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

Chapter 1: Introduction............................................................................................................ 4
  Purpose................................................................................................................................. 4
  Intended audience................................................................................................................ 4
  Document changes since last issue.................................................................................... 4
  Related documents.............................................................................................................. 4
    Documentation.................................................................................................................... 4
    Viewing Avaya Mentor videos......................................................................................... 6
  TSAPI and CVLAN backward compatibility...................................................................... 7
  Support............................................................................................................................... 7
  Warranty.............................................................................................................................. 8

Chapter 2: Installation Prerequisites...................................................................................... 9
  Download location for clients and SDKs............................................................................ 9
  Checklist for downloading client and SDKs....................................................................... 9
  Downloading software from PLDS.................................................................................. 9
  Downloading TSAPI clients.............................................................................................. 11
    Downloading clients and SDKs from Avaya Support....................................................... 11
    Downloading clients from Avaya DevConnect............................................................... 12
    Checklist for installing the TSAPI client...................................................................... 12

Chapter 3: AE Services TSAPI clients and SDKs installation.................................................. 14
  TSAPI client and SDK operating system requirements..................................................... 14
    Installing the TSAPI Windows client without the host name and the IP address............. 15
    Installing the TSAPI Windows client............................................................................ 17
    Accessing the TSAPI Windows client desktop components......................................... 19
    Verifying the TSAPI Windows client installation......................................................... 20
    Using TSAPI Spy while running TSAPI Test................................................................ 21
  Removing the TSAPI Windows client............................................................................... 21
    Removing the TSAPI Windows client from a Windows 7 and 8 systems...................... 21
    Removing the TSAPI Windows client from a non-Windows 8 system........................... 22
  Installing and configuring the TSAPI Linux Client.......................................................... 31
    Installing the TSAPI Linux client.................................................................................. 31
    Linux client configuration file customization............................................................... 32
    TSAPI Links (Tlinks)........................................................................................................ 40
    Port settings for a firewall administration..................................................................... 41
  Installing and managing the TSAPI Windows SDK......................................................... 41
    AE Services TSAPI SDK and the programming environment........................................ 41
    Installing the TSAPI Windows SDK............................................................................ 41
    Viewing the TSAPI Windows SDK Components............................................................ 42
  Removing the TSAPI Windows SDK.............................................................................. 43
    Removing the TSAPI Windows SDK from a Windows 7 and 8 system......................... 43
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:

• Added a new section on Client certificate authentication on page 61.
• Updated TSAPI client and SDK operating system requirements on page 14.
• Updated TSAPI Windows client upgrade on page 22.
• Updated CVLAN client and certificate management on page 47.
• Updated TSAPI Windows client certificate authentication on page 25.

Related documents

The following table lists the related documents for Avaya Aura® Application Enablement Services. Most of the documents listed are Release 6.3.3. Those listed that are for earlier releases have not
required an update and remain compatible with AE Services 6.3.3. Obtain the related documents and documents about other Avaya products mentioned in this guide from the Avaya Support website: Avaya support site.

<table>
<thead>
<tr>
<th>Document title</th>
<th>Number</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Avaya Application Enablement Services Overview and Specification</td>
<td>02-300360</td>
<td>6.3.3</td>
</tr>
<tr>
<td>2. Implementing Avaya Application Enablement Services on Avaya Aura® System Platform</td>
<td>02–603468</td>
<td>6.3.3</td>
</tr>
<tr>
<td>3. Implementing Avaya Application Enablement Services in a Software-Only Environment</td>
<td>02-300355</td>
<td>6.3.3</td>
</tr>
<tr>
<td>4. Implementing Avaya Application Enablement Services for a Bundled Server Upgrade</td>
<td>02-300356</td>
<td>6.3.3</td>
</tr>
<tr>
<td>5. Avaya Application Enablement Services using VMware® in the Avaya Aura® Virtualized Environment Deployment Guide</td>
<td>Not applicable</td>
<td>6.3.3</td>
</tr>
<tr>
<td>6. Avaya Application Enablement Services Administration and Maintenance Guide</td>
<td>02-300357</td>
<td>6.3.3</td>
</tr>
<tr>
<td>8. Avaya Application Enablement Services Integration Guide for IBM Lotus Sametime</td>
<td>02-602818</td>
<td>6.3.3</td>
</tr>
<tr>
<td>9. Avaya Application Enablement Services Online Help (packaged with Application Enablement Services software and not available on the Web)</td>
<td>Not applicable</td>
<td>6.3.3</td>
</tr>
<tr>
<td>10. Avaya Application Enablement Services TSAPI Exerciser Help (Online, packaged with the AE Services TSAPI Client SDK software and not available on the Web)</td>
<td>Not applicable</td>
<td>6.3.3</td>
</tr>
<tr>
<td>11. Avaya Application Enablement Services Web Services Programmer’s Guide</td>
<td>02-300362</td>
<td>5.2</td>
</tr>
<tr>
<td>12. Avaya Application Enablement Services Device, Media and Call Control API .NET Programmer's Guide</td>
<td>02-602658</td>
<td>6.3.3</td>
</tr>
<tr>
<td>13. Avaya Application Enablement Services Device, Media, and Call Control .NET Programmer’s Reference (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)</td>
<td>Not applicable</td>
<td>6.3.3</td>
</tr>
<tr>
<td>15. Avaya Application Enablement Services Device, Media, and Call Control XML Programmer’s Reference (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)</td>
<td>Not applicable</td>
<td>6.3.3</td>
</tr>
<tr>
<td>16. Avaya Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide</td>
<td>02-300359</td>
<td>6.3.3</td>
</tr>
</tbody>
</table>
### 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 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**

