name [port_number]
#
# where:
#
# - host_name is either the domain name or IP address of the AE Services
#   server.
# - port_number is the TSAPI Service port number. The port numbers used
#   by AE Services are 450 for unsecure connection and 453 for secure connection.
#
# Note: In order to use secure connection, you need to install Trusted CA on your
# client and configure Trusted CA File parameter under [Config];
#
# For example:
#
# For using Unsecure connection:
#
# aeserver.mydomain.com 450           # host name example
# 192.168.123.45          450         # IPv4 address example
# 3ffe:ffff:100:f101:2e0:18ff:fe90:9205 450 # IPv6 address example
#
# For using Secure connection:
#
# aeserver.mydomain.com 453           # host name example
# 192.168.123.45          453         # IPv4 address example
# 3ffe:ffff:100:f101:2e0:18ff:fe90:9205 453 # IPv6 address example
#
# Edit the following entry to use the actual host name or IP address of your
# AE Services server.

#127.0.0.1                450           # Edit this entry
#127.0.0.1                453           # Edit this entry

# [Config]
#
# When accessing Telephony Services via a secure, encrypted connection,
# the Application Enablement (AE) Services server sends its certificate
# to the TSAPI client, and the TSAPI client verifies that the certificate
# is signed by a trusted Certificate Authority (CA).
#
# If your organization has installed its own certificate on the AE
# Server, then the TSAPI client must have access to the trusted CA
# certificate(s) for the AE Services server certificate. Provide the
# location of a file containing the trusted CA certificate(s) here.

```

**Figure 3: Editing the tslibr file - Part 1**

```
# [Alternate Tlinks]
#
# This file may specify alternate TSAPI links (Tlinks) for a preferred
# Tlink.
#
# The format of each entry is:
#
# Alternates(preferred_Tlink)=alternate_Tlink_1:alternate_Tlink_2:...
#
# Each entry may specify between one and four alternate Tlinks for the
# preferred Tlink. Up to 16 entries are allowed.
#
# For example:
#
# Alternates(AVAYA#CM1#CSTA#AES1)=AVAYA#CM1#CSTA#AES2:AVAYA#CM1#CSTA#AES3
#
# specifies that both AVAYA#CM1#CSTA#AES2 and AVAYA#CM1#CSTA#AES3 are
# alternate Tlinks for AVAYA#CM1#CSTA#AES1.

# Individual users may override the contents of this file by setting
# the TSLIBRC environment variable to the pathname of an alternate file
# (in this same format) or by creating a ".tslibrc" file in their $HOME
# directory.
```

**Figure 4: Editing the tslibrc file - Part 2**

## Certificate revocation

AE Services client performs revocation check on the certificates provided by AE Services server using Online Certificate Status Protocol (OCSP). Certificate revocation status determines if the certificate is valid with the issuing Certificate Authority (CA) every time when the new secure connection request is initiated. If certificate is REVOKED, the AE Services client rejects the secure connection request.

Before using OCSP revocation check for certificates ensure that either AE Services server certificate contains OCSP responder URL inside certificate AIA extension or OCSP responder URL is configured in TSAPI client configuration. By default, OCSP revocation check on AE Services Server provided certificate is disabled.

OCSP revocation check has the following three levels:

- **NONE**: : Does not perform OCSP revocation check.
- **BEST\_EFFORT**: : allows the secure connection only if certificate is not revoked and if the certificate revocation status can not be fetched. For example, network issues.
- **MANDATORY**: : allows the secure connection only if certificate is not revoked. The default value is 1.

### Example

OCSP Revocation Check Method=1

OCSP Responder URI can be specified if no OCSP responder URI is present in the certificate provided by AE Services server certificates. Also, if OCSP Responder URI Preference is set to 'local, OCSP Responder URI can be set here. The default value is empty.

### Example

OCSP Responder URI=http://127.0.0.1:1234

OCSP Responder URI Preference defines whether the URI presented in presented certificate should be used or Local OCSP responder URI provided shall be used. 1 = Use OCSP Responder URI presented in certificate AIA field. 2 = Use OCSP Responder URI presented in configuration file. The default value is 1.

### Example

OCSP Responder URI Preference=1

## Using TSAPI Test to verify Linux client installations

### Before you begin

Before performing this procedure, you must edit the `/usr/lib/tslibr` file (or the `.tslibrc` file in your home directory) so that it contains the host name or IP address of the AE Services Server. See, [Editing the `tslibrc` file](#) .

### About this task

To verify the TSAPI Linux client installation, use TSAPI Test to make a call. Use this procedure to run a TSAPI Test session for the Linux clients. See, [Example for a TSAPI test session](#).

For information about Application control services (ACS) error messages, see [Appendix A: Universal Failure Events](#), in the *Avaya Aura® Application Enablement Services TSAPI for Avaya Aura® Communication Manager Programmer's Reference*.

For information about CSTA messages see, [Chapter 4 of the Avaya Aura® Application Enablement Services TSAPI for Avaya Aura® Communication Manager Programmer's Reference](#).

### Procedure

1. Log into the client computer.
2. Start the TSAPI Test program by typing `/usr/lib/tstest` at the command prompt.  
The TSAPI Test program displays a numbered list of the available servers.
3. At the prompt to enter a server number (the range of numbers varies according to your configuration), type an appropriate number.
4. At the Server login prompt type your CT User user id.

#### Note:

A CT User is a person or an application administered in the AE Services User database with the **CT User** field set to **yes**. CT User authorization is controlled by the AE Services Security Database.

5. At the Server password prompt enter your CT User password.
6. At the calling number prompt, enter a valid extension number, for example: 72412.

 **Note:**

If the Security Database is enabled for the TSAPI Service, the CT User entered in Step 4 must have permission in the AE Services Security Database to control this phone number.

7. At the called number prompt, type another valid extension number, for example: 75587.

After entering all the information, TSAPI Test attempts to open a stream and make a call from the calling number to the called number. TSAPI Test indicates the results of the test. If the open stream request cannot open a stream to the server, TSAPI Test will display an error message, and TSAPI Test will terminate.

**Related links**

[Editing the tslibrc file](#) on page 30

[Example for a TSAPI test session](#) on page 39

[Example for a TSAPI test session](#) on page 39

## Example for a TSAPI test session

### Start the session

```
Telephony Services
*** Make Call Test ***
```

```
Searching for Servers...
```

```
1) ATT#G3_SWITCH#CSTA#SERVER1
2) ATT#G3_SWITCH#CSTA#POOH
3) ATT#G3_SWITCH#CSTA#DAGOTTO
```

```
Enter a server number between 1 and 3 (default 1):
Server login (default admin):
Server password:
Calling number: 72412
Called number: 75587
```

If the open stream succeeds, TSAPI Test displays the following:

```
cstaMakeCall() succeeded!
cstaClearConnection() succeeded!
```

If the open stream fails, TSAPI Test will display an ACS error, for example:

```
acsOpenStream() failed with ACS Universal Failure
Error 25:
Bad password or login.
```

If a CSTA service fails, TSAPI Test will display a CSTA error, for example:

```
cstaMakeCall() failed with CSTA Universal Failure
Error 12:
Invalid CSTA device identifier
```

**Figure 5: Sample TSAPI Test session**

```
cstaMakeCall() failed with CSTA Universal Failure
Error 12:
Invalid CSTA device identifier
```

## Removing the TSAPI Linux client

### About this task

Use this procedure to remove the TSAPI Linux client.

### Procedure

1. Log in as root.
2. Use the `rpm -e` command to remove the TSAPI client. For example:

```
rpm -e tsapi-client-linux-[VERSION]-[ARCH]
```

The Red Hat Enterprise Linux version 5.x package manager removes the TSAPI Linux client

3. To verify that the software has been removed, type the following command:

```
rpm -q tsapi-client-linux-[VERSION]-[ARCH]
```

The system responds with the following message:

```
package tsapi-client-linux is not installed
```

## Upgrading the TSAPI Linux client

### About this task

Use these steps to upgrade the AE Services TSAPI Linux client.

### Procedure

1. Remove the previous version of the client (see Removing the TSAPI Linux client).
2. Install the latest version of the client (see Installing the TSAPI Linux client).

### Related links

[Removing the TSAPI Linux client](#) on page 39

[Installing the TSAPI Linux client](#) on page 28

## TSAPI Links (Tlinks)

A TSAPI Link (Tlink) represents the availability of the TSAPI Service for a particular switch connection by way of a particular AE Services Server. The AE Services administrator creates a Tlink by adding a TSAPI Link through the AE Services Management Console (**AE Services > TSAPI > TSAPI Links**). A Tlink name has the following format:

```
AVAYA#switch_connection_name#service_type#AE-server-name
```

where:

- AVAYA indicates that the TSAPI Service is provided by AE Services Server.
- switch\_connection\_name represents the Switch Connection name. The AE Services administrator determines the switch connection name when he or she administers a Switch Connection in AE Services Management Console.
- service\_type refers to the CSTA service type. It can be either of the following:
  - CSTA - If the TSAPI Link is administered as unencrypted (nonsecure).
  - CSTA-S - If the TSAPI Link is administered as encrypted (secure).
- AE\_server\_name is the name of the AE Services Server providing the TSAPI Service for the switch connection. The AE Services Server name is assigned by the person who performs the AE Services installation.

Example

