Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide

Release 7.0
Issue 2
May 2016

© 2015-2016, Avaya, Inc.
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 mediums which may include product information, 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

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, and 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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 Inc.

Avaya Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 6
- Purpose 6
- Intended audience 6
- Document changes since last issue 6
- Related documents 6
  - Documentation 6
  - Viewing Avaya Mentor videos 12
- TSAPI and CVLAN backward compatibility 12
- Support 13
- Warranty 13

Chapter 2: Installation Prerequisites 15
- Download location for clients and SDKs 15
- Checklist for downloading client and SDKs 15
- Downloading software from Avaya PLDS 15
- Downloading TSAPI clients 17
  - Downloading clients and SDKs from Avaya Support 17
  - Downloading clients from Avaya DevConnect 18
  - Checklist for installing the TSAPI client 19

Chapter 3: AE Services TSAPI clients and SDKs installation 20
- TSAPI client and SDK operating system requirements 20
  - Installing the TSAPI Windows client 22
  - Accessing the TSAPI Windows client desktop components 24
  - Verifying the TSAPI Windows client installation 25
  - Using TSAPI Spy while running TSAPI Test 26
- Removing the TSAPI Windows client 27
  - Removing the TSAPI Windows client from a Windows 7 and 8 systems 27
  - Removing the TSAPI Windows client from a non-Windows 8 system 27
- Installing and configuring the TSAPI Linux Client 37
  - Installing the TSAPI Linux client 37
  - Linux client configuration file customization 38
  - TSAPI Links (Tlinks) 46
  - Port settings for a firewall administration 47
- Installing and managing the TSAPI Windows SDK 47
  - AE Services TSAPI SDK and the programming environment 47
  - Installing the TSAPI Windows SDK 47
  - Viewing the TSAPI Windows SDK Components 49
- Removing the TSAPI Windows SDK 49
  - Removing the TSAPI Windows SDK from a Windows 7 and 8 system 49
  - Removing the TSAPI Windows SDK from a non-Windows 8 system 50

Installing and managing the TSAPI Linux SDK..... 51
Installing the TSAPI Linux SDK..... 51
Removing the TSAPI Linux SDK..... 51
Upgrading the TSAPI Linux SDK..... 52
Chapter 4: AE Services CVLAN Client/SDK installation..... 53
The CVLAN Client..... 53
CVLAN client and certificate management..... 53
The CVLAN SDK..... 55
CVLAN client connections with AE Services..... 55
CVLAN Client/SDK requirements..... 55
Installing the CVLAN Windows Client/SDK..... 56
Upgrading the CVLAN Windows Client/SDK..... 57
CVLAN Windows Client/SDK removal..... 58
Removing the CVLAN Windows Client from a non-Windows 8 system..... 58
Removing the CVLAN Windows Client from a Windows 8 system..... 58
Installing the CVLAN Linux Client/SDK..... 59
Upgrading the CVLAN Linux Client/SDK..... 60
Removing the CVLAN Linux Client/SDK..... 61
The ASAI test utility..... 61
Using the ASAI test utility..... 61
Appendix A: Certificate management..... 63
Server certificate authentication..... 63
Location and usage of Avaya-installed certificate..... 64
Location of your own certificates..... 65
Usage of your own certificate..... 67
AE Services certificate administration..... 67
Checklist for setting up TSAPI and CVLAN - if you use your own certificates..... 68
Client certificate authentication..... 69
Usage of default client keystore location..... 69
Client keystore location and password configuration..... 70
Appendix B: TSAPI Client Message Tracing..... 72
TSAPI Spy - a Windows client message tracing tool..... 72
Overview of the TSAPI Spy for Windows interface..... 72
Creating a trace file..... 75
Trace output..... 77
Using TSAPI Spy with Windows 2003 Server..... 78
Client message tracing for Linux-based TSAPI clients..... 79
Enabling message tracing..... 79
About Message Tracing feature..... 79
Trace file examination..... 80
Appendix C: File naming conventions..... 82
Glossary..... 84

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.

Intended audience

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

Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated TSAPI and CVLAN backward compatibility for AE Services server 7.0.1.
- Updated TSAPI client and SDK operating system requirements.
- Updated CVLAN client operating system requirements.

Related documents

Documentation

The following table lists the related documents for Avaya Aura® Application Enablement Services. Most of the documents listed are Release 7.0. Those listed that are for earlier releases have not required an update and remain compatible with AE Services 7.0. Obtain the related documents and documents about other Avaya products mentioned in this guide from the Avaya Support website at https://support.avaya.com/

Document number	Title	Use this document to:	Audience	Release
Overview				
02-300360	*Avaya Aura® Application Enablement Services Overview and Specification*	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements	Sales Engineers, Solution Architects, Implementation Engineers, and Support personnel	7.0
02-602818	*Avaya Aura® Application Enablement Services Integration Guide for IBM® Sametime®*	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Implementation Engineers and Support personnel	7.0
Administration				
02-300357	*Administering and Maintaining Avaya Aura® Application Enablement Services*	Describes administrative tasks you will need to perform on Avaya Aura® Communication Manager as well as the Avaya Aura® Application Enablement Services Server.	Implementation Engineers and Support personnel.	7.0
Not applicable	*Avaya Aura® Application Enablement Services Online Help* (packaged with Application Enablement Services software and not available on the Web)		Implementation Engineers and Support personnel.	7.0
Not applicable	*Avaya Aura® Application Enablement Services TSAPI Exerciser Help* (Online, packaged with the AE Services TSAPI Client SDK software and not available on the Web)		Implementation Engineers and Support personnel.	7.0
Deploying				

Table continues…

Document number	Title	Use this document to:	Audience	Release
02-300355	*Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment*	Describes implementing of the tested product, characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Implementation Engineers, Support personnel, and Customers	7.0
Not applicable	*Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*	Provides procedures for deploying the Avaya Aura® Application Enablement Servicesvirtual application in the Avaya Aura® Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.	Implementation Engineers and Support personnel	7.0
02-601893	*Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products*	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Implementation Engineers and Support personnel	7.0
Programmers guides and Reference guides				
02-300362	*Avaya Aura® Application Enablement Services Web Services Programmer's Guide*	Describes the services provided by the following Web Service interfaces: • Telephony Web Service • System Management Service	Implementation Engineers and Support personnel	5.2
02-602658	*Avaya Aura® Application Enablement Services Device, Media*	Describes how to use the Avaya Aura® Application	Application Developers	7.0

Table continues…

Document number	Title	Use this document to:	Audience	Release
	and Call Control API .NET Programmer's Guide	Enablement Services Device, Media and Call Control (DMCC) API to develop, debug, and deploy .NET applications that require first party or third party device, media and call control		
Not applicable	*Avaya Aura® Application Enablement Services Device, Media, and Call Control .NET Programmer's Reference* (an HTML document is available on the Web only at the Avaya Support Site https://support.avaya.com/ or Avaya DevConnect Site http://www.avaya.com/devconnect).	Describes how to use the Avaya Aura® Application Enablement Services Device, Media and Call Control (DMCC) API to develop, debug, and deploy .NET applications that require first party or third party device, media and call control	Application Developers	7.0
02-300358	*Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer's Guide*	Describes how to use the Avaya MultiVantage Avaya Aura® Application Enablement Services Device, Media and Call Control API to develop and debug XML applications that require device, media and call Control.	Application Developers	7.0
Not applicable	*Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer 's Reference* (an HTML document is available on the Web only at the Avaya Support Site https://support.avaya.com/ or Avaya DevConnect Site http://www.avaya.com/devconnect).	Describes how to use the Avaya MultiVantage Avaya Aura® Application Enablement Services Device, Media and Call Control API to develop and debug XML applications that require device, media and call Control.	Application Developers	7.0
02-300359	*Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer 's Guide*	Describes how to use the Application Enablement (AE) Services Device, Media and Call Control API to develop, debug, and deploy applications that require first-party device and media control,	Application Developers	7.0