**TSAPI**
The TSAPI Client, Release 6.3.1, is compatible with the following server releases:
  • AE Services Release 6.3.1 TSAPI Service
  • AE Services Release 6.3.0 TSAPI Service
  • AE Services Release 6.2.x TSAPI Service
  • AE Services Release 6.1.x TSAPI Service
  • AE Services Release 5.2.x TSAPI Service

**CVLAN**
The CVLAN Client, Release 6.3.1, is compatible with the following server releases:
  • AE Services Release 6.3.1 CVLAN Service
  • AE Services Release 6.3.0 CVLAN Service
  • AE Services Release 6.2.x CVLAN Service
  • AE Services Release 6.1.x CVLAN Service
  • AE Services Release 5.2.x CVLAN Service

---

**Support**

Go to the Avaya Support website at [http://support.avaya.com](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) Web site
  https://plds.avaya.com
- Avaya Support Web site (for Avaya customers with maintenance agreements)
  http://support.avaya.com
- Avaya DevConnect Web site (for DevConnect members)
  http://www.avaya.com/devconnect

Checklist for downloading client and SDKs

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Download software from PLDs. See, Downloading software from PLDS on page 9.</td>
<td></td>
</tr>
<tr>
<td>2. Download TSAPI client. See, Downloading TSAPI clients</td>
<td></td>
</tr>
</tbody>
</table>

Downloading software from PLDS

Before you begin

Ensure that you are an Avaya customer and you have registered on the Avaya PLDS Web site.

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 (PLDS) Web site.

Note:

The TSAPI client, CVLAN client, and SDK are available from the Avaya PLDS Web site, but the TSAPI SDK is not. To obtain the TSAPI SDK, contact an authorized Avaya Business Partner or an Avaya Account Executive.
Installation Prerequisites

Procedure

1. In your web browser, type https://plds.avaya.com to open the Product Licensing and Delivery System Web site.
2. On the LOGIN NOW page, type your email address and password, and click SUBMIT.
3. From the main menu on the Home page, click Assets > View Downloads.
4. On the Search by Download tab in the Company name field, enter the name of your company.
5. From the Application field, select Application Enablement Services.
6. From the Download Type field, select Software Downloads.
7. From the Version field, select the current release.
8. Click Search Downloads.
9. On the Software Downloads list, locate the appropriate download, and click Download.
   - Avaya Aura Application Enablement Services TSAPI Client Linux 6.3.3
   - Avaya Aura Application Enablement Services TSAPI Client MS Windows 6.3.3
   - Avaya Aura Application Enablement Services CVLAN Client Windows 6.3.3
   - Avaya Aura Application Enablement Services CVLAN Client Linux 6.3.3
10. On the About Download Manager page, click Click to download your file now.

   ✪ Note:
   The first time you use the Download Manager, your browser displays a Security Warning and asks if you want to install the Download Manager. You can click Install and complete the procedure for installing the Download Manager.

11. From the Save As dialog box, which displays the file name (for example, tsapi-client-win32-6.3.3-454.zip), browse to a folder on your file system and click Save.

   ✪ Note:
   This is an example file name. The numbers following tsapi-client-win32-6.3.3 are subject to change.

   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 you specified in the Save As dialog box.

12. Click Exit to exit Avaya Download Manager. Your browser displays the PLDS Downloads page. A check mark appears next to the software you downloaded.

13. Click Log out to log out of PLDS.


15. For the Windows clients, go to the folder you specified in the Save as dialog box, and extract the zip file.
Next steps
Start the installation as directed in the following chapters. The installation instructions assume that you have downloaded (and, when necessary, extracted) the files to an appropriate directory on your file system.

---

**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. This procedure assumes 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, but the TSAPI SDK is not. To obtain the TSAPI SDK, contact an authorized Avaya Business Partner or an Avaya Account Executive.