```
AVAYA#CM1#CSTA-S#AESRV1
```

## Port settings for a firewall administration

If a firewall is present between the AE Services Server and the TSAPI client machine, make sure that the address in the `TSLIB.INI` or `tslibrc` configuration file uses the externally facing IP address of your firewall instead of the IP address of the AE Services Server.

---

# Installing and managing the TSAPI Windows SDK

## AE Services TSAPI SDK and the programming environment

AE Services recommends that you install the TSAPI client before you install the TSAPI SDK. The TSAPI client provides the run-time libraries that are necessary for running your application in the Avaya Aura® Communication Manager environment, and it provides tools for verifying the installation. Also, if you plan to use the TSAPI Exerciser, you must install the TSAPI Windows client.

**\* Note:**

The TSAPI Exerciser is available for the TSAPI Windows client only.

After you install the AE Services TSAPI client and SDK for your particular operating system, see the *Avaya Aura® Application Enablement Services TSAPI for Avaya Aura® Communication Manager Programmer's Reference* for information about using the SDK components.

The TSAPI SDK must be purchased. If you are a customer, contact an authorized Avaya Business Partner or an Avaya Account Executive to obtain the TSAPI SDK. If you are a Gold or Platinum DevConnect member, you can order the TSAPI SDK through DevConnect.

**\* Note:**

From Release 8.1.3 onwards, Avaya Aura® Application Enablement Services supports four new client SDK ISO files for TSAPI 32-bit client and TSAPI 64-bit client which shall be compatible with AE Services Releases 10.1 and later.

Examples:

- `-tsapi-client-sdk-linux32-8.1.3-23.iso`
- `-tsapi-client-sdk-linux64-8.1.3-23.iso`
- `-tsapi-client-sdk-windows32-8.1.3-23.iso`
- `-tsapi-client-sdk-windows64-8.1.3-23.iso`

## Installing the TSAPI Windows SDK

### Procedure

1. Log on to your computer as a user with administrator-equivalent permissions.

2. Insert the TSAPI SDK CD into your computer's CD-ROM drive.
3. From the toolbar, click **Start > Run**.
4. In the Run window, type the drive ID of your CD-ROM drive (for example, D:\), and click **OK**.
5. From the window displaying the files on the CD, navigate to the `sdk\Windows` folder, open the file `tsapi-sdk-win32-10.2.x-xxx-build.zip`, and double-click **setup.exe**.  
Setup displays the Welcome dialog box.
6. Click **Next**.

Setup searches for any older versions of the TSAPI SDK.

- If Setup detects the Avaya Computer Telephony version of the SDK, it issues the following warning and stops the installation: The Avaya CT SDK needs to be uninstalled before the installation can continue.
- If Setup detects an earlier, incompatible version of the Avaya Aura® Application Enablement Services TSAPI SDK, it displays a dialog box with the message:

```
Setup has detected an older version of the Avaya Aura
Application Enablement Services TSAPI SDK on your system.
This version needs to be removed before the installation can
continue. Would you like Setup to remove this version for you
now?
```

Click **Yes** to have Setup remove the earlier version of the TSAPI SDK software for you automatically.

Setup displays the License Agreement dialog box.

7. Carefully review the license agreement, select **I accept the terms of the license agreement**, and then click **Next**.

Setup displays the Choose Destination Location dialog box with the default destination folder. For 64-bit Windows platforms, the default destination for TSAPI 32-bit client is `C:\Program Files(x86)\Avaya\AE Services\SDKs\TSAPI` and the default destination for TSAPI 64-bit client is `C:\Program Files\Avaya\AE Services\SDKs\TSAPI`.

8. Click **Next**.

Setup displays the Select Features dialog box with all of the TSAPI SDK Components selected by default: Headers and Libraries, Sample Code, and TSAPI Exerciser.

9. Click **Next**.

Setup displays the Ready to Install the Program dialog box

10. Click **Install**.

Setup installs the files. When it has finished installing files, Setup displays the InstallShield Wizard Complete dialog box.

11. Click **Finish**.

### Next steps

Continue with Viewing the TSAPI Windows SDK Components to learn more about the TSAPI SDK.

### Related links

[Viewing the TSAPI Windows SDK Components](#) on page 43

## Viewing the TSAPI Windows SDK Components

### Procedure

1. Click **Start** click **All Programs > Avaya AE Services > SDKs > TSAPI**.
2. Select any of the following components:
  - a. **Explore Sample Code** - When you select Explore Sample Code, a windows displays the Samples directory which includes additional directories that contain coding examples for developing applications. For more information about Sample Code, see Contents of the TSAPI SDK in Chapter 2 of the *Avaya Aura® Application Enablement Services TSAPI for Avaya Aura® Communication Manager Programmer's Reference*.
  - b. **TSAPI SDK Readme** - When you select **Read Me**, Windows displays the **TSAPI Windows SDK Readme** file, which contains late-breaking information that might be not included in the documentation.
  - c. **TSAPI Exerciser** - When you select TSAPI Exerciser, Windows opens the TSAPI Exerciser. The TSAPI Exerciser is an application that enables you to send CSTA requests across a TSAPI CTI link and view the exchange of messages between the TSAPI Exerciser and the AE Services Server. For more information about using the TSAPI Exerciser, see TSAPI Exerciser Help, which is included with the TSAPI Exerciser.
  - d. **TSAPI Exerciser Scripting Instructions** - When you select TSAPI Exerciser Scripting Instructions, Windows opens a PDF file that describes the TSAPI Exerciser script interpreter.

---

## Removing the TSAPI Windows SDK

### Removing the TSAPI Windows SDK from a Windows system

#### Before you begin

Check the supported Windows operating systems at [TSAPI client and SDK system requirements and compatibility matrix](#) on page 12.

#### Procedure

1. Access the **Control Panel**.

2. From the Control Panel, click **Programs and Features**.  
Windows displays the Programs and Features window.
3. Select **Avaya Application Enablement Services TSAPI SDK**, and click **Uninstall**.  
A confirmation dialog box appears.
4. Click **Yes**.  
Setup uninstalls the software, and displays the Uninstall Complete dialog box.

## TSAPI Windows SDK upgradation

If you are upgrading from an older version of the Avaya Aura® Application Enablement Services TSAPI Windows SDK to a newer version, remove the older version first. See, [Installing the TSAPI Windows SDK](#) to follow the installation procedure.

 **Note:**

To install the TSAPI 64-bit client or SDK on Windows and Linux platforms, you must remove the TSAPI 32-bit client or SDK from the respective platform.

### Related links

[Installing the TSAPI Windows SDK](#) on page 41

---

# Installing and managing the TSAPI Linux SDK

## Installing the TSAPI Linux SDK

### About this task

The TSAPI Linux Client must be installed before the TSAPI Linux SDK can be installed.

### Procedure

1. Log in to the computer where you are installing the SDK as root.
2. Insert the TSAPI SDK CD into your computer's CD-ROM drive.
3. Type `mount /mnt/cdrom/` to mount the file system.
4. Type `cd /mnt/cdrom/sdk/Linux` to change to the directory containing the TSAPI Linux SDK installation program `tsapi-sdk-linux-version-build.bin`

Where:

- version is the TSAPI Linux SDK version number.
  - build is the TSAPI Linux SDK build number.
5. Run the TSAPI Linux installation program to begin the installation. For example: `./tsapi-sdk-linux-10.2.x-xx.bin`

6. Press the `Enter` key to display the SDK License Agreement.
7. Carefully review the license agreement. When the installation program asks `Do you agree to the license terms?`, enter `y`.
8. When the installation program asks you to enter a temporary directory for the installation RPM, enter a valid directory, or press the `Enter` key to accept the default directory (`/tmp`).
9. When the installation program prompts for confirmation, enter `y`.

## Removing the TSAPI Linux SDK

### Procedure

1. Log in as root.
2. Use the `rpm -e` command to remove the TSAPI Linux SDK. For example:

```
rpm -e tsapi-sdk-linux-[VERSION]-[ARCH]
```

The Red Hat Enterprise Linux version 5.x package manager removes the TSAPI Linux SDK.

3. To verify that the software has been removed, type the following command:

```
rpm -e tsapi-sdk-linux-[VERSION]-[ARCH]
```

The system responds with the following message:

```
package tsapi-sdk-linux is not installed
```

## Upgrading the TSAPI Linux SDK

### About this task

Use this procedure to upgrade the AE Services TSAPI Linux SDK.

### Procedure

1. Remove the previous version of the SDK (see [Removing the TSAPI Linux SDK](#)).
2. If a previous version of the TSAPI Linux client is installed, remove the previous version of the client (see [Removing the TSAPI Linux client](#)).
3. Install the latest version of the TSAPI Linux client (see [Installing the TSAPI Linux client](#)).
4. Install the latest version of the SDK (see [Installing the TSAPI Linux SDK](#)).

### Related links

[Removing the TSAPI Linux SDK](#) on page 45

[Removing the TSAPI Linux client](#) on page 39

[Installing the TSAPI Linux client](#) on page 28

[Installing the TSAPI Linux SDK](#) on page 44

# Chapter 4: AE Services CVLAN Client installation

The Avaya Aura® Application Enablement Services CVLAN Client, which can be installed on a client workstation, provides client computers with remote access to the Avaya Aura® Communication Manager third-party call control capabilities. Access is provided by the CVLAN Service running on an AE Services Server.

The CVLAN Client and the CVLAN Software Development Kit (referred to in this document as the CVLAN Client) are packaged together.

**\* Note:**

The CVLAN Client is provided for maintaining existing applications. It is not intended for new application development.

**\* Note:**

AE Services does not support the following operating systems as Microsoft has ended its support for the following operating systems from January 2020:

- Microsoft Windows Server 2008 R2
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Ultimate

---

## The CVLAN Client

The CVLAN client provides the runtime libraries (`cvlancli.dll` for Windows-based systems, and `libasai.so` for Linux-based systems) that are required by CVLAN applications.

---

## CVLAN client and certificate management

The CVLAN client can use Transport Layer Security (TLS) to encrypt data exchanged between the CVLAN client and the AE Services Server. When the CVLAN client requests a secure connection to the AE Services Server, the CVLAN Service sends a certificate to the CVLAN client that allows the client to verify the server's identity. This process is known as server certificate authentication.

The CVLAN Service may be configured to request a certificate from the client so that the AE Services Server can verify the client's identity. This process is known as client certificate authentication.

For server certificate authentication up to AE Services 7.x, you may either use the Avaya Product Root Certificate Authority (CA) certificate as the server certificate, or a CA certificate issued by a trusted in-house or third-party certificate authority. This certificate is also referred to as your own certificate.

A fresh install does not have an Avaya signed default certificate. A self-signed certificate is created during install time to be used as the Default. It is recommended to replace the self-signed certificate with a proper certificate.

The self-signed certificate on the AE Services 10.2.x server can be exported and saved for the CVLAN client to use for development and testing purposes to an AE Services 10.2.x server. The self-signed certificate should not be used in production environment.

The Avaya Product Root CA certificate is installed on the CVLAN client in the following location:

- Windows: <installation-directory>\certs\ca\avayaprca.cer
- Linux: /usr/adm/cvlan/certs/CA/avayaprca.pem

If you choose to use your own certificates, a file in Privacy Enhanced Mail (PEM) format that contains the certificate(s) for your trusted CA must be installed in the following location:

- Windows: <installation-directory>\certs\ca\aesCerts.cer
- Linux: /usr/adm/cvlan/certs/CA/aesCerts.pem

Note that this file may contain several certificates.

For client certificate authentication, AE Services does not provide a default certificate. You must provide and install your own certificates for client certificate authentication.

The default location for the PKCS12 (Public-Key Cryptography Standards #12) keystore containing the client certificate for client certificate authentication is:

- Windows: <installation-directory>\certs\cvlanClient.pfx
- Linux: /usr/adm/cvlan/certs/cvlanClient.pfx

If you choose to use a different file for the client keystore, the environment variable CLIENT\_KEYSTORE must contain the full path name of the keystore. Otherwise, this environment variable must not be set.

If the client keystore is password protected, then the environment variable KEYSTORE\_PWD must contain the password for the keystore. Otherwise, this environment variable must not be set.

For more information about certificates, see Certificates management.

**Related links**

[Certificate management](#) on page 60

---

## CVLAN client system requirements and compatibility matrix

**Table 2: CVLAN client system requirements and compatibility matrix**

CVLAN client and SDK version (file system)	Microsoft Windows version (file system)	Linux Version (file system)	AES Version
10.2 (32-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition</li> <li>• Microsoft Windows Server 2022 Standard Edition, (64-bits)</li> </ul>	Red Hat Enterprise Linux version 8.4 and later (32-bits)	<ul style="list-style-type: none"> <li>• 10.x</li> <li>• 8.x</li> </ul>
10.1 (32-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition</li> <li>• Microsoft Windows Server 2022 Standard Edition, (64-bits)</li> </ul>	Red Hat Enterprise Linux version 8.4 and later (32-bits)	<ul style="list-style-type: none"> <li>• 10.x</li> <li>• 8.x</li> </ul>
8.1.2 and later (32-bits)	<ul style="list-style-type: none"> <li>• Microsoft Windows 8.1 Pro</li> <li>• Microsoft Windows 8.1 Enterprise</li> <li>• Microsoft Windows 10 Professional Edition (64-bits)</li> <li>• Microsoft Windows Server 2012 R2 Standard Edition (32-bits and 64-bits)</li> <li>• Microsoft Windows Server 2016 Standard Edition (64-bits)</li> <li>• Microsoft Windows Server 2019 Standard Edition</li> </ul>	Red Hat Enterprise Linux version 6.10 (32-bits and 64-bits)	<ul style="list-style-type: none"> <li>• 8.x</li> </ul>

---

# Installing and managing CVLAN Windows client

## Installing the CVLAN Windows Client

### About this task

Follow this procedure to install the CVLAN Windows Client on a Windows workstation.

#### Important:

Make sure you have completed the instructions for downloading the installation files and saving them to your computer. For more information, see [Download location for clients](#).

### Procedure

1. Log on to your computer as a user with administrator-equivalent permissions.
2. Go to the directory that contains the CVLAN Windows client files that you downloaded, and double-click **setup.exe**.  
Setup displays the Welcome dialog box.
3. Click **Next**.  
Setup displays the License Agreement dialog box.
4. Carefully review the license agreement, select **I accept the terms of the license agreement**, and then click **Next**.  
Setup displays the Choose Destination Location dialog box with the default destination folder. For 64-bit Windows platforms, the default destination folder is C:\Program Files (x86)\Avaya\AE Services\CVLAN.
5. Click **Next**.  
Setup displays the Ready to Install the Program dialog box.
6. Click **Install**.  
Setup installs the files. Next, Setup displays a Question dialog box asking if you want to view the Readme file now.
7. Click **Yes** to view the Readme file. After reviewing the Readme file, either close the file or minimize the display.  
Setup displays the InstallShield Wizard Complete dialog box.
8. Click **Finish**.

### Next steps

Continue with [Using the ASAI test utility](#).

### Related links

[Using the ASAI test utility](#) on page 52

[Download location for clients and SDKs](#) on page 7

## Upgrading the CVLAN Windows Client

### About this task

Use this procedure if you are upgrading a previous CVLAN Windows client.

### Procedure

1. Uninstall the previous version of the Client.
2. Install the latest version of the Client.

### Related links

[Removing the CVLAN Windows Client](#)

[Removing the CVLAN Windows Client](#) on page 50

[Installing the CVLAN Windows Client](#) on page 49

## Removing the CVLAN Windows Client

### Procedure

1. Access **Control Panel**.
2. From the Control Panel, click **Programs and Features**.  
Windows displays the Programs and Features window.
3. Select **Avaya Application Enablement Services CVLAN Client**, and click **Uninstall**.  
A confirmation dialog box appears.
4. Click **Yes**.  
The uninstall program removes the software and displays an Information box indicating that the program and all of its components have been removed.
5. Click **Finish**.

---

## Installing and managing CVLAN Linux Client

### Installing the CVLAN Linux Client

#### Before you begin

Ensure that you have completed the instructions for downloading the installation files and saving them to your computer. For more information, see Download location for clients.

#### Procedure

1. Log in to the computer where you are installing the CVLAN Linux client as root.
2. Go to the directory that contains the CVLAN Linux Client installation program `cvlan-client-linux-version-build.bin`.

Where,

- version is the CVLAN Linux Client version number.
  - build is the CVLAN Linux Client build number.
3. Use the `chmod` command to make the CVLAN Linux Client installation program executable. For example, `chmod +x cvlan-client-linux-10.2.x-xx.bin`
  4. Run the CVLAN Linux Client installation program to begin the installation. For example, `./cvlan-client-linux-10.2.x-xx.bin`
  5. Press the `Enter` key to display the **End User License Agreement**.
  6. Carefully review the license agreement. When the installation program asks if you agree to the license terms, enter `y`.
  7. When the installation program asks you to enter a temporary directory for the installation RPM, enter a valid directory, or press the `Enter` key to accept the default directory (`/tmp`).
  8. When the installation program prompts for confirmation, enter `y`. This completes the procedure to install the CVLAN Linux Client.

 **Note:**

Review the readme file (`/usr/adm/cvlan/readme`) for release-specific information.

### Next steps

Continue with Using the ASAI test utility.

### Related links

[Using the ASAI test utility](#) on page 52

[Download location for clients and SDKs](#) on page 7

## Upgrading the CVLAN Linux Client

### About this task

Use the following guidelines to upgrade the AE Services CVLAN Linux Client.

### Procedure

1. Remove the previous version of the Client.
2. Install the latest version of the Client.

### Related links

[Removing the CVLAN Linux Client](#) on page 51

[Installing the CVLAN Linux Client](#) on page 50

## Removing the CVLAN Linux Client

### About this task

Use this procedure to remove the CVLAN Linux Client.

## Procedure

1. Log in to the client computer as **root**.
2. To remove the CVLAN Linux Client type the following command:

```
rpm -e cvlan-client-linux
```

3. To verify that the software has been removed, type

```
rpm -q cvlan-client-linux
```

The system responds with the following message:

```
package cvlan-client-linux is not installed
```

---

## The ASAI test utility

Use the ASAI test utility (**asai\_test**) to determine if the CVLAN client and AE Services Server are communicating. The usage of the **asai\_test** command is as follows:

Linux

```
/usr/adm/cvlan/bin/asai_test -m<server><link number>
```

where:**<server>** is the host name or IP address of the AE Services Server. **<link number>** is the link number (1-16) of the CVLAN link to be tested. (The link number is also known as the signal number.)

Windows

```
<installation-directory> utils\asai_test -m <server> <link number>
```

where:**<server>** is the host name or IP address of the AE Services Server. **<link number>** is the link number (1-16) of the CVLAN link to be tested. (The link number is also known as the signal number.)

---

## Using the ASAI test utility

### About this task

Follow this procedure to using the ASAI test utility.

### Procedure

1. At the command prompt (Linux based systems) or MS-DOS prompt (Windows), type the following command.

Linux

```
/usr/adm/cvlan/bin/asai_test -m abcserver 2
```

where: **abcserver** is the host name or IP address of the AE Services Server.

Windows

```
<installation-directory>\utils\asai_test -m abcserver 2
```

where: **abcserver** is the host name or IP address of the AE Services Server.

If the test is successful, the CVLAN Service responds with results similar to the following:

```
=== Test for CVLAN Link 2===Heartbeat test with switch for CVLAN
Link 02 was successful===Test Completed===
```

2. If **asai\_test** fails, take the appropriate course of action:

- Contact the AE Services administrator.
- If you are authorized to perform AE Services OAM administration, continue with the following steps.

- a. Log into the AE Services Server, and select **Utilities > Diagnostics > AE Services > ASAI test**.

AE Services OAM displays the ASAI Test Result page.

- b. Select the link numbers you want to test with the ASAI Test utility, and click **Test**.

OAM displays the ASAI Test Result page, which indicates the results of the test. A successful test will display the following message on the ASAI Test Result page.