Table continues…

Document number	Title	Use this document to:	Audience	Release
		as well as third-party call control		
Not applicable	*Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site, https://support.avaya.com/ or Avaya DevConnect Site, http://www.avaya.com/devconnect)	Describes how to use the Application Enablement (AE) Services Device, Media and Call Control API to develop, debug, and deploy applications that require first-party device and media control, as well as third-party call control	Application Developers	7.0
Not applicable	*Avaya Aura® Application Enablement Services Device, Media, and Call Control Media Stack API Reference* (an HTML document is available on the Web only at the Avaya Support Site https://support.avaya.com/ or Avaya DevConnect Site http://www.avaya.com/devconnect).	Describes how to use the Avaya Aura® Application Enablement Services Device, Media and Call Control (DMCC) API to develop, debug, and deploy applications that require first party or third party device, media and call control	Application Developers	7.0
02-300543	*Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide*	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Implementation Engineers, Support personnel, and Customers.	7.0
02-300544	*Avaya Aura® Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference*	Primary documentation resource for developing and maintaining TSAPI based applications in an Avaya Communication Manager environment. TSAPI is the acronym for Telephony Services Application Programming Interface.	Application developers	7.0
02-300545	*Avaya Aura® Application Enablement Services TSAPI Programmer's Reference*	Primary documentation resource for developing and maintaining TSAPI based applications in an	Application developers	4.1

Table continues…

Document number	Title	Use this document to:	Audience	Release
		Avaya Communication Manager environment. TSAPI is the acronym for Telephony Services Application Programming Interface.		
02-300546	*Avaya Aura® Application Enablement Services CVLAN Programmer's Reference*	Provides you with enough general, basic information to develop CVLAN applications.	Application developers	4.1
02–603488	*Avaya Aura® Application Enablement Services JTAPI Programmer's Guide*	Describes you how to use the Avaya Aura® Application Enablement Services JTAPI implementation to develop, debug, and deploy telephony applications	Application developers	5.2
Not applicable	*Avaya Application Enablement Services JTAPI Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site, https://support.avaya.com/ or Avaya DevConnect Site, http://www.avaya.com/devconnect)	Describes you how to use the Avaya Aura® Application Enablement Services JTAPI implementation to develop, debug, and deploy telephony applications	Application developers	5.2
03-300549	*Avaya Application Enablement Services ASAI Technical Reference*	This Document protocol level reference manual for the Adjunct Switch Application Interface (ASAI). This part of the document contains general information about this manual.	Application developers	4.1
03-300550	*Avaya Aura® Application Enablement Services ASAI Protocol Reference*	This Document protocol level reference manual for the Adjunct Switch Application Interface (ASAI). This part of the document contains general information about this manual.	Application developers	3.1

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.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

    Note:

    Videos are not available for all products.

TSAPI and CVLAN backward compatibility

In AE Services Release 7.0.1, only the Transport Layer Security (TLS) 1.2 protocol is enabled by default. The lower level TLS protocols 1.0 and 1.1 are disabled by default.

Note:

According to the National Institute of Standards and Technology (NIST) Special Publication 800-52, TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on the TLS 1.0 protocol. The use of TLS 1.2 is strongly recommended.

This change may cause older AE Services clients (version AE Services 7.0 and earlier) that are using TLS, to fail to establish a secure socket connection to the AE Services 7.0.1 server. In order to achieve a more secure client/server socket connection, we encourage current client applications to use an AE Services 7.0 SDK where the TLS 1.2 protocol is supported.

Note:

The previously released AE Services 7.0 Windows TSAPI client (tsapi-client-win32) did not initially support TLS 1.2. It has been updated to support TLS 1.2. All the latest versions of the AE Services 7.0 SDKs support TLS 1.2.

If upgrading to AE Services 7.0 SDK is not a viable option, an AE Services administrator can enable the TLS 1.1 and/or TLS 1.0 protocol via the AE Services Management Console Web interface.

Note:

All three 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

The Telephony Services Application Programming Interface (TSAPI) Client, Release 7.0.1 is compatible with the following server releases:

- AE Services Release 7.0.x TSAPI Service.
- AE Services Release 6.3.x TSAPI Service.
- AE Services Release 5.2.x TSAPI Service.

CVLAN

The Call Visor Local Area Network (CVLAN) Client, Release 7.0.1 is compatible with the following server releases:

- AE Services Release 7.0.x CVLAN Service.
- AE Services Release Release 6.3.x CVLAN Service.
- AE Services Release 5.2.x CVLAN Service.

Support

Go to the Avaya Support website at http://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.

Warranty

Avaya provides a 90-day limited warranty on Application Enablement Services. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Application Enablement Services in the warranty period is available on the Avaya Support website at https://

support.avaya.com/ under **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

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

#	Task	✔	Links/Notes
1.	Download software from Avaya PLDS.		Downloading software from PLDS on page 15
2.	Download the TSAPI client.		Downloading clients and SDKs from Avaya Support on page 17

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 or the CVLAN client and SDK from the Avaya Product Licensing and Delivery System (Avaya PLDS) website .

The TSAPI client, CVLAN client, and SDK 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**.
   - Avaya Aura® Application Enablement Services TSAPI Client MS Windows 7.0.1
   - Avaya Aura® Application Enablement Services TSAPI Client MS Windows 7.0
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 6 7.0
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 5 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Windows 7.0.1
   - Avaya Aura® Application Enablement Services CVLAN Client Windows 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Linux for RHEL 6 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Linux for RHEL 5 7.0.
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. In the Save As dialog box, which displays the file name for example, `tsapi-client-win32-7.0.0-131.zip` click **Save** to the browsed folder on your system.

   The numbers following `tsapi-client-win32-7.0.0-` are subject to change.

   The system displays the Avaya Download Manager window. Use this window to monitor the status of your download. When the status is

   `Finished`

   your file is saved to the folder that you specified in the Save As dialog box.

9. 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.
10. Click **Log out** .
11. Close your browser.
12. For Windows clients, go to the folder that you specified in the Save as dialog box, and extract from the zip file.

Next steps

Start the installation .

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 **7.0**.
5. In the **Downloads** list, click one of the following:
   - Avaya Aura® Application Enablement Services TSAPI Client Windows 7.0
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 6 7.0
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 5 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Windows 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Linux for RHEL 6 7.0
   - Avaya Aura® Application Enablement Services CVLAN Client Linux for RHEL 5 7.0.

6. On the Downloads page, click the file name, for example `tsapi-client-win32-7.0-454.zip`.
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 7.0 TSAPI Client (Win32)
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 6 7.0
   - Avaya Aura® Application Enablement Services TSAPI Client Linux for RHEL 5 7.0.
6. Read and accept the license agreement, and then click **Download** .
7. Save the file to your computer. For example, `tsapi-client-win32-6.3.3-454.zip`.
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.

Beginning with AE Services 7.0.1, 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 7.0.1 will retain the default certificate for backward compatibility.

The AE Services 7.0.1 TSAPI and CVLAN client installation continues to install the default certificate. This is so that 7.0.1 clients can connect to AE Services servers 6.3.3 and older, as well as servers that have been upgraded to 7.0.1.

TSAPI client and SDK operating system requirements

The AE Services TSAPI client can be installed on the following client platforms:

- For information about Windows, see Table 1.
- For information about Linux, see Table 2.
- Citrix - Avaya supports multiple Citrix clients connected to a single Citrix Server running a TSAPI Windows client application. AE Services supports Citrix Client Metaframe XPE v4.0. For more information refer to the Citrix documentation at www.citrix.com.