**Procedure**

2. From the main menu on the Welcome to Avaya Support page, click Downloads.
3. Enter Application Enablement Services in the Enter Your Product field.
4. From the Choose Release menu, select 6.3.x.
5. From the Downloads list, click the appropriate download.
   - Avaya Aura Application Enablement Services TSAPI Client MS Windows 6.3.3
   - Avaya Aura Application Enablement Services TSAPI Client Linux 6.3.3
   - Avaya Aura Application Enablement Services CVLAN Client Windows 6.3.3
   - Avaya Aura Application Enablement Services CVLAN Client Linux 6.3.3
6. From the Downloads page, click the file name; for example, `tsapi-client-win32-6.3.3-454.zip`. (Keep in mind that this is an example of a file name. The numbers following `tsapi-client-win32-6.3.3` are subject to change.)
7. Save the file to your computer. For the Windows clients, extract the .zip file in a separate directory on your computer. It can be any directory on your file system.

**Next steps**
Start the installation as directed in the following chapters. The installation instructions assume that you have downloaded (and, when necessary, extracted) the files to an appropriate directory on your file system.
Downloading clients from Avaya DevConnect

About this task

Use the following procedure to download the TSAPI clients from the Avaya DevConnect Web site.

Note:

This procedure assumes that you are an Avaya DevConnect member and that you have registered on the Avaya DevConnect Web site.

Important:

The TSAPI client is available from the DevConnect Web site, 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 Web site,
   http://www.avaya.com/devconnect
2. Click Downloads.
3. Click Telephony Services API (TSAPI).
4. Click the arrow after Programming Resources, and then check the Software Development Kits check box.
5. From the list of results, select the appropriate download.
   - Avaya Aura Application Enablement Services 6.3.3 TSAPI Client (Win32)
   - Avaya Aura Application Enablement Services 6.3.3 TSAPI Client (Linux)
6. Read and accept the license agreement, and then click the Download button.
7. Save the file to your computer; for example, tsapi-client-win32-6.3.3-454.zip. (Keep in mind that this is an example of a file name. The numbers following tsapi-client-win32-6.3.3 are subject to change.)
8. For the Windows clients, extract the .zip file in a separate directory on your computer. It can be any directory on your file system.

Checklist for installing the TSAPI client

<table>
<thead>
<tr>
<th>Task</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the IP address or Host Name of the AE Services server from the AE Services administrator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check whether the TSAPI links are encrypted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments? infodev@avaya.com
<table>
<thead>
<tr>
<th>Task</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check whether the default CA certificate is being used for encryption.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check whether alternate TSAPI links are administered. If alternate TSAPI links are administered, you should configure the alternate Tlinks after the installation.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
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.

**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](http://www.citrix.com).

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel 8086 instruction set architecture</td>
</tr>
</tbody>
</table>
| 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 64-bit Client Platform Operating Systems supporting TSAPI applications running in 32-bit compatibility mode | - Windows 8 Pro  
- Windows 8 Enterprise  
- Windows 7 Professional |
### Table 2: TSAPI Linux client and SDK - hardware and software requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel 8086 instruction set architecture</td>
</tr>
</tbody>
</table>
| Red Hat Enterprise Linux (RHEL) 32-bit Versions | - Red Hat Enterprise Linux ES v4.0 Update 6  
- Red Hat Enterprise Linux ES v5.0 Update 7  
- Red Hat Enterprise Linux ES v5.0 Update 8 |
| Red Hat Enterprise Linux (RHEL) 64-bit Versions supporting TSAPI applications running in 32-bit compatibility mode | - Red Hat Enterprise Linux ES v5.0 Update 7  
- Red Hat Enterprise Linux ES v5.0 Update 8  
- Red Hat Enterprise Linux ES v5.0 Update 9  
- Red Hat Enterprise Linux ES v5.0 Update 10 |

**Note:**
To install the TSAPI Linux Client on a Red Hat Enterprise Linux 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 Red Hat Linux installation media and is also available for download at [http://rpm.pbone.net](http://rpm.pbone.net).

### Installing the TSAPI Windows client without the host name and the IP address

**Procedure**

1. Log on to your computer as a user with administrator-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 Application Enablement Services TSAPI client, it displays a dialog box with the message “Setup has detected an older version of the Avaya Application Enablement Services TSAPI Client on your system. This version needs to be removed before the installation can continue. Would you like Setup to remove this version for you now?”

Click **Yes** to have 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** on page 15.

   In the **Host Name or IP Address** field type a valid host name or IP address of the AE Server, for example:

   **192.168.123.44** (IP address)

   **aeserver1** or **aeserver.company.com** (host name)

   In the **Port Number** field, accept the default **450**. If your installation uses more than one AE Server, click **Add to List**.

   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 Servers (along with the default port) in the Configured AE Services Servers dialog box. If you are re-using any of the same AE Servers from the list, you can click **Next** to proceed. Otherwise, you can delete the AE Servers that are not required.