```
Heartbeat test with switch for CVLAN Link 02 was successful.
```

# Chapter 5: Resources

## Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Design		
<i>Avaya Aura® Application Enablement Services Overview and Specification</i>	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
<i>Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide</i>	Installing TSAPI and CVLAN Client and SDK	Customers and sales, services, and support personnel
Using		
<i>Upgrading Avaya Aura® Application Enablement Services</i>	Upgrading Application Enablement Services applications.	System administrators and IT personnel
<i>Administering Avaya Aura® Application Enablement Services</i>	Administering Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel
<i>Avaya Aura® Application Enablement Services Data Privacy Guidelines</i>	Describes how to administer Application Enablement Services to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation		
<i>Deploying Avaya Aura® Application Enablement Services in Virtualized Environment</i>	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
<i>Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments</i>	Deploy Application Enablement Services applications in Software-Only and Infrastructure as a Service Environments	Implementation personnel
Maintenance and Troubleshooting		

*Table continues...*

Title	Description	Audience
<i>Maintaining Avaya Aura® Application Enablement Services</i>	Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel

### Related links

[Finding documents on the Avaya Support website](#) on page 55

[Accessing the port matrix document](#) on page 55

[Avaya Documentation Center navigation](#) on page 56

## Finding documents on the Avaya Support website

### Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.  
 For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
9. Press **Enter**.

### Related links

[Application Enablement Services documentation](#) on page 54

## Accessing the port matrix document

### Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list

8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
  - **Application & Technical Notes**
  - **Design, Development & System Mgt**The list displays the product-specific Port Matrix document.
10. Press **Enter**.

### Related links

[Application Enablement Services documentation](#) on page 54

## Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.

### **Important:**

For documents that are not available on Avaya Documentation Center, click **More Sites > Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Center, you can:

- Search for keywords.  
To filter by product, click **Filters** and select a product.
- Search for documents.  
From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (  ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (  ).  
Navigate to the **Manage Content > My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (  ).

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**\* Note:**

Some functionality is only available when you log in to the website. The available functionality depends on your role.

### Related links

[Application Enablement Services documentation](#) on page 54

---

## Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20980W	What's New with Avaya Aura®

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

**\* Note:**

Videos are not available for all products.

---

## Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

### Related links

[Using the Avaya InSite Knowledge Base](#) on page 58

## Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

The system displays the Avaya Support page.

5. Click **Support by Product > Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

**Related links**

[Support](#) on page 58

# Appendix A: Certificate management

## Important:

The information in this appendix applies only if you are using encrypted client connections.

This appendix of certificate management describes certificate authentication for TSAPI and CVLAN client connections. Prior to AE Services Release 7.x, only server certificate authentication was available. Beginning with AE Services Release 7.x, client certification authentication is also available.

Additionally, this overview describes how to configure the TSAPI and CVLAN clients for certificate authentication.

A fresh install does not have an Avaya signed default certificate. A self-signed certificate is created during install time to be used as default.

AE Services servers that have upgraded to version 10.2.x, and AE Services servers on version 7.x or older will have the default server certificate, which is signed by the Avaya Product Certificate Authority.

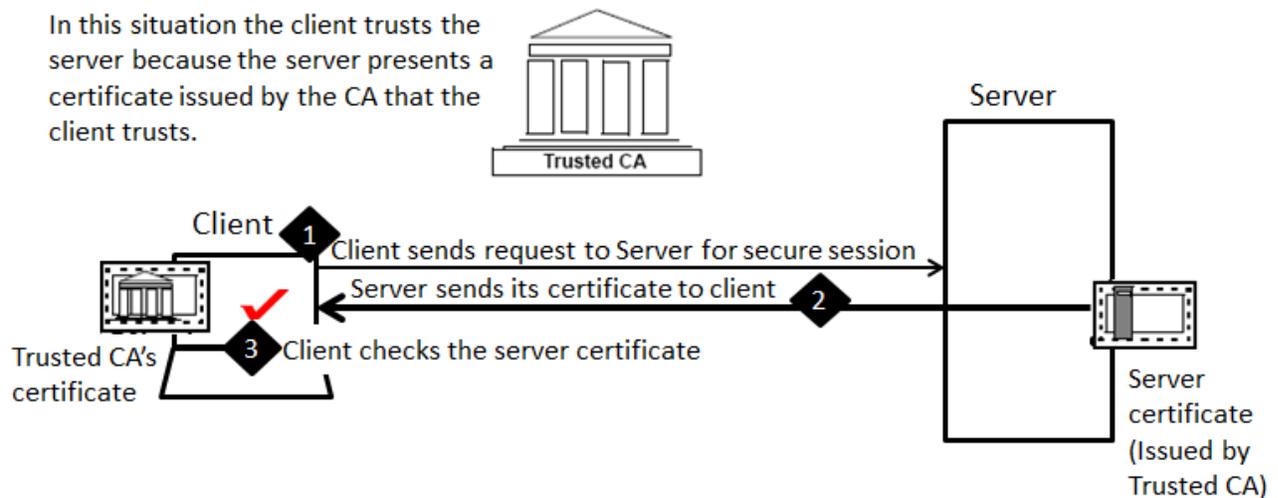
## Note:

The TSAPI and CVLAN Linux client, installed on RHEL ES version 6.5 system and later, will be able to establish a secure connection to the CVLAN Service running on AE Services 10.2.x server when using certificates with SHA2, for example SHA256 signatures.

---

## Server certificate authentication

When the AE Services TSAPI or CVLAN client establishes a secure connection to the AE Services Server, the server sends a certificate to the client that allows the client to verify the server's identity. This process is known as server certificate authentication. This process is the same if you use your own certificates or if you use the AE Services default server certificate, or AE Services self-signed certificate. See Figure 1: Server certificate authentication figure for an illustration.



**Figure 6: Server certificate authentication**

1. The client sends a request to the server for a secure session.
2. The server sends its server certificate to the client.
3. The client checks the server certificate to determine the following:
  - a. If the server certificate is issued by a certificate authority that the client trusts, the client checks the name of the CA.
 

To comply, the name of the certification authority (CA) on the certificate must match the name of the CA on the client's trusted certificate.
  - b. If the server certificate is within its validity window.
 

The client checks to see if the current time falls between the Not Before and Not After dates in the server certificate.
  - c. If the common name in the server certificate matches the name of the server to which the client is connected.
 

If the names do not match, the client cannot trust the certificate. This only applies if the client has been configured with Verify Server FQDN=1.

**\* Note:**

The server identity certificate must have the following values to establish a secure connection from a TSAPI client to a AE Services server:

- **Key Usage:** Digital Signature, Non-repudiation, Key encipherment
- **Extended Key Usage:** serverAuth

**\* Note:**

**Extended Key Usage** is an optional field, it must have the mentioned value only if it is present in the certificate configuration.

The connection will be dropped if the certificate does not meet the above criteria.

## Location and usage of Avaya-installed certificate

If you need to use TLS connection when connecting to TSAPI service, you can export the AE Services server trust certificates installed on the AE Services server. This certificate can be obtained via AE Services server management Web console. Go to **Security > Certificate Management > CA Trusted Certificates** page, select the certificate you want to export, then click on **export** button. This opens a new page with the certificate in a window. Copy the entire text in the window and add it to the end of the existing `CLIENT_INSTALL_PATH/certs/ca/avayaprca.cer` that is installed on the client.

For AE Services servers upgraded to 10.2.x and servers on 7.x and older versions, the AE Services Server includes a default server certificate, which is signed by the Avaya Product Certificate Authority (CA). The AE Services client installation programs for TSAPI and CVLAN install the Avaya Product CA certificate on the client computer. If you plan to use the default certificate you do not have to perform any additional client configuration for server certificate authentication when connecting to an AE Services server version 7.x and older.

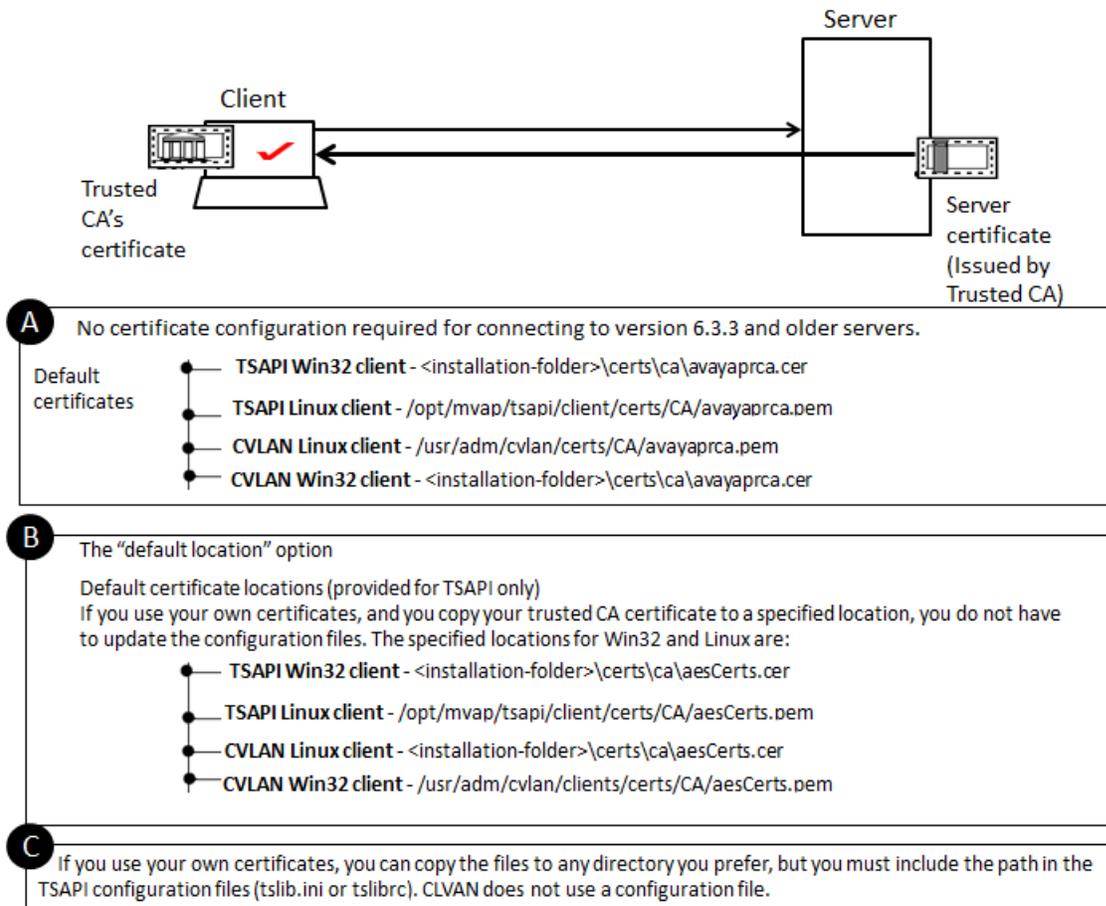
The default server certificate should be for lab use only.

**Table 3: Where AE Services installs the default CA certificate**

#	Name	Description
1	TSAPI Win32 client	<installation-folder>\certs\ca\avayaprca.cer
2	TSAPI Linux client	/opt/mvap/tsapi/client/certs/CA/avayaprca.pem
3	CVLAN Linux client	/usr/adm/cvlan/certs/CA/avayaprca.pem
4	CVLAN Win32 client	<installation-folder>\certs\ca\avayaprca.cer

## Location of your own certificates

Notice that frame B is labeled as the default location option in the following figure — Where AE Services installs the CA certificate per client:



**Figure 7: Where AE Services installs the CA certificate per-client**

If you use your own certificates, and you copy your certificates to a specified location, you do not have to update the configuration files (tslib.ini, for Win32 clients and tslibrc, for Linux clients). The specified locations are listed in the following table:

**Table 4: TSAPI and CVLAN- if you use your own certificates: the default location option**

#	Name	Description
1	TSAPI Win32 client	<installation-folder>\certs\ca\aesCerts.cer
2	TSAPI Linux client	/opt/mvap/tsapi/client/certs/CA/aesCerts.pem
3	CVLAN Win32 client	<installation-folder>\certs\ca\aesCerts.cer
4	CVLAN Linux client	/usr/adm/cvlan/clients/certs/CA/aesCerts.pem

## Usage of your own certificate

You can use the procedures below for using the certificates issued by a trusted in-house or third-party certificate authority.

## Setting up AE Services if you use your own certificate for TSAPI

### Procedure

1. On the computer where the client software is installed, install the Trusted CA's Certificate on your client.
2. On the Linux computer where the TSAPI client software is installed, edit the `tslibrc` file. See TSAPI Linux client certificate authentication.
3. If you are using your own certificates, and you are not using the predefined location for storing certificates, you must add statements to the configuration file that specify where your certificates are located.

### Related links

[TSAPI Linux client certificate authentication](#) on page 32

## Setting up AE Services if you use your own certificate for CVLAN

### Procedure

1. On the computer where the client software is installed, install the Trusted CA's Certificate on your client.
2. Make sure the certificate is installed in the proper location. On the computer that the client is installed on. See CVLAN client and certificate management.

### Related links

[CVLAN client and certificate management](#) on page 47

---

## AE Services certificate administration

If you are using your own certificates, the scope of both AE Services client and AE Services server administration tasks increases. To be able to use your own certificates for the AE Services TSAPI and CVLAN clients, certificate administration is required on the AE Services server.

If you are configuring TSAPI and CVLAN clients in an environment that uses certificates issued by a trusted in-house or third-party certificate authority, the checklist for setting up TSAPI and CVLAN - if you use your own certificates, provides you with a general frame of reference for the related AE Services administrative tasks.