Table 1: TSAPI Windows client and SDK - operating system requirements

Component	Requirements
CPU	Intel 8086 instruction set architecture
Windows 32-bit Client Platform Operating Systems	- Windows 8 Pro - Windows 8 Enterprise - Windows 7 Professional - Windows 7 Enterprise

Table continues…

Component	Requirements
	- Windows 7 Ultimate - Windows 2003 Server Standard Edition
Windows 64-bit Client Platform Operating Systems supporting TSAPI applications running in 32-bit compatibility mode	- Windows 8 Pro - Windows 8 Enterprise - Windows 7 Professional - Windows 7 Enterprise - Windows 7 Ultimate - Windows Server 2008 R2 - Windows Server 2012 R2

Table 2: TSAPI Linux client and SDK - hardware and software requirements

Component	Requirements
CPU	Intel 8086 instruction set architecture
Linux® Operating System 32-bit Versions	- Linux® Operating System ES v4.0 Update 6 - Linux® Operating System ES v5.0 Update 7 - Linux® Operating System ES v5.0 Update 8 - Linux® Operating System ES v5.0 Update 9 - Linux® Operating System ES v5.0 Update 10 - Linux® Operating System ES v6.0 Update 5
Linux® Operating System 64-bit Versions supporting TSAPI applications running in 32-bit compatibility mode	- Linux® Operating System ES v5.0 Update 7 - Linux® Operating System ES v5.0 Update 8 - Linux® Operating System ES v5.0 Update 9 - Linux® Operating System ES v5.0 Update 10 - Linux® Operating System ES v6.0 Update 5

Note:

To install the TSAPI Linux Client on a Linux® Operating System ES v5.0 system, you must perform a separate installation of the following RPM: `openssl097a-0.9.7a-9.el5_4.2.i386.rpm` This RPM is available with Linux® Operating System installation media and is also available for download at http://rpm.pbone.net.

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 theAvaya Aura® Application Enablement Services TSAPI Windows client, you must remove the Avaya CT TS Win32 client before you install the Avaya Aura® Application Enablement Services TSAPI Windows client.

About this task

Use the following procedure to install the TSAPI Windows client.

Note:

Use the network drive based installation procedure if you need 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 prior to installation.

Important:

Make sure you have completed the instructions for downloading the installation files and saving them to your computer. 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 that contains the TSAPI Windows client files that 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 warning The Avaya CT Win 32 Client needs to be uninstalled before the installation can continue. When you click **OK**, the installation program exits.
   - 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 your now?
     ```

   Click **Yes** to have the setup remove the earlier version of the TSAPI client software for you automatically. Your existing TSAPI client configuration settings will be preserved.

   After completing the search, 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. For 32-bit Windows platforms, the default destination folder is `C:\Program Files\Avaya\AE Services\TSAPI Client`. For 64-bit Windows platforms, the default destination folder is `C:\Program Files (x86)\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 host name and the IP address.

   a. In the **Host Name or IP Address** field type a valid host name 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, accept the default 450. If your installation uses more than one 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 are re-using 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**.

   Setup exits.

Next steps

Verify that the components in your configuration can communicate. See Verifying the TSAPI Windows client installation.

Related links

Customizing the tslib.ini file prior to installation on page 34

Downloading software from Avaya PLDS on page 15
Verifying the TSAPI Windows client installation on page 25

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. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **TSAPI Test**
   - For non-Windows 8, on the **Start** menu, click **All Programs** > **Avaya AE Services** > **TSAPI Client** > **TSAPI Test**
2. Select one of the following:
   a. **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`).
   b. **TSAPI Spy** - The TSAPI Spy (`TSSPY32.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.
   c. **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.
   d. **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.
   e. **OpenSSL License** - Open the `OpenSSL License file` to review the terms of the license. Select **OpenSSL License** to open the `OpenSSL License` file.
   f. **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
   g. **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 28
TSAPI Spy - a Windows client message tracing tool on page 72

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. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **TSAPI Test**
   - For non-Windows 8, 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® Communication Managerthat 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® 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® 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® 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 7.0.1 server with TLS 1.2 enabled, and the version of TSAPI client does not support TLS 1.2. The latest version of the AE Services 7.0 Windows TSAPI client (tsapi-client-win32) supports TLS 1.2. Installing the latest version of the TSAPI client may solve this problem.

Note:

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 26

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. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **TSAPI Test**
   - For non-Windows 8, 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 25

Removing the TSAPI Windows client

Removing the TSAPI Windows client from a Windows 7 and 8 systems

About this task

Use the following procedure to remove either the TSAPI Windows client or the Avaya CT Windows client from Windows 7 and 8 systems.

Procedure

1. Open the **Control Panel**.
2. From the Control Panel, click **Uninstall a program**.

   Windows displays the Programs and Features window.
3. Select **Avaya Application Enablement Services TSAPI Client**, and click **Uninstall**.

   A confirmation dialog box appears.
4. Click **Yes**.

   This 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.

Removing the TSAPI Windows client from a non-Windows 8 system

About this task

Use the following procedure to remove the TSAPI Windows client from a non-Windows 8 system.

Procedure

1. Click **Start > Control Panel**.
2. From the Control Panel, click **Add or Remove Programs**.

   Windows displays the Add or Remove Programs dialog box.
3. Select **Avaya Application Enablement Services TSAPI Client**, and click **Remove**.

   A confirmation dialog box appears.
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.

TSAPI Windows client upgrade

If you are upgrading from an older version of the Avaya Aura® Application Enablement Services TSAPI Windows client to a newer version, you do not need to remove the older version first. For upgrading see, Installing the TSAPI Windows client.

Related links

Installing the TSAPI Windows client on page 22

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. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **Edit TSLIB.INI**.
   - For non-Windows 8, 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 28

TSAPI Windows client configuration file field description

Name	Description
Telephony Servers	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): hostname=port_number or IPaddress=port_number. For example: aeserver.domain.com=450 or 192.168.123.44=450.
Config	Use this section to configure settings for server certificate and client certificate authentication if you are using secure (encrypted) TSAPI links. If

Table continues…

Name	Description
	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.
Alternate Tlinks	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.
Shared Admin	Use this section when you want to use a pointer to a server-based `tslib.ini` file. See Installing the next client by sharing a single `tslib.ini` 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 29
Installing the next client by sharing a single tslib.ini file among clients on page 36
TSAPI Windows client certificate authentication on page 30
Server certificate authentication using your own certificate on page 31

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. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **Edit TSLIB.INI**
   - For non-Windows 8, 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 46

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 6.3.3 and older and servers upgraded to AE Services 7.0.1, the self-signed certificate created during 7.0.1 fresh installation, or a CA certificate issued by a trusted in-house or third-party certificate authority or your own certificate.

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 63

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 Product Root CA 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.