   Click **Next**.

   Setup displays the Ready to Install the Program dialog box.

7. On the AE Services Server Configuration dialog box, in the **Host Name or IP Address** field, type a place holder, such as **myserver** or **1.2.3.4** and accept the default port number.
8. Click Add to List or Next, the setup program issues a Warning dialog and you can continue with the installation.

9. 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.

10. From the Installation Wizard Complete dialog box, click Finish.
11. Setup exits.

Next steps
After installation, when you get a valid host name or IP address, edit the tslib.ini file and add the appropriate host name or IP address for the AE Services Server. For more information, see Editing the TSAPI Windows client configuration file (tslib.ini) on page 23.

Installing the TSAPI Windows client

Before you begin
If you are upgrading from the Avaya Computer Telephony (Avaya CT) TSAPI Windows (TS Win32) client to the Avaya Application Enablement Services TSAPI Windows client, you must remove the Avaya CT TS Win32 client before you install the Avaya 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 Network-based installations for the TSAPI Windows client on page 28.

Important:
Make sure you have completed the instructions for downloading the installation files and saving them to your computer. See Chapter 2: Installation prerequisites.

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 Application Enablement Services TSAPI client, it displays a dialog box with the message “Setup has detected an older version of the Avaya Application Enablement Services TSAPI Client on your system. This version needs to be removed before the installation can continue. Would you like Setup to remove this version for you now?”

Click Yes to have 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 on page 15.

   a. In the Host Name or IP Address field type a valid host name or IP address of the AE 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 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 Servers (along with the default port) in the Configured AE Services Servers dialog box. If you are re-using any of the same AE Servers from the list, you can click Next to proceed. Otherwise, you can delete the AE 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](#) on page 20.

---

### 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. Perform one of the following steps depending on the operating system you are using:
   - If you are using Windows 8, on the Start page, click **TSAPI Test**.
   - If you are not using Windows 8, click **Start** > **All Programs** > **Avaya AE Services** > **TSAPI Client** > **TSAPI Test**.

2. Select any of the following:
   - **Edit TSLIB.INI** - When you select **Edit TSLIB.INI**, Windows opens the tslib.ini file. For more information, see [Editing the TSAPI Windows client configuration file (tslib.ini)](#) on page 23.
   - **TSAPI Spy** - When you select **TSAPI Spy**, Windows opens the TSAPI Spy application. TSAPI Spy is a client message tracing application that allows you to see the flow of messages through the Telephony Services client library. For more information, see [TSAPI Spy - a Windows client message tracing tool](#) on page 64.
   - **TSAPI Test** - When you select **TSAPI Test**, Windows opens the TSAPI Test application. The TSAPI Test application allows you to test your TSAPI Client installation by opening a stream and making a call.
   - **TSAPI Client Readme** - When you select **TSAPI Client Readme**, Windows opens the TSAPI Windows Client Readme file. Review the Readme file for information about this release of the TSAPI Windows client.
   - **OpenSSL License** - When you select **OpenSSL License**, Windows opens the OpenSSL License file. Open the OpenSSL License file to review the terms of the license.
f. **Apache Software Foundation License** - When you select Apache Software Foundation License, Windows opens the Apache Software Foundation License file. The TSAPI Spy application includes software developed by the Apache Software Foundation.

g. **Apache Software Foundation Notice** - When you select Apache Software Foundation Notice, Windows opens the Apache Software Foundation Notice file. This file describes the software components developed by the Apache Software Foundation that are included with the TSAPI Spy application.

### 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. Perform one of the following steps depending on the operating system you are using:
   - If you are using Windows 8, on the Start page, click **TSAPI Test**.
   - If you are not using Windows 8, click **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 Communication Manager that you want to test. Tlinks are names that the TSAPI Service assigns to the TSAPI CTI links between the AE Server and Communication Manager.
   
   b. In the **User** field, type your CT User user ID.
   
   ![Note:](image)

   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 Communication Manager.

   ![Note:](image)

   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 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 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 on page 21.

g. Click Close to exit TSAPI Test.

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 Server and the client running TSAPI Test. For more information about TSAPI Spy, see . Use this procedure to monitor your call with TSAPI Spy.

Procedure

1. Perform one of the following steps depending on the operating system you are using:
   • If you are using Windows 8, on the Start page, click TSAPI Test.
   • If you are not using Windows 8, click Start > All Programs > Avaya AE Services > TSAPI Client > TSAPI Spy. Windows opens the TSAPI Spy application.

2. Perform the procedure Verifying the TSAPI Windows client installation on page 20 and monitor the activity between the AE Services TSAPI Service and TSAPI Test.