## Checklist for setting up TSAPI and CVLAN - if you use your own certificates

Table 5: Checklist for setting up TSAPI and CVLAN client

#	Task	Notes
1.	Create a server certificate request for AE Services.  See Creating a server certificate signing request for the AE Services in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> , 02-30357.	
2.	Create an AE Services server certificate.  See Creating a server certificate for AE Services in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> .	
3.	Import the server certificate into AE Services.  See Importing the server certificate into AE Services in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> .	
4.	Check whether alternate TSAPI links are administered. If alternate TSAPI links are administered, you should configure the alternate Tlinks after the installation.	
TSAPI-related administrative tasks		
6.	Administer TSAPI links as encrypted.  See Administering TSAPI Links in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> .	
CVLAN-related administrative tasks		
7.	Add a CVLAN link.  See Administering CVLAN Links in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> .	
8.	Add a CVLAN client.  See Adding CVLAN Clients in the <i>Administering and Maintaining Avaya Aura® Application Enablement Services</i> .	

---

## Client certificate authentication

The TSAPI and CVLAN Services may be configured to request a certificate from the client so that the AE Services Server can verify the client's identity. This process is known as client certificate authentication.

1. After the client has authenticated the server's certificate, the server sends a request to the client for its certificate.

2. The client sends its certificate to the server.
3. The server checks the client certificate to determine the following:
  - a. If the client certificate is issued by a certificate authority that the server trusts.
  - b. If the client certificate is within its validity window. The server checks to see if the current time falls between the Not Before and Not After dates in the client certificate.
  - c. If the client certificate can be used for client authentication. The server checks to see if the client certificate's Extended Key Usage field includes Client Authentication.

When all the security checks are satisfied the client and server can exchange secure messages.

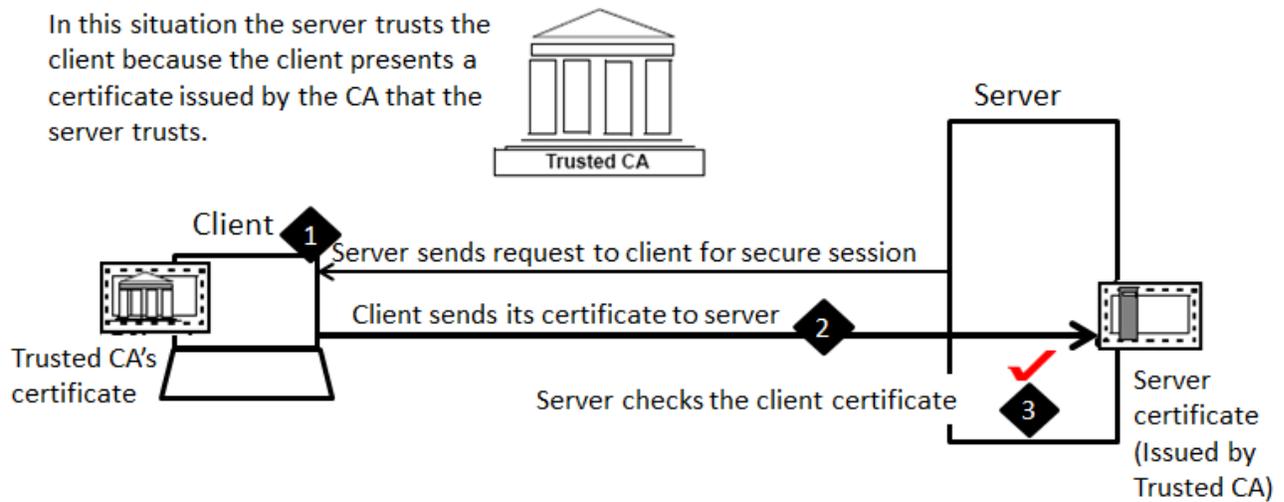


Figure 8: Client Certificate Authentication

## Usage of default client keystore location

If the TSAPI Service is configured to perform client certificate authentication and you install the client keystore containing the client certificate in the default location, you do not need to configure the location of the client keystore in the TSAPI client library configuration file. The following table lists the default location of the client keystore for the TSAPI Windows and Linux client libraries.

Table 6: TSAPI - Default client keystore locations

Name	Description
TSAPI Windows client	<installation-folder>\certs\tsapiClient.pfx
TSAPI Linux client	/opt/mvap/tsapi/client/certs/tsapiClient.pfx

If the CVLAN Service is configured to perform client certificate authentication and you install the client keystore containing the client certificate in the default location, then you do not need to set the environment variable CLIENT\_KEYSTORE for your CVLAN applications. The following table lists the default location of the client keystore for the CVLAN Windows and Linux client libraries.

**Table 7: CVLAN - Default TSAPI client keystore locations**

Name	Description
CVLAN Windows client	<installation-folder>\certs\cvlanClient.pfx
CVLAN Linux client	/usr/adm/cvlan/certs/cvlanClient.pfx

## Client keystore location and password configuration

If the client keystore is not installed in the default location, or if the client keystore is password protected, familiarize yourself with the following two tasks for specifying the client keystore location and password.

### Specifying the client keystore location and password for TSAPI

#### Procedure

1. Install the client keystore on the computer where the TSAPI client software is installed.
2. If you are not using the default location for the client keystore file, see Table 8: TSAPI - Default client keystore locations in Usage of default client keystore location, or if the client keystore file is password protected, you must add statements to the TSAPI client library configuration file that specify where the client keystore is located and or the password for the client keystore.
3. On the Windows computer where the TSAPI client software is installed, edit the `tslib.ini` file to provide values for the **Client KeyStore and/or KeyStore Password** settings. See Server certificate authentication using your own certificate.
4. On the Linux computer where the TSAPI client software is installed, edit the `tslibrc` file to provide values for the **Client KeyStore and/or KeyStore Password** settings. See Certificate configuration statements addition to the `tslibrc` file.

#### Related links

[Usage of default client keystore location](#) on page 66

[Server certificate authentication using your own certificate](#) on page 22

[Certificate configuration statements addition to the `tslibrc` file](#) on page 33

### Specifying the client keystore location and password for CVLAN

#### Procedure

1. Install the client keystore on the computer where the CVLAN client software is installed.
2. If you are not using the default location for the client keystore file, see Table 9: CVLAN - Default TSAPI client keystore locations in Usage of default client keystore location, you must set the environment variable `CLIENT_KEYSTORE` to the location of the client keystore file.
3. On the computer where the CVLAN client software is installed, set the environment variable `CLIENT_KEYSTORE` to the location of the client keystore file. See CVLAN client and certificate management.

## Certificate management

4. If the client keystore file is password protected, you must set the environment variable KEYSTORE\_PWD to the password for the client keystore.
5. On the computer where the CVLAN client software is installed, set the environment variable KEYSTORE\_PWD to the password for the client keystore file. See CVLAN client and certificate management.

### Related links

[Usage of default client keystore location](#) on page 66

[CVLAN client and certificate management](#) on page 47

# Appendix B: TSAPI Client Message Tracing

---

## TSAPI Spy - a Windows client message tracing tool

The TSAPI Client includes TSAPI Spy, a client message tracing application that lets you see the flow of messages through the client TSAPI Library (TSLIB). TSAPI Spy traces messages as they enter and leave the library in both directions: from application(s) to the TSAPI Service; from the TSAPI Service to application(s).

### Overview of the TSAPI Spy for Windows interface

Use this section to familiarize yourself with the TSAPI Spy for Windows interface.

- Read the table below for an operational summary of TSAPI Spy.

Name	Description
Tracing..	<ul style="list-style-type: none"><li>• Enabled - the default setting. When Tracing is enabled, message tracing information is displayed in the two display areas of the TSAPI Spy main window.</li><li>• Disabled - Select <b>Disabled</b> to disable message tracing. Tracing can be disabled at any time while TSAPI Spy is running. If you disable tracing, and then exit <b>TSAPI Spy (File &gt; Exit)</b>, the next time you start TSAPI Spy, it will be Disabled.</li></ul>
Open Streams (+)	Indicates the number of streams currently open from the TSLIB to all Telephony servers. This number is updated in real time as applications open and close connections.
Closed Streams (-)	Indicates the number of streams previously open from the TSLIB to all AE Services Servers, which are now closed. This number is updated in real time as applications close streams.
Streams list (white background)	Displays information about currently and previously open connections from the TSLIB to all telephony servers. For more information see, Streams list.

*Table continues...*

Name	Description
<b>Handle</b>	The internal ID for a stream. All the message lines in the trace file are prefixed with the handle of the connection to which the message belongs. The handle is generated by the TSLIB. Currently open connections are indicated with a + prefix on the Handle. Streams that were previously open but are now closed are indicated with a - prefix on the Handle
<b>Server ID</b>	The Tlink to which this connection has been opened. This information is provided to the TSLIB by the application when a request is made to open a connection.
<b>Appl</b>	The name of the application that has opened this connection. This information is provided to the TSLIB by the application when a request is made to open a connection.
<b>Login</b>	The login ID under which the application has opened this connection. Multiple applications may be opened under the same or different login ID(s) at a single client. This information is provided to the TSLIB by the application when a request is made to open a connection.
<b>Output display window (grey background)</b>	Displays the trace output in real time as messages are passed through TSLIB. This output window can display approximately 30,000 characters of trace history. Once the output limit has been reached, the oldest trace information is deleted in favor of the newer trace information. For long trace outputs, it is recommended that the trace be logged to a file. For more information, see Usage of the Log to File option to direct output to a trace file.
<b>Trace file status</b>	This line, below the Output window, indicates whether the Log To File option has been selected, and tracing. The default is "No trace file." When file logging is active, this line indicates the file name (with full path) and file size.
<b>File</b>	<ul style="list-style-type: none"> <li>• <b>Exit</b> - Use menu item is used to exit TSAPI Spy. The system menu may also be used to exit the application.</li> </ul>

*Table continues...*

Name	Description
<p><b>Edit</b></p>	<ul style="list-style-type: none"> <li>• <b>Copy</b> - copies the selected text (if any) from the Output window onto the Clipboard. The text is then available to be pasted into any application of your choosing. If no text is selected in the Output window, this menu item is grayed and disabled.</li> <li>• <b>Clear Buffer</b> - clears out the contents of the Output window. Once this is done, the original contents are lost (the data is NOT copied to the Clipboard).</li> <li>• <b>Select All</b> - selects all of the text in the Output window. The Copy menu item can then be used.</li> <li>• <b>Purge Closed Streams</b> - deletes all closed connections (indicated with a "-" prefix) from the streams list and resets the Closed Streams count to 0, leaving only currently open connections in the Streams List.</li> </ul>