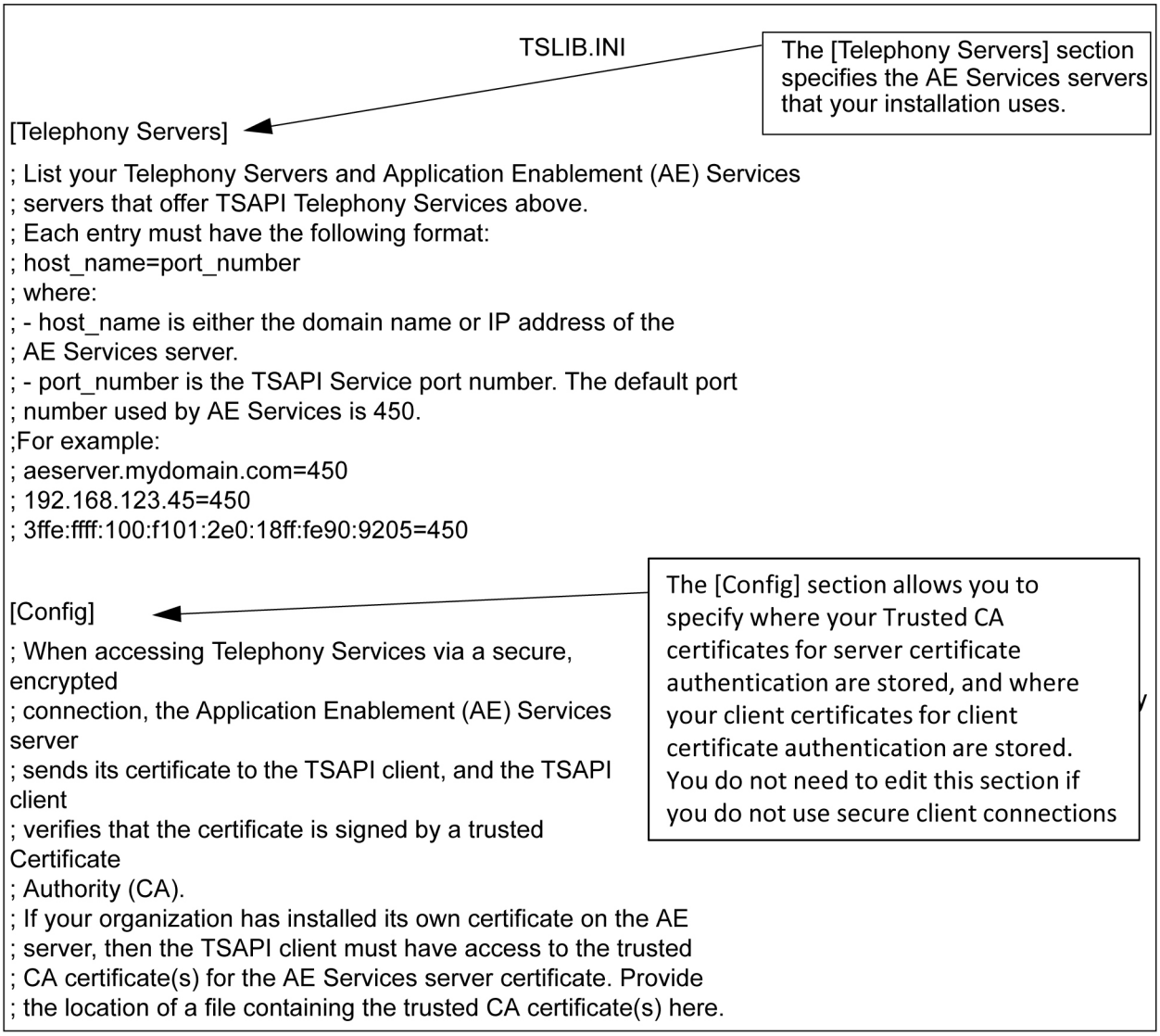


Figure 1: Sample tslib.ini file - Part 1

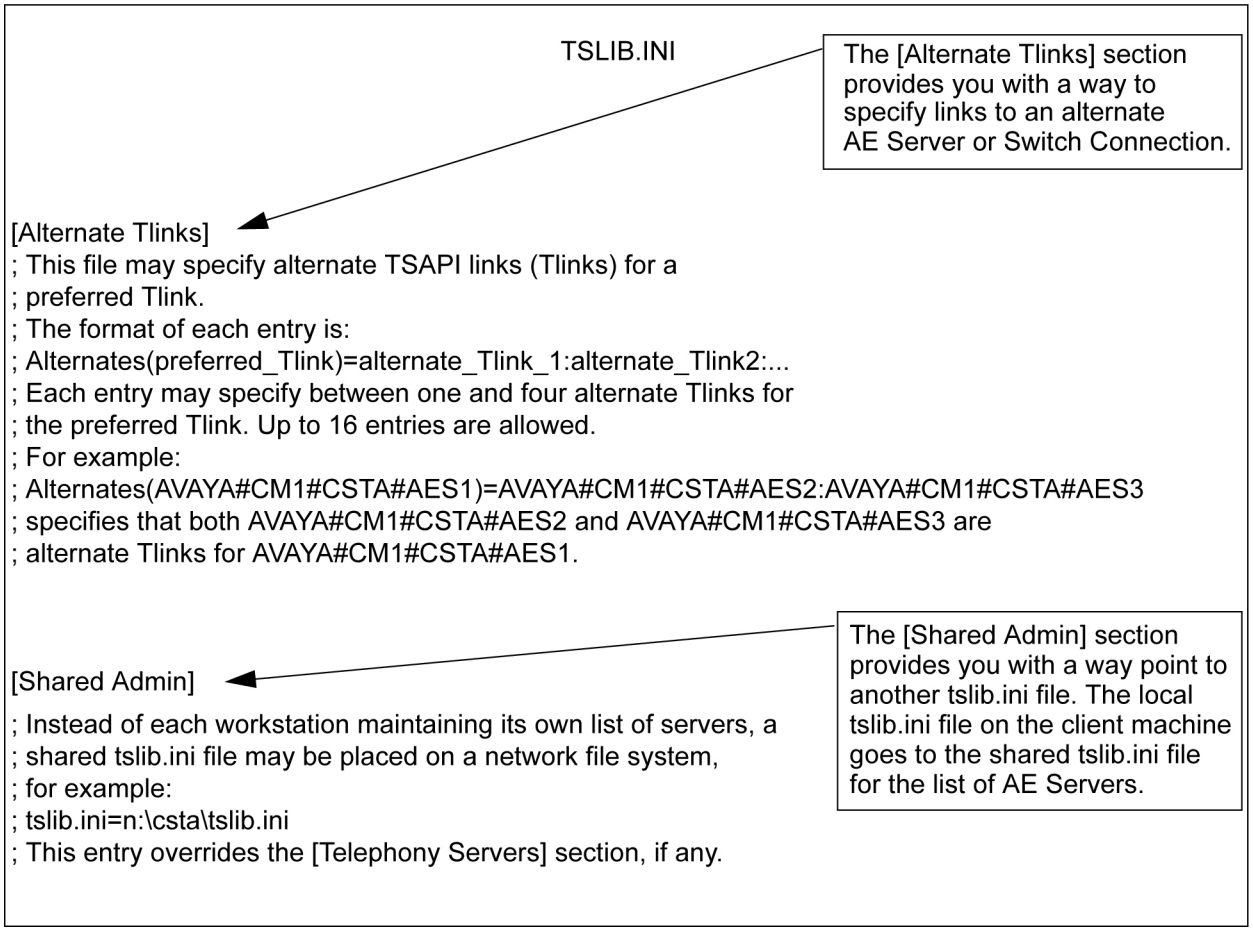


Figure 2: Sample tslib.ini file - Part 2

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 35
Installing the next client customizing the tslib.ini file prior to installation on page 36

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 35
Installing the next client by sharing a single tslib.ini file among clients on page 36

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, see Downloading software from PLDS.
- Before installing the TSAPI Linux Client on a Linux® Operating System ES v5.0 system, you may need to perform a separate installation of the following RPM: `openssl097a-0.9.7a-9.el5_4.2.i386.rpm` This RPM may be available with your Linux® Operating System installation media and is also available for download at http://rpm.pbone.net

Procedure

1. Log in to the client computer as **`root`**.
2. Go to the directory that contains the TSAPI Linux Client installation program `tsapi-client-linux-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-7.0-94.bin`.
4. Run the TSAPI Linux Client installation program to begin the installation. For example: `./tsapi-client-linux-7.0-94.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. See, Linux client configuration file customization.

Related links

Downloading software from Avaya PLDS on page 15
Linux client configuration file customization on page 38

Linux client configuration file customization

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 in `/usr/lib/tslibrc`.

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 `tslibrrec` 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`.

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.
2. Replace `127.0.0.1` with either the fully qualified domain name or the IP address of the AE Services Server that you want to gain access to, and the port number you want to use (450 is the default port number for the TSAPI Service).

   ```
   host_name port_number # comment
   ```

where:

- host_name is an Internet domain name or IP address (spaces are not valid in host names)
- port_number is the TCP port for the TSAPI Service's name. If the port number is omitted, a default value of 450 is assumed.
- # comment is the area to the right of the pound sign for comments.

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

Related links

Port settings for a firewall administration on page 47

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.
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® 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 46

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#CSTA#AESRV3:AVAYA#CM1#CSTA#AESRV4

In Example 1, there are two AE ServicesServers, AESRV1 and AESRV2, that each have a TSAPI link to the same switch, Avaya Aura® 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® 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, then the TSAPI client will attempt to use AESRV3.
- If AESRV3 is also unavailable, then the TSAPI client will attempt to use AESRV4.
- If AESRV4 is also unavailable, then 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=p@ssWord!