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 a 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**.
   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 Application Enablement Services TSAPI Windows client to a newer version, you do not need to remove the older version first. Follow the installation procedure in **Installing the TSAPI Windows client** on page 17.
Editing the TSAPI Windows client configuration file (tslib.ini)

About this task

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

Procedure

1. Perform one of the following steps depending on the operating system you are using:
   - If you are using Windows 8, on the Start page, click on **Edit TSLIB.INI**.
   - If you are not using Windows 8, click **Start > All Programs > Avaya AE Services > TSAPI Client > Edit TSLIB.INI**.

2. To edit the configuration file, refer to the TSAPI Windows client configuration file field description on page 23.

TSAPI Windows client configuration file field description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Telephony Servers]</td>
<td>When you install the TSAPI Client and complete the AE Services Server Configuration dialog box, AE Services adds the host name or IP address to this field of the tslib.ini file. You can edit [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</td>
</tr>
<tr>
<td>[Config]</td>
<td>Use this section to configure settings for server certificate and client certificate authentication if you are using secure (encrypted) TSAPI links. If you are not sure whether you need to use this section, see <strong>TSAPI Windows client certificate authentication on page 30</strong> on page 25. If you do plan to set up the [Config] section, see <strong>Server certificate authentication using your own certificate on page 31</strong> on page 26.</td>
</tr>
<tr>
<td>[Alternate Tlinks]</td>
<td>Use this section if you want your TSAPI Windows clients to use the Alternate Tlinks feature. See <strong>Specifying Alternate Tlinks for the TSAPI Windows client</strong> on page 23</td>
</tr>
<tr>
<td>[Shared Admin]</td>
<td>Use this section when you want to use a pointer to a server-based tslib.ini file. See <strong>Installing the next client by sharing a single tslib.ini file among clients on page 37</strong> on page 30.</td>
</tr>
</tbody>
</table>

Note:

If you use a firewall, see **Port settings for a firewall administration** on page 41.

Specifying Alternate Tlinks for the TSAPI Windows 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,
specify the alternate Tlinks in the TSAPI Configuration file. For a brief description of Tlinks, see [TSAPI Links (Tlinks)] on page 40.

**Important:**

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

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

**Procedure**

1. Perform one of the following steps depending on the operating system you are using:
   a. If you are using Windows 8 system: On the Start page, click on **Edit TSLIB.INI**.
   b. If you are using non-Windows 8 system: Click **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. Following the *[Alternate Tlinks]* line, add a list of alternate Tlink entries.

   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® CM1#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 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 as alternates for the preferred Tlink.

**Examples**

In Example 1, there are two AE Servers, AESRV1 and AESRV2, that each have a TSAPI link to the same switch, Avaya Aura® CM1. When opening a stream, if AESERV1 is unavailable, the TSAPI client will attempt to use AESRV2 instead of AESRV1.

*Example 1*

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

In Example 2, there are four AE Servers that each have a TSAPI link to the same switch, Avaya Aura® CM1.
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 server.

Example 2

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

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 either use the Avaya Product Root Certificate Authority (CA) certificate as the server certificate (this is the default), 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 on page 56.

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 \certs\tsapiClient.pfx and does not have a password.

Server certificate authentication using your own certificate

If you are using your own certificates for server certificate authentication, and you are not using the predefined location for storing certificates (that is, the aesCerts.cer file), you must add statements to the tslib.ini file that specify where your certificates are located. For example,

[Config]
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,

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

  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 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. If you do not want the client to check the certificate for the FQDN, you can use the **Verify Server FQDN=0** setting.

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 tslib.ini file that specify the location and/or password of the client keystore. For example:

[Config]
Client KeyStore=\keystore-location>
KeyStore Password=\keystore-password>
where:

- **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="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**

- **TSLIB.INI**
  - The [Telephony Servers] section specifies the AE Services servers that your installation uses.
  - [Telephony Servers]
    - ; List your Telephony Servers and Application Enablement (AE) Services servers that offer TSAPI Telephony Services above.
    - ; Each entry must have the following format:
      - ; host_name=port_number
      - ; where:
        - ; - host_name is either the domain name or IP address of the AE Services server.
        - ; - port_number is the TSAPI Service port number. The default port number used by AE Services is 450.
        - ; For example:
          - aeserver.mydomain.com=450
          - 192.168.123.45=450
          - 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=450

- **[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.
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 on page 29.

2. Install the next TSAPI client and all subsequent clients as described in Installing the next client: customizing the tslib.ini file prior to installation on page 30.

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 Server.

Procedure
1. Copy the software and install the first TSAPI client as described in Copying the TSAPI Windows client software on page 29.
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 on page 30.