<p><b>Options All options, except Auto-Trace New Streams, are disabled by default</b></p>	<ul style="list-style-type: none"> <li>• <b>Always On Top</b> - causes the TSAPI Spy window to be topmost on the screen display. This setting is disabled by default (a check mark does not appear next to it).</li> <li>• <b>Auto-Trace New Streams</b> - causes newly opened connections (which open after TSAPI Spy is started) to be traced automatically. This option is described in more detail in Streams list. This setting is enabled by default (a check mark appears next to it).</li> <li>• <b>Show Internal Events</b> - causes non-application messages to be traced. The majority of messages normally traced through the <code>CSTA32.DLL</code> are application-to-telephony server and telephony server-to-application messages. There are, however, a small number of messages that the TSLIB generates to facilitate application/telephony server communications. This setting is disabled by default (a check mark does not appear next to it).</li> <li>• <b>Log To File</b> - causes all trace messages to be logged to a file specified by the user. See Usage of the Log to File option to direct output to a trace file. This setting is disabled by default (a check mark does not appear next to it).</li> </ul>

**Related links**

[Streams list](#) on page 73

[Usage of the Log to File option to direct output to a trace file](#) on page 72

## Usage of the Log to File option to direct output to a trace file

The TSAPI Spy application allows you to trace the TSAPI messages exchanged by the TSAPI Windows client library and the TSAPI Service. The trace output is displayed in the main window, but you may also direct the trace output to a file by enabling the Log to File option.

You can use the TSAPI Spy Log to File option to limit the amount of disk space. See [Limiting the amount of disk space](#), for more information on how to use the Log to File option.

Each time the trace file reaches its maximum size, the trace file will roll over. This means that if messages are being logged to file `tsapispy.trc`, then the first time the trace file rolls over, that file is renamed as `tsapispy.trc.1` and a new `tsapispy.trc` file is created to receive additional log output.

To generalize, if the Trace File Name is `tsapispy.trc` and the Maximum Number of Trace Files to Create is some value `n`, then each time the `tsapispy.trc` file reaches the maximum size:

1. The file `tsapispy.trc.n` is removed.
2. Any trace files (`tsapispy.trc.1`, `tsapispy.trc.2`, ..., `tsapispy.trc.n-1`) that exist are renamed as (`tsapispy.trc.2`, `tsapispy.trc.3`, ..., `tsapispy.trc.n`).
3. The file `tsapispy.trc` is renamed `tsapispy.trc.1`.
4. A new `tsapispy.trc` file is created to receive additional log output.

### Related links

[Limiting the amount of disk space](#) on page 72

## Limiting the amount of disk space

### Procedure

1. Within the TSAPI Spy Log to File dialog box, set the check box for **Use Multiple Trace Files**.
2. Adjust the values for **Maximum Number of Trace Files to Create** and **Maximum Size for Each Trace File** based on your preferences.

## Creating a trace file

### Procedure

1. Click **Start > All Programs > Avaya AE Services > TSAPI Client > TSAPI Test**.
2. From the Telephony Services Spy for Win32 window, select **Options > Log To File**.  
Windows displays the Log to File dialog box.
3. On the Create Trace File dialog box, accept the default for Log Trace Messages (enabled).
4. In the **Trace File Name** field, type a name for the trace file (for example, `c:\cstatrace.txt`), or, choose a location by clicking **Browse**.
5. The default extension assigned to trace files is `.trc`, but you can use any filename and extension.

- If you would like the trace messages to be logged to a single file that grows without bound, clear the check box for **Use Multiple Trace Files** and click **OK**.

 **Important:**

Use this option with care to avoid using excessive disk space.

- If you would like to control the amount of disk space consumed by the trace files, set the check box for **Use Multiple Trace Files**. Then adjust the values for **Maximum Number of Trace Files to Create** and **Maximum Size for Each Trace File** based on your preferences and click **OK**.

## Turning off Log to File

### About this task

Use this procedure when you want to stop TSAPI Spy from writing output to the trace file.

### Procedure

- Select **Options > Log To File**.
- Clear the **Log Trace Messages** check box.

All of the options become disabled.

- Click **OK**.

TSAPI Spy displays an information box that prompts you to confirm that you want to close the trace file.

- Click **OK**.

TSAPI Spy closes the trace file.

## Streams list

When you first start TSAPI Spy, **Tracing** and **Auto-Trace New Streams** are enabled by default. When **Tracing** is enabled, all connections that are currently open are traced. When **Auto-Trace New Stream** is enabled, tracing is enabled when a new connection is opened.

## Indicating that tracing is enabled for a connection

### About this task

To indicate that the tracing is enabled for a connection (or connections), TSAPI Spy highlights the connection displayed in the streams list. Follow the procedure below:

### Procedure

- To disable Tracing for all streams, select the **Disabled** option button.
- To disable Auto-Trace New Streams, select **Options > Auto-Trace New Streams**. When you clear the check mark for **Auto-Trace New Streams**, tracing is not enabled for a new connection when it is opened.

## Trace output

To understand trace output, think of the client library as a two-way pipeline, with messages entering and leaving both ends. Messages may originate or terminate in one of three places:

- the application
- the TSAPI Service
- the client library (for internal events)

The trace records track the progress of a message through the pipeline, enabling you to determine which messages have been sent and whether or not they have reached their destination.

Normally, two trace records are generated for each message: one as it enters the pipeline, and one as it exits. Messages entering and leaving the application side (or the library itself) are presented in detail, with the value of each data element displayed in an appropriate format. The corresponding trace records to or from the TSAPI Service only indicate successful transport of the message across the network.

## TSAPI Spy Trace Records

Trace records displayed in the Output window (or trace file) are separated by blank lines. Each begins with a time stamp and one of the following phrases which describes the record:

- RECEIVED FROM APPLICATION - the application has generated a message to be delivered to the TSAPI Service. The message is displayed in detail.
- RECEIVED FROM TSERVER - a message from the TSAPI Service has arrived in the client library receive queue. Notification only.
- DELIVERED TO APPLICATION - the application has accepted the message from the client library. The message is displayed in detail.
- FROM LIBRARY - the client library has generated an internal message to be delivered to the TSAPI Service. The message is displayed in detail.
- FOR LIBRARY - the client library has accepted an internal message from the TSAPI Service. The message is displayed in detail.

A typical request from an application generates three trace records, in the following sequence: RECEIVED FROM APPLICATION, RECEIVED FROM TSERVER, DELIVERED TO APPLICATION. An event report from the TSAPI Service generates only the latter two records. Trace records from multiple messages may be interleaved.

## TSAPI Spy Error Records

Certain network errors are also reported by TSAPI Spy. These reports are displayed in the following form:

- CONNECTION TERMINATED BY TSERVER (condition code = xxxx)

where xxxx is a numerical error code in hexadecimal notation. The most common error codes reported are:

- 2745 (this means the connection is aborted)
- 2746 (the connection has been reset)
- 2742 (the network is down)
- CONNECTION TERMINATED BY CLIENT LIBRARY (condition code = 0), which indicates that the client has detected a loss of connectivity with the AE Services Server

Other codes are possible under unusual conditions. Report the code to technical support when you request assistance.

---

## Client message tracing for Linux-based TSAPI clients

For Linux-based clients, the message tracing ability is built into the shared client library file (`libcsta.so`). The tracing capability allows a user to log the flow of messages through applications using the TSAPI Linux clients.

Messages are traced as they enter and leave the library in both directions, from applications to the TSAPI Service and from the TSAPI Service to applications. Trace messages are written directly to a file specified by the user. Message tracing is performed on an application-by-application basis, according to each application's environment settings.

### Enabling message tracing

#### About this task

Use this procedure to enable the TSAPI Message Tracing feature.

#### Procedure

Set and export the environment variable `CSTATRACE` before starting your TSAPI application. The `CSTATRACE` environment variable specifies the name of the file where the TSAPI messages will be logged.

### About Message Tracing feature

You can control the amount of disk space used by the TSAPI Message Tracing feature by setting and exporting the following additional environment variables:

- `CSTATRACE_MAX_FILE_INDEX` - This environment variable controls the number of TSAPI trace files that will be created.

Each time the trace file reaches its maximum size (see `CSTATRACE_MAX_FILE_SIZE`, described below), the trace file will roll over. This means that if messages are being logged to file `cstatrace`, then the first time the trace file rolls over, that file is renamed as `cstatrace.1` and a new `cstatrace` file is created to receive additional log output.

To generalize, if messages are being logged to file `cstatrace` and `CSTATTRACE_MAX_FILE_INDEX` is set to some value `n`, then each time the `cstatrace` file reaches its maximum size:

- The file `cstatrace.n` is removed.
- Any trace files (`cstatrace.1`, `cstatrace.2`, ..., `cstatrace.n-1`) that exist are renamed as (`cstatrace.2`, `cstatrace.3`, ..., `cstatrace.n`).
- The file `cstatrace` is renamed `cstatrace.1`.
- A new `cstatrace` file is created to receive additional log output.

In effect, the number of TSAPI trace files that may be created is limited to `CSTATTRACE_MAX_FILE_INDEX + 1`.

Valid values for `CSTATTRACE_MAX_FILE_INDEX` are 1-9. If `CSTATTRACE_MAX_FILE_SIZE` is set but `CSTATTRACE_MAX_FILE_INDEX` is not set, then `CSTATTRACE_MAX_FILE_INDEX` defaults to 9.

- `CSTATTRACE_MAX_FILE_SIZE` - This environment variable controls the maximum size of each TSAPI trace file.

Valid values for `CSTATTRACE_MAX_FILE_SIZE` are 1-10000 (MB). If `CSTATTRACE_MAX_FILE_INDEX` is set but `CSTATTRACE_MAX_FILE_SIZE` is not set, then `CSTATTRACE_MAX_FILE_SIZE` defaults to 10 (MB).

When neither `CSTATTRACE_MAX_FILE_INDEX` nor `CSTATTRACE_MAX_FILE_SIZE` is set, then messages will be logged to a single file that grows without bound. Use caution when collecting TSAPI trace messages this way to avoid using excessive disk space.

Also, note that the TSAPI Message Tracing feature is provided for troubleshooting purposes only. Enabling this feature will degrade the performance of the TSAPI Linux client library.

## Trace file examination

Following is the sample output from a tracing session started by setting `CSTATTRACE`. The number that appears at the beginning of each line, is the ACS handle for the stream.