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

```
# /usr/lib/tslibrc - 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 default port number
#   used by AE Services is 450.
#
# For example:
#
# 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
#
# 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

# [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.
# For example:
#
# Trusted CA File=/usr/local/ssl/certs/verisign.pem
```

Figure 3: Editing the tslibrc 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

Using TSAPI Test to verify Linux client installations

Before you begin

Before performing this procedure, you must edit the `/usr/lib/tslibrc` 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*, 02-300544.

For information about CSTA messages see, Chapter 4 of the *Avaya Aura® Application Enablement Services TSAPI for Avaya Aura® Communication Manager Programmer's Reference*, 02-300544.

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 38
Example for a TSAPI test session on page 45
Example for a TSAPI test session on page 45

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
   ```

The Linux® Operating System 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
   ```

   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 45
Installing the TSAPI Linux client on page 37

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 theTSAPI 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 when 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*, 02-3005444, 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.

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-win32-7.0-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 32-bit Windows platforms, the default destination is `C:\Program Fles\Avaya\AE Services\SDKs\TSAPI` . For 64-bit Windows platforms, the default destination is `C:\Program Fles (x86)\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 49

Viewing the TSAPI Windows SDK Components

Procedure

1. Depending on the operating system, perform one of the following:
   - For Windows 8, on the **Start** menu, click **Avaya AE Services**
   - For non Windows 8 on the **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*, 02-300544.
   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 7 and 8 system

Procedure

1. Access the **Control Panel**.
2. From the Control Panel, click **Uninstall a program**.

   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.

Removing the TSAPI Windows SDK from a non-Windows 8 system

About this task

Use the standard Windows procedure to remove the TSAPI Windows SDK.

Procedure

1. From the desktop, go to **Start** > **Control Panel**.
2. From the Control Panel, click **Add or Remove Programs**.

   Windows displays the Add or Remove Programs dialog box.

3. Select **Avaya Application Enablement Services TSAPI SDK**, and click **Remove**.

   A confirmation dialog box appears.

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.

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, you do not need to remove the older version first. See, Installing the TSAPI Windows SDK to follow the installation procedure.