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 directory on the network drive, and double-click setup.exe to install the TSAPI Windows client.
2. At this point you would follow Steps 3 through 8 of the procedure to install the TSAPI Windows client, see Installing the TSAPI Windows client on page 17. 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 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. Setup will get this information from the tslib.ini file on the server. When 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 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**

Make sure you have completed the procedure for downloading the installation files and saving them to your computer. See Chapter 2: Installation prerequisites. Before installing the TSAPI Linux Client on a Red Hat Enterprise Linux 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

**About this task**

Use this procedure to install the TSAPI Linux client. This RPM may be available with your Red Hat Linux installation media and is also available for download at [http://rpm.pbone.net](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-6.3.3-94.bin.
4. Run the TSAPI Linux Client installation program to begin the installation. For example: ./tsapi-client-linux-6.3.3-94.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.

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 tslibrc configuration file.

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

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 Server that you want to access, 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 on page 41.

Specifying Alternate Tlinks for the Linux client

About this task

The Alternate Tlinks feature allows the TSAPI client library to select an alternate Tlink if the preferred Tlink is unavailable when trying to establish a session. To put this feature into effect, you must specify the alternate Tlinks in the TSAPI Configuration file. For a brief description of Tlinks, see TSAPI Links (Tlinks) on page 40.
Important:

When multiple AE Servers are used as alternates, the CT User user id and password used by the application must be configured identically for each AE 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®
   CM1#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.

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 Servers, AESRV1 and AESRV2, that each have a TSAPI link to the same switch, Avaya Aura® CM1. 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 Servers that each have a TSAPI link to the same switch, Avaya Aura® CM1.

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 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 (this is the 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 on page 56.

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 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=</path/to/keystore>**

**KeyStore Password=</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.
AE Services TSAPI clients and SDKs installation

# /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:100:2101:2e0:18ff: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
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 on page 39 on page 32.

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 the figure on page 39 for an example of 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
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 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.
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 Red Hat 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 on page 39)
2. Install the latest version of the client (see Installing the TSAPI Linux client on page 31).

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 Avaya.

• **switch_connection_name** represents the Switch Connection name. The AE Services administrator determines the switch connection name when he/she administers a Switch Connection in AE Services Management Console.

• **service_type** refers to the CSTA service type. It can be either of the following:
  - CSTA - If the TSAPI Link is administered as unencrypted (nonsecure).
  - CSTA-S - If the TSAPI Link is administered as encrypted (secure).

• **AE_server_name** is the name of the AE Server providing the TSAPI Service for the switch connection. The AE 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 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 AE Services-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 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-win32-6.3.3-build.zip, and double-click setup.exe.
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 Application Enablement Services TSAPI SDK, it displays a dialog box with the message: “Setup has detected an older version of the Avaya 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 Files\Avaya\AE Services\SDKs\TSAPI. For 64-bit Windows platforms, the default destination is C:\Program Files (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 on page 42 to learn more about the TSAPI SDK.

---

**Viewing the TSAPI Windows SDK Components**

**Procedure**

1. Perform one of the following steps depending on the operating system you are using:
   a. If you are using Windows 8: On the Start page, click on Avaya AE Services.
   b. If you are not using Windows 8: Click Start > All Programs > Avaya AE Services > SDKs > TSAPI.
2. Select any of the following components:

a. **Explore Sample Code** - When you select Explore Sample Code, 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 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 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 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, open the Control Panel. For example, 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 SDK, and click Remove.
4. A confirmation dialog box appears.
5. Click Yes.
   Setup uninstalls the software, and displays the Uninstall Complete dialog box.
6. Click Finish.

TSAPI Windows SDK upgradation
If you are upgrading from an older version of the Avaya Application Enablement Services TSAPI Windows SDK to a newer version, you do not need to remove the older version first. Follow the installation procedure in Installing the TSAPI Windows SDK on page 48. See Installing the TSAPI Windows SDK on page 41.

Installing and managing the TSAPI Linux SDK

Installing the TSAPI Linux SDK

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

Procedure
1. Log in to the computer where you are installing the SDK as root.
2. Insert the TSAPI SDK CD into your computer’s CD-ROM drive.
3. Type mount /mnt/cdrom/ to mount the file system.
4. Type cd /mnt/cdrom/sdk/Linux to change to the directory containing the TSAPI Linux SDK installation program tsapi-sdk-linux-version-build.bin. 
   - 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-6.3.3-94.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 Red Hat 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 on page 45).
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 on page 39).
3. Install the latest version of the TSAPI Linux client (see Installing the TSAPI Linux client on page 31).
4. Install the latest version of the SDK (see Installing the TSAPI Linux SDK on page 44).
The Avaya Aura® Application Enablement Services CVLAN Client/SDK, which can be installed on a client workstation, provides client computers with remote access to Communication Manager third-party call control capabilities. Access is provided by the CVLAN Service running on an AE Services Server (referred to as the AE 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, you may either use the Avaya Product Root Certificate Authority (CA) certificate as the server certificate (this is the default), or a CA certificate issued by a trusted in-house or third-party certificate authority (also referred to as your own certificate).
The Avaya Product Root CA certificate is installed on the CVLAN client in the following location:

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

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

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

Note that this file may contain several certificates.