```

:
00722aa0: [10/26/09 19:26:44.444]
00722aa0: RECEIVED FROM APPLICATION:
00722aa0: InvokeID 00000002
00722aa0: ACSOpenStream ::=
00722aa0: {
00722aa0:   streamType stCsta,
00722aa0:   serverID "AVAYA#SCORPION#CSTA#LZMVAP244",
00722aa0:   loginID "jgresh",
00722aa0:   cryptPass '3A2578E343C2F56B95B84571F56B95 ...'H,
00722aa0:   applicationName "TSTEST",
00722aa0:   level acsLevel1,
00722aa0:   apiVer "TS1-2",
00722aa0:   libVer "AES6.3.3 Build 415",
00722aa0:   tsrvVer ""
00722aa0: }

00722aa0: [10/26/09 19:26:44.451]
00722aa0: DELIVERED TO APPLICATION:
00722aa0: InvokeID 00000002
00722aa0: ACSOpenStreamConfEvent ::=
00722aa0: {
00722aa0:   apiVer "ST2",
00722aa0:   libVer "AES6.3.3 Build 415",
00722aa0:   tsrvVer "6.3.3 Build 415",
00722aa0:   drvrVer "6.3.3 Build 415"
00722aa0: }

00722aa0: [10/10/13 19:26:44.452]
00722aa0: RECEIVED FROM APPLICATION:
00722aa0: InvokeID 00000003
00722aa0: CSTAMakeCall ::=
00722aa0: {
00722aa0:   callingDevice "32201",
00722aa0:   calledDevice "32202"
00722aa0: }
00722aa0: [10/26/09 19:26:44.599]
00722aa0: DELIVERED TO APPLICATION:
00722aa0: InvokeID 00000003
00722aa0: CSTAMakeCallConfEvent ::=
00722aa0: {
00722aa0:   newCall
00722aa0:   {
00722aa0:     callID 2261,
00722aa0:     deviceID "32201",
00722aa0:     devIDType staticId
00722aa0:   }
00722aa0: }

```

**Figure 9: Sample output from CSTA Trace**

# Appendix C: File naming conventions

---

## File naming conventions

The following file naming convention provides you with a convenient way of interpreting the file names of AE Services deliverable. This naming convention is not a formal standard, it is simply a guideline for reading file names.

<api>- <type>- <target>- <version> - <build> - <arch>.<suffix>

Where:

Name	Description
<api>-	Refers to the name of the API. For example, tsapi or cvlan
<type>-	Refers to the type of deliverable. Can be client-, sdk- or client-sdk (for ISOs).
<target>	Refers to the name of the operating system.
<version>	Refers to the software version.
- <build>	Refers to the software build number, preceded by a dash.  <b>Note:</b> This number changes frequently. It is often represented in this document by x instead of an actual build number.
-<arch>	Refers to the architecture, preceded by a dash.
.<suffix>	Refers to the file or package type.

### Examples

- TSAPI Windows client:

- tsapi-sdk-win32-10.2.x-23.zip
- tsapi-sdk-x86\_64-10.2.x-23.zip
- tsapi-client-win32-10.2.x-23.zip
- tsapi-client-x86\_64-10.2.x-23.zip

- TSAPI Linux client:

- tsapi-sdk-linux-10.2.x.rhel6-23.i386.bin
- tsapi-sdk-linux-10.2.x-23.i386.bin
- tsapi-sdk-linux-10.2.x-23.x86\_64.bin

- tsapi-client-linux-10.2.x.rhel6-23.i386.bin
- tsapi-client-linux-10.2.x-23.i386.bin
- tsapi-client-linux-10.2.x-23.x86\_64.bin
- TSAPI Windows SDK:
  - tsapi-sdk-win32-10.2.x-23.zip
  - tsapi-sdk-x86\_64-10.2.x-23.zip
- TSAPI Linux SDK:
  - tsapi-sdk-linux-10.2.x-94.bin
- CVLAN Windows client:
  - cvlan-client-win32-10.2.x-23.zip
- CVLAN Linux client:
  - cvlan-client-linux-10.2.x-23.bin
  - cvlan-client-linux-10.2.x.rhel6-23.bin

**\* Note:**

The numbers following the build version are subject to change. For example, the numbers following `tsapi-client-win32-10.2.x-` are subject to change.

The table applies the naming convention to the AE Services deliverables.

**Table 8: AE Services TSAPI and CVLAN software deliverables -- file names**

<api>-	<type>-	<target>-	<version>	-<build>	-<arch>	<suffix>
tsapi-	client-	linux-	10.2.x	-23	i386 or x86_64	.bin
tsapi-	client-	win32-	10.2.x	-23	NA	.zip
tsapi-	sdk-	linux-	10.2.x	-23	i386 or x86_64	.bin
tsapi-	sdk-	win32-	10.2.x	-23	NA	.zip
cvlan-	client-	linux-	10.2.x	-23	NA	.bin
cvlan-	client-	win32-	10.2.x	-23	NA	.zip

**\* Note:**

Build numbers change frequently. These numbers are provided as examples only.

# Glossary

<b>API</b>	Application Programming Interface. An API is a published specification that describes how to access the functions of a software-based service.
<b>ASAI</b>	Adjunct Switch Application Interface - ASAI is a protocol that enables software applications to access call processing capabilities provided by Avaya Aura <sup>®</sup> Communication Manager.
<b>Certificate Authority (CA)</b>	A certificate authority is an organization that issues and manages security credentials, including digitally signed certificates containing public keys for message encryption and decryption.
<b>Computer Telephony Integration</b>	Abbreviated as CTI. The integration of services provided by a computer and a telephone. In simplest terms, it means connecting a computer to a communications server (or switch) and having the computer issue commands that control calls. All services running on the AE Services (TSAPI, CVLAN, DLG, and DMCC) are CTI services.
<b>CT User</b>	Computer Telephony User. A user (or an application) administered in the AE Services User Service as a CT User derives authorization from the Security Database. CT Users include the following users or applications: TSAPI Service users (including JTAPI users), Telephony Web Service users, and Device, Media and Call Control users who use the Call Control Services (CSTA III Single-Step Conference, Snapshot Call, and Snapshot Device).
<b>CTI</b>	Computer Telephony Integration. CTI is the use of computers to manage telephone calls.
<b>CTI Link</b>	The term CTI link refers to a generic link type that is used in the context of Avaya Aura <sup>®</sup> Communication Manager administration. As a generic link type, it can refer to any of the following: AE Services links: CVLAN links, DLG links, and TSAPI links (JTAPI and the Telephony Web Service use TSAPI links). When an OAM Web page, such as TSAPI Service Summary, displays a column heading for a CTI link type, it is referring to TSAPI link as it is administered on Avaya Aura <sup>®</sup> Communication Manager. Up to 64 links can be administered on Avaya Aura <sup>®</sup> Communication Manager.
<b>CVLAN</b>	CallVisor/LAN is a C programming API based on the ASAI message set.

<b>JTAPI</b>	Java Telephony Application Programming Interface. JTAPI is a scalable, extensible API integrating both first-party and third-party call control models. The AE Services JTAPI implementation provides access to the complete set of Third Party call control features provided by the TSAPI Service. JTAPI uses the TSAPI Service for communication with Avaya Aura® Communication Manager. For information about JTAPI, see the Avaya Aura® Application Enablement Services JTAPI Programmer's Guide, 02-603488.
<b>Link</b>	A communications channel between system components.
<b>Operations, Administration, and Maintenance</b>	Abbreviated as OAM. The administrative interface for the Avaya Aura® Application Enablement Services platform.
<b>PEM</b>	Privacy Enhanced Mail is a file format for storing private keys, public keys, and certificates. A PEM file may contain either personal certificates or certificates from a Certificate Authority.
<b>Private Data</b>	Private data is a switch-specific software implementation that provides value added services.
<b>Routing</b>	Routing is selecting an appropriate path for a call. When a routing application is started, it sends route registration requests, which contain a device ID, to Avaya Aura® Communication Manager. Routing requests instructs the Avaya Aura® Communication Manager to send all incoming calls to these device IDs (in the TSAPI Service). The TSAPI Service sends the call to the application for routing. Avaya Aura® Communication Manager does not route these calls, also referred to as adjunct routing.
<b>SDK</b>	A Software Development Kit is a package that enables a programmer to develop applications for a specific platform. Typically, an SDK includes one or more APIs, documentations, and, in some cases, programming tools.
<b>Tlink</b>	A Tlink is a service identifier that is created when the administrator adds a TSAPI Link in the AE Services OAM. A Tlink refers to a switch connection between a specific switch and a specific AE Services Server.
<b>TLS</b>	Transport Layer Security is a protocol intended to secure and authenticate communications across public networks through data encryption. TLS is an enhancement to SSL version 3, and is a proposed Internet Standard.