Related links

Installing the TSAPI Windows SDK on page 47

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-7.0-94.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
   ```

   The Linux® Operating System package manager removes the TSAPI Linux SDK.
3. To verify that the software has been removed, type the following command:

   ```
   rpm -q tsapi-sdk-linux
   ```

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 51
Removing the TSAPI Linux client on page 45
Installing the TSAPI Linux client on page 37
Installing the TSAPI Linux SDK on page 51

Chapter 4: AE Services CVLAN Client/SDK installation

The Avaya Aura® Application Enablement Services CVLAN Client/SDK, 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/SDK) are packaged together.

Note:

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

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.

Similarly, beginning with AE Services Release 6.3.3, 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 6.3.3, you may, 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.

Beginning with AE Services 7.0.1, 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 7.0.1 server can be exported and saved for the CVLAN client to use for development and testing purposes to an AE Services 7.0.1 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 certifcate(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 63

The CVLAN SDK

The CVLAN SDK provides additional software for developing and maintaining CVLAN based applications. The CVLAN SDK contains the following components for developing or updating your applications:

- CVLAN client (`cvlancli.dll` for Windows based systems and `libasai.so` for Linux systems)
- header files
- sample code
- utilities

For information about developing and maintaining CVLAN applications, see the *Avaya Aura® Application Enablement Services CVLAN Programmer's Reference*, 02-300546.

CVLAN client connections with AE Services

CVLAN application programs use the asai_open() and asai_open_port() functions to initiate connections to the AE Services Server.

Use the asai_open() function in your program to specify a non-secure connection for port number 9999 and a secure connection for any other port number. For more information, see the *Avaya Aura® Application Enablement Services CVLAN Programmer's Reference*, 02300546. See asai_open (3ASAI).

The asai_open_port() API call allows your program to specify a specific port number in the port_number parameter and to explicitly indicate whether the connection is secure. For more information, see *Avaya Aura® Application Enablement Services CVLAN Programmer's Reference*, 02300546. See asai_open_port (3ASAI).

CVLAN Client/SDK requirements

The AE Services CVLAN Client/SDK can be installed on the following client platforms:

- Windows
- Linux

Table 3: CVLAN Windows Client/SDK - hardware and software requirements

Component	Requirements
CPU	Intel 8086 instruction set architecture

Table continues…

Comments on this document? infodev@avaya.com

Component	Requirements
Windows 32-bit Client Platform Operating Systems	- Windows 8 Pro - Windows 8 Enterprise - Windows 7 Professional - Windows 7 Enterprise - Windows 7 Ultimate - Windows XP Professional - Windows 2003 Server Standard Edition
Windows 64-bit Client Platform Operating Systems supporting CVLAN applications running in 32-bit compatibility mode	- Windows 8 Pro - Windows 8 Enterprise - Windows 7 Professional - Windows 7 Enterprise - Windows 7 Ultimate - Windows Server 2008 R2 - Windows Server 2012 R2

Table 4: CVLAN Linux Client/SDK - hardware and software requirements

Component	Requirements
Linux® Operating System 32-bit Versions	Linux® Operating System ES v5.0 Update 8 Linux® Operating System ES v5.0 Update 9 Linux® Operating System ES v5.0 Update 10
Linux® Operating System 64-bit Versions supporting CVLAN applications running in 32-bit compatibility mode	Linux® Operating System ES v5.0 Update 8 Linux® Operating System ES v5.0 Update 9 Linux® Operating System ES v5.0 Update 10

Installing the CVLAN Windows Client/SDK

About this task

Follow this procedure to install the CVLAN Windows Client/SDK 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 and SDKs.

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/SDK 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 32-bit Windows platforms, the default destination folder is `C:\Program Files\Avaya\AE Services\CVLAN`. 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 61
Download location for clients and SDKs on page 15

Upgrading the CVLAN Windows Client/SDK

About this task

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

Procedure

1. Remove the previous version of the Client/SDK. Depending on the operating system see, Removing the CVLAN Windows Client from a non-Windows 8 or Removing the CVLAN Windows Client from a Windows 8 system
2. Install the latest version of the Client/SDK. See Installing the CVLAN Windows Client/SDK.

Note:

Although it is not a requirement that you remove the previous version of the Client/SDK, it is strongly recommended.

Related links

Removing the CVLAN Windows Client from a non-Windows 8 system on page 58
Removing the CVLAN Windows Client from a Windows 8 system on page 58
Installing the CVLAN Windows Client/SDK on page 56

CVLAN Windows Client/SDK removal

Removing the CVLAN Windows Client from a non-Windows 8 system

About this task

Use this procedure to remove the CVLAN Windows Client/SDK from a non-Windows 8 system.

Procedure

1. From the desktop, click **Start** > **Control Panel**.
2. From the Control Panel, click **Add/Remove Programs**.

   Windows displays the Add/Remove Programs Properties dialog box.
3. Select **Avaya Application Enablement Services CVLAN Client**, and click **Remove**.

   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**.

Removing the CVLAN Windows Client from a Windows 8 system

About this task

Use this procedure to remove the CVLAN Windows Client/SDK from a Windows 8 system.

Procedure

1. Access **Control Panel**.

2. From the Control Panel, click **Uninstall a program**.

   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 the CVLAN Linux Client/SDK

About this task

Before installing this release of the CVLAN Linux Client on a Linux® Operating System ES v5.8 system, you may need to perform a separate installation of the following RPM:

`openssl097a-0.9.7a-9.el5_4.2.i386.rpm`

Note:

This is valid is you are using the RHEL5 version of the CVLAN client.

This RPM may be available with your Linux® Operating System installation media and is also available for download at http://rpm.pbone.net.

Use this procedure to install the CVLAN Linux Client/SDK.

Note:

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 and SDKs.

Note:

Before installing this release of the CVLAN Linux Client on a Linux® Operating System ES v5.8 system, you may need to perform a separate installation of the following RPM: `openssl097a-0.9.7a-9.el5_4.2.i386.rpm`. This RPM may be available with your Linux® Operating System installation media and is also available for download at http://rpm.pbone.net.

Procedure

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

   Where,

   - version is the CVLAN Linux Client/SDK version number.
   - build is the CVLAN Linux Client/SDK build number.

3. Use the **chmod** command to make the CVLAN Linux Client/SDK installation program executable. For example, `chmod +x cvlan-client-linux-7.0-94.bin`
4. Run the CVLAN Linux/Client SDK installation program to begin the installation. For example, `./cvlan-client-linux-7.0-94.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/SDK.

   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 61
Download location for clients and SDKs on page 15

Upgrading the CVLAN Linux Client/SDK

About this task

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

Procedure

1. Remove the previous version of the Client/SDK. See Removing the CVLAN Linux Client/SDK.
2. Install the latest version of the Client/SDK. See Installing the CVLAN Linux Client/SDK.

   Note:

   Although it is not a requirement that you remove the previous version of the Client/SDK, it is strongly recommended.

Related links

Removing the CVLAN Linux Client/SDK on page 61
Installing the CVLAN Linux Client/SDK on page 59

Removing the CVLAN Linux Client/SDK

About this task

Use this procedure to remove the CVLAN Linux Client/SDK.

Procedure

1. Log in to the client computer as **root**.
2. To remove the CVLAN Linux Client/SDK, 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.