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

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

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

If you choose to use a different file for the client keystore, the environment variable CLIENT_KEYSTORE must contain the full pathname 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 on page 56 on page 67.

---

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 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 - for more information, see the table
- Linux - for more information, see the table

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel 8086 instruction set architecture</td>
</tr>
</tbody>
</table>
| 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 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 |
Table 4: CVLAN Linux Client/SDK - hardware and software requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Red Hat Enterprise Linux (RHEL) 32-bit Versions | Red Hat Enterprise Linux ES v5.0 Update 8  
Red Hat Enterprise Linux ES v5.0 Update 9  
Red Hat Enterprise Linux ES v5.0 Update 10 |
| Red Hat Enterprise Linux (RHEL) 64-bit Versions  
supporting CVLAN applications running in 32-bit compatibility mode | Red Hat Enterprise Linux ES v5.0 Update 8  
Red Hat Enterprise Linux ES v5.0 Update 9  
Red Hat Enterprise Linux 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. See Chapter 2: Installation prerequisites.

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** on page 55.

---

**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. See [CVLAN Windows Client/SDK removal](#).
2. Install the latest version of the Client/SDK. See [Installing the CVLAN Windows Client/SDK](#) on page 50).

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

---

**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**.
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 Red Hat Enterprise Linux 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 Red Hat Linux 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. See Chapter 2: Installation prerequisites.
Before installing this release of the CVLAN Linux Client on a Red Hat Enterprise Linux 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 Red Hat Linux 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-6.3.3-94.bin
4. Run the CVLAN Linux/Client SDK installation program to begin the installation. For example, ./cvlan-client-linux-6.3.3-94.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 on page 55.

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 on page 54.
2. Install the latest version of the Client/SDK. See Installing the CVLAN Linux Client/SDK on page 52.
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 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 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 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 Server.

   **Windows**
   
   ```
   "<installation-directory>\utils\asai_test -m abcserver 2"
   ```
   
   where: *abcserver* is the host name or IP address of the AE 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 Server, and select **Utilities > Diagnostics > AE Services > ASAI Test**.
      
         AE Services OAM displays the ASAI Test 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: Certificates 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.

⚠ Note:

The TSAPI Linux client and the CVLAN Linux client do not support certificates signed with SHA-2 (e.g., SHA-256 or SHA-512) hash functions.

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, which is signed by the Avaya Product Certificate Authority certificate. See the figure on page 57 for an illustration.

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.
   a. 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.

a. 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 can not trust the certificate. This only applies if the client has been configured with “Verify Server FQDN=1”.

![Server certificate authentication diagram]

**Figure 6: Server certificate authentication**

---

**Location and usage of a default certificate**

The AE Services server includes a default server certificate, which is signed by the Avaya Product Certificate Authority (CA). Also, 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.

<table>
<thead>
<tr>
<th>Table 5: Where AE Services installs the default CA certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSAPI Win32 client</td>
</tr>
<tr>
<td>&lt;installation-folder&gt;\certs\ca\avayaprca.cer</td>
</tr>
<tr>
<td>TSAPI Linux client</td>
</tr>
<tr>
<td>/opt/mvap/tsapi/client/certs/CA/avayaprca.pem</td>
</tr>
<tr>
<td>CVLAN Linux client</td>
</tr>
<tr>
<td>/usr/adm/cvlan/certs/CA/avayaprca.pem</td>
</tr>
<tr>
<td>CVLAN Win32 client</td>
</tr>
<tr>
<td>&lt;installation-folder&gt;\certs\ca\avayaprca.cer</td>
</tr>
</tbody>
</table>

---

**Location of your own certificates**

Notice in the figure on page 58 that frame B is labeled as the “default location” option.
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 table.

**Table 6: TSAPI and CVLAN- if you use your own certificates: the “default location option”**

<table>
<thead>
<tr>
<th>Client Type</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSAPI Win32 client</td>
<td><code>&lt;installation-folder&gt;\certs\ca\aesCerts.cer</code></td>
</tr>
<tr>
<td>TSAPI Linux client</td>
<td><code>/opt/mvap/tsapi/client/certs/CA/aesCerts.pem</code></td>
</tr>
<tr>
<td>CVLAN Win32 client</td>
<td><code>&lt;installation-folder&gt;\certs\ca\aesCerts.cer</code></td>
</tr>
<tr>
<td>CVLAN Linux client</td>
<td><code>/usr/adm/cvlan/clients/certs/CA/aesCerts.pem</code></td>
</tr>
</tbody>
</table>