<b>TSAPI</b>	Telephony Services API is a C- language based API for third-party call and device control, and based on CSTA standards.

# Index

## Special Characters

.trc ..... [72](#)  
/usr/lib/tslibrc file ..... [37](#)

## A

accessing port matrix ..... [55](#)  
aesCerts.cer ..... [22](#)  
AESRV1 ..... [32](#)  
alternate location ..... [30](#)  
alternate tlinks ..... [32](#)  
alternate Tlinks ..... [20](#)  
Alternate Tlinks ..... [31](#)  
ASAI test ..... [52](#)  
    link number ..... [52](#)  
    utility ..... [52](#)  
authentication ..... [64](#)  
Avaya CT SDK ..... [41](#)  
Avaya Product Certificate Authority certificate ..... [60](#)  
Avaya support website ..... [58](#)

## B

backward compatibility ..... [5](#)

## C

centrally-located configuration file ..... [26](#)  
certificate ..... [62](#)  
    authentication ..... [22](#)  
    certificate authority ..... [63](#)  
certificate administration ..... [64](#)  
certificate authentication  
    server .....  
    validity ..... [65](#)  
certificate authentication for TSAPI CVLAN ..... [60](#)  
Certificate Authority ..... [21](#)  
certificate management ..... [47, 60, 64](#)  
certificate revocation check ..... [36](#)  
checklist  
    IP address ..... [10](#)  
checklist for setting up TSAPI and CVLAN ..... [65](#)  
Citrix ..... [12](#)  
client build number ..... [28](#)  
client certificate authentication  
    specification ..... [33](#)  
client configuration  
    certificate ..... [19](#)  
client directory ..... [26](#)  
client keystore ..... [66, 67](#)  
client platforms ..... [48](#)

client version number ..... [28](#)  
client's trusted certificate ..... [60](#)  
clients and SDKs ..... [7](#)  
collection  
    delete ..... [56](#)  
    edit name ..... [56](#)  
    generating PDF ..... [56](#)  
    sharing content ..... [56](#)  
configuration statements ..... [67](#)  
content  
    publishing PDF output ..... [56](#)  
    searching ..... [56](#)  
    sharing ..... [56](#)  
    sort by last updated ..... [56](#)  
    watching for updates ..... [56](#)  
CSTA ..... [40](#)  
cstatrace ..... [75](#)  
CSTATRACE ..... [75, 76](#)  
CSTATRACE\_MAX\_FILE\_INDEX ..... [75](#)  
CT user ..... [20](#)  
customize tslib.ini ..... [26](#)  
CVLAN  
    installing Windows client ..... [49](#)  
    installing Windows Client ..... [49](#)  
CVLAN client ..... [64](#)  
CVLAN Client ..... [46](#)  
CVLAN service ..... [46](#)  
CVLAN-related administrative tasks ..... [65](#)

## D

default certificate  
    location ..... [62](#)  
default location  
    configuration ..... [62](#)  
documentation  
    Application Enablement Services ..... [54](#)  
documentation center ..... [56](#)  
    finding content ..... [56](#)  
    navigation ..... [56](#)  
documentation portal ..... [56](#)  
    finding content ..... [56](#)  
    navigation ..... [56](#)  
download PLDS ..... [7](#)  
downloading  
    clients and SDKs from Avaya Support ..... [8](#)  
    clients from Avaya DevConnect ..... [9](#)  
    downloading software from plds ..... [7](#)  
downloading client and SDKs ..... [7](#)

## E

edit

edit ( <i>continued</i> )		location ( <i>continued</i> )	
customize TSAPI windows .....	<a href="#">19</a>	configuration .....	<a href="#">67</a>
TSLIB.INI .....	<a href="#">19</a>	password .....	<a href="#">67</a>
Edit TSLIB.INI .....	<a href="#">16</a>	log trace messages .....	<a href="#">73</a>
encrypted client connections .....	<a href="#">60</a>		
encrypted Tlinks		<b>M</b>	
avaya product root .....	<a href="#">32</a>	maintenance agreements .....	<a href="#">7</a>
environment variable		message tracing .....	<a href="#">75</a>
CLIENT_KEYSTORE .....	<a href="#">67</a>	My Docs .....	<a href="#">56</a>
KEYSTORE_PWD .....	<a href="#">67</a>		
examination .....	<a href="#">76</a>	<b>N</b>	
example sample code .....	<a href="#">43</a>	naming conventions	
		deliverable .....	<a href="#">78</a>
<b>F</b>		network based .....	<a href="#">25</a>
finding content on documentation center .....	<a href="#">56</a>	network drive .....	<a href="#">26</a>
finding port matrix .....	<a href="#">55</a>	new connection is opened .....	<a href="#">73</a>
firewall .....	<a href="#">30</a>		
firewall administration .....	<a href="#">41</a>	<b>O</b>	
		operating system requirement .....	<a href="#">12</a>
<b>G</b>		outage .....	<a href="#">26</a>
gold or platinum DevConnect member .....	<a href="#">41</a>	own certificate .....	<a href="#">64</a>
<b>H</b>		<b>P</b>	
host name .....	<a href="#">10, 27</a>	port 450 .....	<a href="#">13, 30</a>
		port 453 .....	<a href="#">13, 30</a>
<b>I</b>		port matrix .....	<a href="#">55</a>
in-house certificate authority .....	<a href="#">32</a>	previous version .....	<a href="#">45, 51</a>
InSite Knowledge Base .....	<a href="#">58</a>	Privacy Enhanced Mail .....	<a href="#">47</a>
installation			
CVLAN Linux Client		<b>R</b>	
RPM .....	<a href="#">50</a>	removing CVLAN Linux Client .....	<a href="#">51</a>
Linux .....	<a href="#">50</a>	removing TSAPI Linux SDK .....	<a href="#">45</a>
installation for TSAPI Windows client		RPM .....	<a href="#">28</a>
scenarios .....	<a href="#">25</a>	rpm -e cvlan-client-linux .....	<a href="#">51</a>
installation RPM .....	<a href="#">44</a>	run-time libraries .....	<a href="#">41</a>
Installing CVLAN Windows Client .....	<a href="#">49</a>	runtime libraries .....	<a href="#">46</a>
Installing TSAPI Linux client .....	<a href="#">28</a>		
Installing TSAPI Linux SDK .....	<a href="#">44</a>	<b>S</b>	
Installing TSAPI Windows SDK .....	<a href="#">41</a>	Scripting Instructions .....	<a href="#">43</a>
IP address		searching for content .....	<a href="#">56</a>
external .....	<a href="#">41</a>	secure Tlinks .....	<a href="#">27</a>
		server .....	<a href="#">60, 62</a>
<b>L</b>		server certificate authentication .....	<a href="#">33</a>
latest version of SDK .....	<a href="#">45</a>	server certificate request .....	<a href="#">65</a>
libcsta.so .....	<a href="#">75</a>	service	
Linux		administrator .....	<a href="#">40</a>
hardware and software requirements		SHA-2 .....	<a href="#">60</a>
components .....	<a href="#">48</a>	share admin .....	<a href="#">26</a>
Operating Systems .....	<a href="#">48</a>	shared admin	
linux client .....	<a href="#">31</a>	drawback	
location			

drawback ( <i>continued</i> )		TSAPI Windows and Linux client libraries	66
drawback ( <i>continued</i> )		TSAPI windows client	26, 27
outage	28	TSAPI Windows client	16
shared client library file	75	installation	13
shared TSLIB.INI	28	TSAPI windows client configuration file	19
sharing content	56	TSAPI Windows Client only	41
shell environment variable	30	TSAPI Windows SDK components	43
sort documents by last updated	56	TSAPI-related administrative tasks	65
stop TSAPI Spy from writing output	73	TSLIB	
support	58	trace messages	69
		TSAPI Spy	69
		tslib.ini	22
		tslib.ini configuration	21
		tslibrc configuration file	30
		tslibrc file	30
<b>T</b>		<b>U</b>	
telephony servers	69	uninstall	
third-party certificate authority	32, 47, 64	CVLAN windows client	50
Tlinks	10	TSAPI windows client	18
trace file		uninstall TSAPI Windows SDK	
create	72	Windows	43
Trace Messages	72	upgrading	
tracing	73	CVLAN windows client	50
tracing is enabled for a connection	73	upgrading CVLAN Linux Client	51
training	57	upgrading TSAPI Linux SDK	45
transport layer security	21, 32	upgrading TSAPI Windows SDK	
trusted in-house certificate authority	64	installation	44
TSAPI and CVLAN clients	64	utility	
TSAPI client	21, 26	ms-dos prompt	52
SDK	11		
verifying installation	17	<b>V</b>	
TSAPI client and SDK	41	version	40
TSAPI client library	20, 67	videos	57
TSAPI exerciser	41	<b>W</b>	
TSAPI Exerciser	43	watch list	56
TSAPI links	40	windows 8	18
TSAPI links are encrypted	10	Windows 8	16
TSAPI Linux client		windows interface	69
remove	39		
upgrade	40		
TSAPI Linux client installation	37		
TSAPI Linux clients	75		
TSAPI Message Tracing	75		
TSAPI SDK CD	41		
TSAPI SDK Readme	43		
TSAPI service	18, 20, 21		
TSAPI spy	18		
TSAPI Spy	16		
client library model	74		
error records			
reported by TSAPI Spy	74		
file logging	72		
trace file	72		
trace records	74		
TSAPI Spy highlights	73		
TSAPI Spy Log			
disk space	72		
TSAPI Spy menu options	69		
TSAPI test	18		
TSAPI test session	37		