        ```

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 6.3.3, only server certificate authentication was available. Beginning with AE Services Release 6.3.3, client certification authentication is also available.

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

Beginning with AE Services 7.0, 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 7.0.1, and AE Services servers on version 6.3.3 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 v5.0 system, may not be able to establish a secure connection to the CVLAN Service when using certificates with SHA2 , for example SHA256 signatures. Use certificates with SHA1 signatures instead.

The TSAPI and CVLAN Linux client, installed on RHEL ES v6.5 system, will be able to establish a secure connection to the CVLAN Service running on AE Services 7.0.1 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.

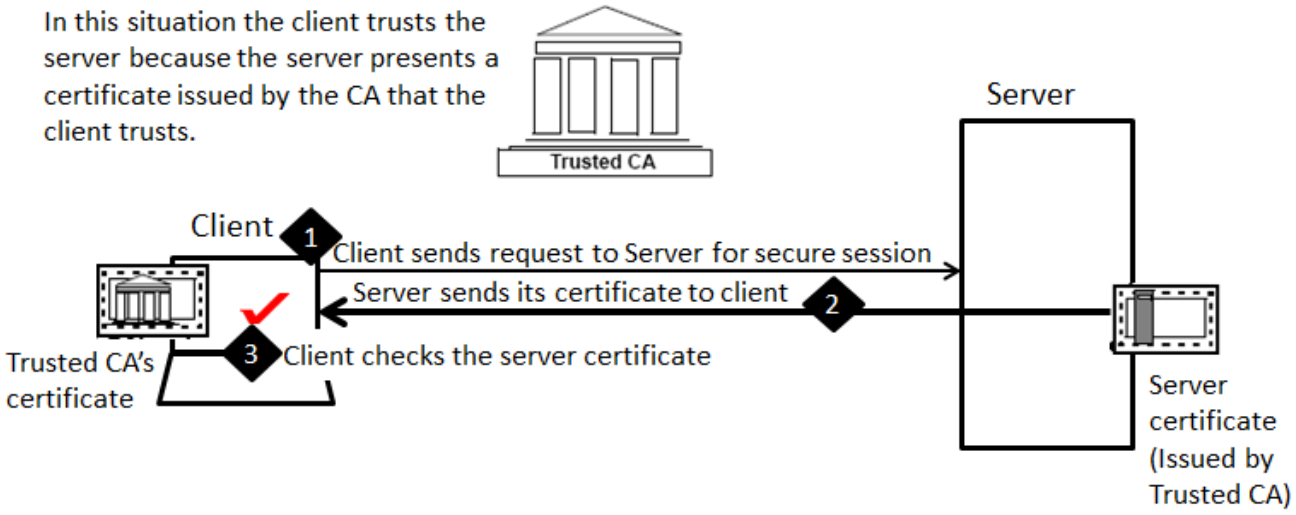


Figure 6: Server certificate authentication

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.

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 7.0.1 and servers on 6.3.3 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 6.3.3 and older.

The default server certificate should be for lab use only.

Table 5: 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:

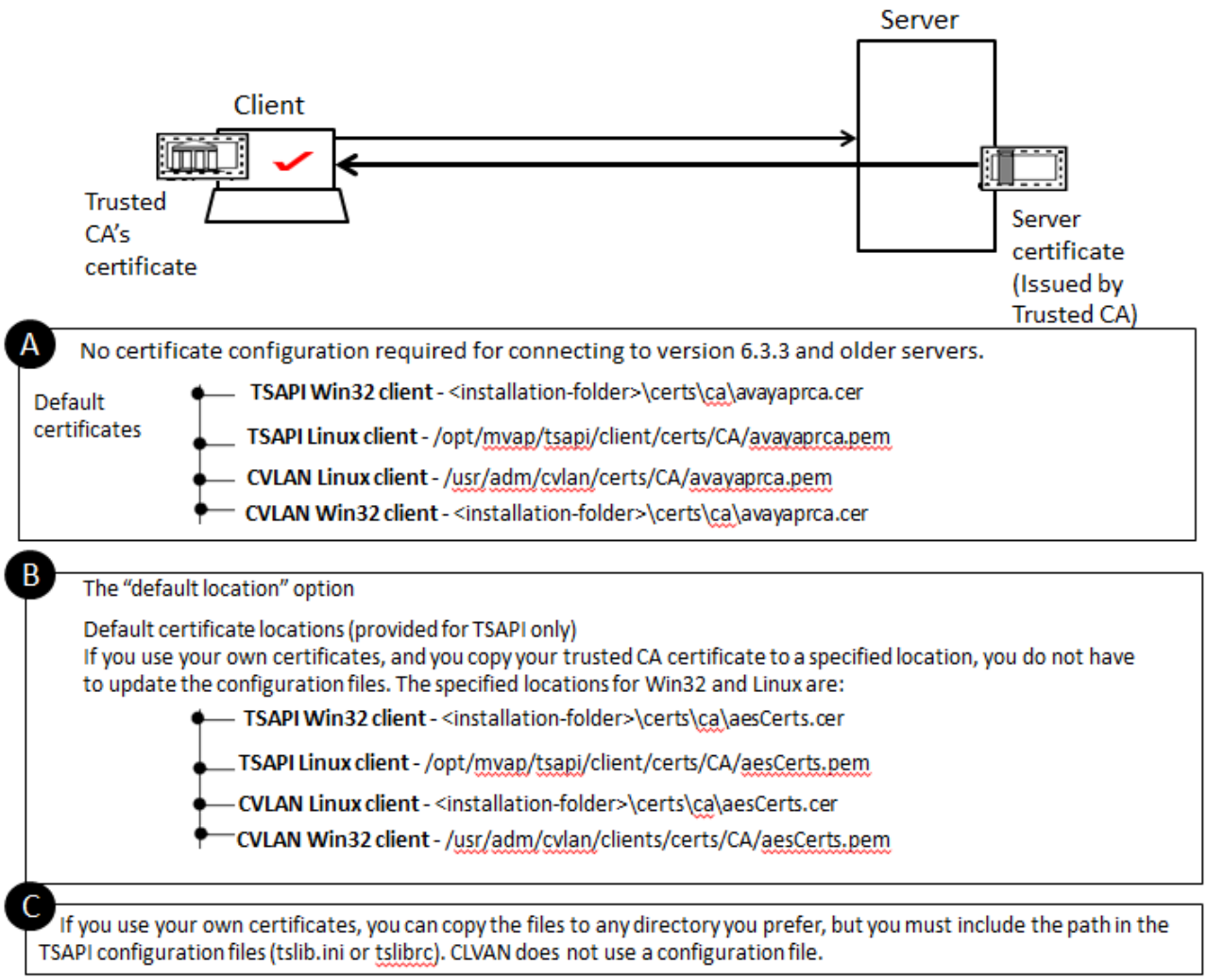


Figure 7: Where AE Services installs the CA certificate per-client

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 6: 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 40

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 53

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 7: 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 *Administering and Maintaining Avaya Aura® Application Enablement Services*, 02-30357.	
2.	Create an AE Services server certificate. See Creating a server certificate for AE Services in the *Administering and Maintaining Avaya Aura® Application Enablement Services*.	
3.	Import the server certificate into AE Services. See Importing the server certificate into AE Services in the *Administering and Maintaining Avaya Aura® Application Enablement Services*.	
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 *Administering and Maintaining Avaya Aura® Application Enablement Services*.	
CVLAN-related administrative tasks		
7.	Add a CVLAN link. See Administering CVLAN Links in the *Administering and Maintaining Avaya Aura® Application Enablement Services*.	
8.	Add a CVLAN client. See Adding CVLAN Clients in the *Administering and Maintaining Avaya Aura® Application Enablement Services*.	

Client certificate authentication

Beginning with AE Services Release 6.3.3, 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.

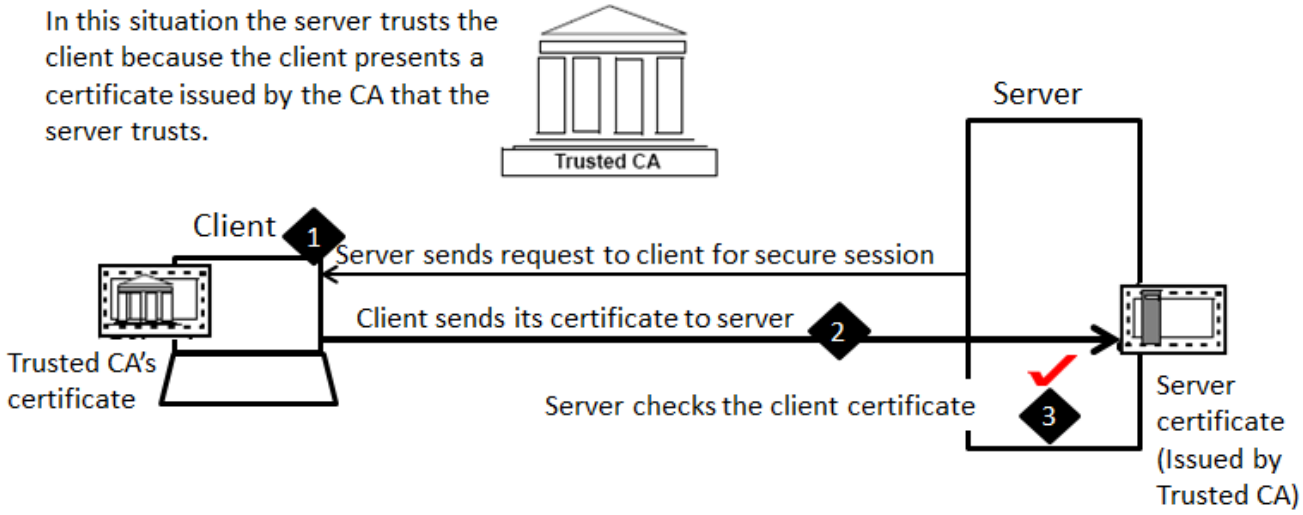


Figure 8: Client Certificate Authentication

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 8: 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 9: 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 69
Server certificate authentication using your own certificate on page 31
Certificate configuration statements addition to the tslibrc file on page 41

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.
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 69
CVLAN client and certificate management on page 53

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..	• Enabled - the default setting. When Tracing is enabled, message tracing information is displayed in the two display areas of the TSAPI Spy main window. • Disabled - Select **Disabled** to disable message tracing. Tracing can be disabled at any time while TSAPI Spy is running. If you disable tracing, and then exit **TSAPI Spy** (**File** > **Exit**), the next time you start TSAPI Spy, it will be Disabled.
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
Handle	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
Server ID	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.
Appl	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.
Login	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.
Output display window (grey background)	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.
Trace file status	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.
File	• **Exit** - Use menu item is used to exit TSAPI Spy. The system menu may also be used to exit the application.
Edit	• **Copy** - 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.

Table continues…

Name	Description
	• **Clear Buffer** - 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). • **Select All** - selects all of the text in the Output window. The Copy menu item can then be used. • **Purge Closed Streams** - 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.
Options All options, except Auto-Trace New Streams, are disabled by default	• **Always On Top** - 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). • **Auto-Trace New Streams** - 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). • **Show Internal Events** - causes non-application messages to be traced. The majority of messages normally traced through the `CSTA32.DLL` 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). • **Log To File** - 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).

Related links

Streams list on page 76
Usage of the Log to File option to direct output to a trace file on page 74

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.

Prior to Release 5.2, this option created a single log file that would grow without bound. Beginning with Release 5.2, 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 75

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. Depending on the operating system, perform one the following:
   - For Windows 8 on the **Start** menu click **TSAPI Test**
   - For non Windows 8 click on the **Start** menu click **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.
6. 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.
7. 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

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

   All of the options become disabled.
3. Click **OK**.

   TSAPI Spy displays an information box that prompts you to confirm that you want to close the trace file.
4. 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

1. To disable Tracing for all streams, select the **Disabled** option button.

2. 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.

Using TSAPI Spy with Windows 2003 Server

About this task

When using a standard Windows Remote Desktop Connection to start the TSAPI Spy on a Windows 2003-based server where the TSAPI application is running as a Windows service, the TSAPI Spy will not provide any trace messages. To capture the messages sent and received by the TSAPI application, the Remote Desktop Connection used to start the TSAPI Spy must connect to the console session.

Use this procedure to open a console session to the Windows 2003-based server:

Procedure

1. Click **Start** > **Run**.

   The Run dialog box appears.

2. Type `c:\windows\system32\mstsc.exe /console` and click **OK**.

   A Remote Desktop Connection window appears.

3. Complete the host name or IP address of the application, and configure any other options you want.

4. Click **Connect**.

   Note:

   Each computer has only one console session. When you connect to the console session remotely, other users may be unable to log on to the computer locally.

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

Beginning with Release 5.2 of the AE Services TSAPI Linux client, 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 CSTATRACE_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 CSTATRACE_MAX_FILE_INDEX + 1.

Valid values for CSTATRACE_MAX_FILE_INDEX are 1-9. If CSTATRACE_MAX_FILE_SIZE is set but CSTATRACE_MAX_FILE_INDEX is not set, then CSTATRACE_MAX_FILE_INDEX defaults to 9.

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

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

  When neither CSTATRACE_MAX_FILE_INDEX nor CSTATRACE_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 `CSTATRACE`. 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 '3A2578E343C2F56B95B84571FBF0F56B95 ...'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

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>.<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. **Note:** This number changes frequently. It is often represented in this document by x instead of an actual build number.
.<suffix>	Refers to the file or package type.

Examples

- TSAPI Windows client:
  - `tsapi-sdk-win32-7.0.0-131.zip`
  - `tsapi-client-win32-7.0.0-131.zip`
- TSAPI Linux client:
  - `tsapi-sdk-linux-7.0.0-131.bin`
  - `tsapi-sdk-linux-7.0.0rhel5-131.bin`
  - `tsapi-client-linux-7.0.0-131.bin`
  - `tsapi-client-linux-7.0.0.rhel5-131.bin`
- TSAPI Windows SDK:
  - `tsapi-sdk-win32-7.0-170.zip`
- TSAPI Linux SDK:
  - `tsapi-sdk-linux-7.0-94.bin`

- CVLAN Windows client and SDK:
  - `cvlan-client-win32-7.0.0-131.zip`
- CVLAN Linux client and SDK:
  - cvlan-client-linux-7.0.0-131.bin
  - cvlan-client-linux-7.0.0.rhel5-131.bin

Note:

The numbers following the build version are subject to change. For example, the numbers following `tsapi-client-win32-7.0.0-` are subject to change.

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

Table 10: AE Services TSAPI and CVLAN software deliverables -- file names

<api>-	<type>-	<target>-	<version>	-<build>	.<suffix>
tsapi-	client-	linux-	7.0	-170	`.bin`
tsapi-	client-	win32-	7.0	-170	`.zip`
tsapi-	sdk-	linux-	7.0	-170	`.bin`
tsapi-	sdk-	win32-	7.0	-170	`.zip`
cvlan-	client-	linux-	7.0	-70	`.bin`
cvlan-	client-	win32-	7.0	-70	`.zip`

Note:

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

Glossary

API	Application Programming Interface. An API is a published specification that describes how to access the functions of a software-based service.
ASAI	Adjunct Switch Application Interface - ASAI is a protocol that enables software applications to access call processing capabilities provided by Avaya Aura® Communication Manager.
Certificate Authority (CA)	A certificate authority is an organization that issues and manages security credentials, including digitally signed certificates containing public keys for message encryption and decryption.
Computer Telephony Integration	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.
CT User	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).
CTI	Computer Telephony Integration. CTI is the use of computers to manage telephone calls.
CTI Link	The term CTI link refers to a generic link type that is used in the context of Avaya Aura® 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® Communication Manager. Up to 64 links can be administered on Avaya Aura® Communication Manager.
CVLAN	CallVisor/LAN is a C programming API based on the ASAI message set.

JTAPI	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.
Link	A communications channel between system components.
Operations, Administration, and Maintenance	Abbreviated as OAM. The administrative interface for the Avaya Aura® Application Enablement Services platform.
PEM	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.
Private Data	Private data is a switch-specific software implementation that provides value added services.
Routing	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.
SDK	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.
Tlink	A Tlink is a service identifier that is created when the administrator adds a TSAPI Link in theAE Services OAM. A Tlink refers to a switch connection between a specific switch and a specific AE Services Server.
TLS	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.
TSAPI	Telephony Services API is a C- language based API for third-party call and device control, and based on CSTA standards.

Index

Special Characters

/usr/lib/tslibrc file 43
.trc 75

A

aesCerts.cer 31
AE Services
    Avaya Support
        devconnect 6
    documentation 6
    guide 6
AESRV1 40
alternate location 38
alternate tlinks 40
alternate Tlinks 29
Alternate Tlinks 39
ASAI test 61
    link number 61
    utility 61
authentication 67
Avaya CT SDK 47
Avaya CT Windows SDK 50
Avaya Product Certificate Authority certificate 63

B

backward compatibility 12

C

centrally-located configuration file 35
certificate 65
    authentication 31
    certificate authority 67
certificate administration 67
certificate authentication
    server .....
        validity 69
certificate authentication for TSAPI CVLAN 63
Certificate Authority 30
certificate management 53, 63, 67
changes document
    update
        issue 6
checklist
    IP address 19
checklist for setting up TSAPI and CVLAN 68
Citrix 20
client build number 37
client certificate authentication
    specification 41
client configuration
    certificate 28
client directory 35
client keystore 69, 70
client platforms 55
clients and SDKs 15
client upgrade
    TSAPI Windows 28
client version number 37
client's trusted certificate 63
configuration statements 70
CSTA 46
cstatrace 79
CSTATRACE 79, 80
CSTATRACE_MAX_FILE_INDEX 79
CT user 29
customize tslib.ini 34
CVLAN
    installing Windows Client 56
    installing Windows SDK 56
cvlancli.dll 55
CVLAN client 67
CVLAN Client/SDK 53
CVLAN-related administrative tasks 68
CVLAN service 53
CVLAN Windows Client 58

D

default certificate
    location 64
default location
    configuration 65
downloading
    clients and SDKs from Avaya Support 17
    clients from Avaya DevConnect 18
    downloading software from plds 15
downloading client and SDKs 15
download PLDS 15

E

edit
    customize TSAPI windows 28
    TSLIB.INI 28
Edit TSLIB.INI 24
encrypted client connections 63
encrypted Tlinks
    avaya product root 40
environment variable
    CLIENT_KEYSTORE 71
    KEYSTORE_PWD 71

examination 80
example sample code 49

F

firewall 38
firewall administration 47

G

gold or platinum DevConnect member 47

H

host name 19, 35

I

in-house certificate authority 40
installation
    CVLAN Linux Client/SDK
        RPM 59
    Linux 59
installation for TSAPI Windows client
    scenarios 34
installation RPM 51
Installing CVLAN Windows Client and SDK 56
Installing TSAPI Linux client 37
Installing TSAPI Linux SDK 51
Installing TSAPI Windows SDK 47
Intel 8086 instruction 55
IP address
    external 47

L

latest version of SDK 52
libasai.so 55
libcsta.so 79
limited warranty
    standard warranty 13
Linux
    hardware and software requirements
        components 55
    Operating Systems 55
linux client 39
location
    configuration 70
    password 70
log trace messages 76

M

maintenance agreements 15
messages sent and received by the TSAPI application 78
message tracing 79

N

naming conventions
    deliverable 82
network based 34
network drive 35
new connection is opened 76
non-Windows 8 system 58

O

operating system requirement 20
outage 35
own certificate 67

P

port 450 38
previous version 52, 60
Privacy Enhanced Mail 53

R

Remote Desktop Connection 78
Removing
    TSAPI Windows SDK 50
removing CVLAN Linux Client/SDK 61
removing TSAPI Linux SDK 51
RPM 37
rpm -e cvlan-client-linux 61
runtime libraries 53
run-time libraries 47

S

Scripting Instructions 49
secure Tlinks 35
server 63, 64
server certificate authentication 41
server certificate request 68
service
    administrator 46
SHA-2 63
share admin 35
shared admin
    drawback
        outage 36
shared client library file 79
shared TSLIB.INI 36
shell environment variable 38
stop TSAPI Spy from writing output 76
support 13

T

telephony servers 72

third-party certificate authority 40, 53, 67
Tlinks 19
trace file
create 75
Trace Messages 75
tracing 76
tracing is enabled for a connection 76
transport layer security 30, 40
trusted in-house certificate authority 67
TSAPI and CVLAN clients 67
TSAPI client 30, 34, 35
SDK 20
verifying installation 25
TSAPI client and SDK 47
TSAPI client library 29, 70
TSAPI exerciser 47
TSAPI Exerciser 49
TSAPI links 46
TSAPI links are encrypted 19
TSAPI Linux client
remove 45
upgrade 46
TSAPI Linux client installation 43
TSAPI Linux clients 79
TSAPI Message Tracing 79
TSAPI-related administrative tasks 68
TSAPI SDK CD 47
TSAPI SDK Readme 49
TSAPI service 26, 29, 30
TSAPI spy 26
TSAPI Spy 24
client library model 77
error records
reported by TSAPI Spy 78
file logging 74
trace file 74
trace records 77
TSAPI Spy highlights 76
TSAPI Spy Log
disk space 75
TSAPI Spy menu options 72
TSAPI test 26
TSAPI test session 43
TSAPI windows 27
TSAPI Windows and Linux client libraries 69
TSAPI windows client 35
TSAPI Windows client 24
installation 22
TSAPI windows client configuration file 28
TSAPI Windows Client only 47
TSAPI Windows SDK components 49
TSLIB
trace messages 72
TSAPI Spy 72
tslib.ini 31
tslib.ini configuration 30
tslibrc configuration file 38
tslibrc file 38

U

uninstall 27
CVLAN windows client 58
TSAPI windows client 27
uninstall program 58
uninstall TSAPI Windows SDK
Windows 49
upgrading
CVLAN windows client/SDK 57
upgrading CVLAN Linux Client/SDK 60
upgrading TSAPI Linux SDK 52
upgrading TSAPI Windows SDK
installation 50
utility
ms-dos prompt 61

V

version 46
videos 12

W

windows 8 27
Windows 8 24
windows interface 72