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

- **A** No certificate configuration required
  - Default certificates
    - TSAPI Win32 client - `\certs\ca\avayapca.cer`
    - TSAPI Linux client - `/opt/mvap/tsapi/client/certs/CA/avayapca.pem`
    - CVLAN Linux client - `/usr/adm/cvlan/certs/CA/avayapca.pem`
    - CVLAN Win32 client - `<installation-folder>\certs\ca\avayapca.cer`

- **B** The “default location” option
  - Default certificate locations (provided for TSAPI only)
  - If you use your own certificates, and you copy your trusted CA certificate to a specified location, you do not have to update the configuration files. The specified locations for Win32 and Linux are:
    - TSAPI Win32 client - `<installation-folder>\certs\ca\aesCerts.cer`
    - TSAPI Linux client - `/opt/mvap/tsapi/client/certs/CA/aesCerts.pem`
    - CVLAN Linux client - `<installation-folder>\certs\ca\aesCerts.cer`
    - CVLAN Win32 client - `/usr/adm/cvlan/clients/certs/CA/aesCerts.pem`

- **C** If you use your own certificates, you can copy the files to any directory you prefer, but you must include the path in the TSAPI configuration files (tslib.ini or tslibrc). CVLAN does not use a configuration file.
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 on page 34.
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.

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 on page 47.

AE Services certificate administration

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

If you are configuring TSAPI and CVLAN clients in an environment that uses certificates issued by a trusted in-house or third-party certificate authority, the table 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1. Create a server certificate request for AE Services.  
See “Creating a server certificate signing request for the AE Services server” in the Avaya Aura® Application Enablement Services Administration and Maintenance Guide, 02-30357 (AE Services Administration and Maintenance Guide). | |
| 2. Create an AE Services server certificate.  
See “Creating a server certificate for AE Services” in the AE Services Administration and Maintenance Guide. | |
| 3. Import the server certificate into AE Services.  
See “Importing the server certificate into AE Services” in the AE Services Administration and Maintenance Guide. | |
| 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 6. Administer TSAPI links as encrypted.  
See “Administering TSAPI Links” in the AE Services Administration and Maintenance Guide. | |

CVLAN-related administrative tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 7. Add a CVLAN link.  
See “Administering CVLAN Links” in the AE Services Administration and Maintenance Guide. | |
| 8. Add a CVLAN client.  
See “Adding CVLAN Clients” in the AE Services Administration and Maintenance Guide. | |
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.

![Diagram of Client Certificate Authentication](image.png)

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 table locations lists the default location of the client keystore for the TSAPI Windows and Linux client libraries.
Table 8: TSAPI - Default client keystore locations

<table>
<thead>
<tr>
<th></th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSAPI Windows client</td>
<td><code>&lt;installation-folder&gt;\certs\tsapiClient.pfx</code></td>
</tr>
<tr>
<td>TSAPI Linux client</td>
<td><code>/opt/mvap/tsapi/client/certs/tsapiClient.pfx</code></td>
</tr>
</tbody>
</table>

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 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

<table>
<thead>
<tr>
<th></th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVLAN Windows client</td>
<td><code>&lt;installation-folder&gt;\certs\cvlanClient.pfx</code></td>
</tr>
<tr>
<td>CVLAN Linux client</td>
<td><code>/usr/adm/cvlan/certs/cvlanClient.pfx</code></td>
</tr>
</tbody>
</table>

---

**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 the table, 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 on page 26.
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 on page 34.

**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 the table, 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 on page 47.

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 on page 47.
Appendix B: TSAPI Client Message Tracing

TSAPI Spy - a Windows client message tracing tool

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

Overview of the TSAPI Spy for Windows interface

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

- Read the table on page 64 and the table on page 65 for an operational summary of TSAPI Spy.

<table>
<thead>
<tr>
<th>Tracing...</th>
<th>Enabled - the default setting. When Tracing is enabled, message tracing information is displayed in the two display areas of the TSAPI Spy main window.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 &gt; Exit), the next time you start TSAPI Spy, it will be Disabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Open Streams (+)</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed Streams (-):</td>
<td>Indicates the number of streams previously open from the TSLIB to all AE Servers, but which are now closed. This number is updated in real time as applications close streams.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Streams list (white background)</th>
<th>Displays information about currently and previously open connections from the TSLIB to all telephony servers. For more information see, Streams list on page 67.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handle:</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Server ID</strong></td>
<td>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.</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Appl</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Login</strong></td>
<td>The login ID under which the application has opened this connection. Multiple applications may be opened under the same or different login IDs at a single client. This information is provided to the TSLIB by the application when a request is made to open a connection.</td>
</tr>
</tbody>
</table>

**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 on page 66.

**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.
- **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 toplmost 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 on page 67. 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** on page 66. This setting is disabled by default (a check mark does not appear next to it).

---

**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** on page 66, 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.

**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**

**About this task**

Use this procedure to create a trace file.

**Procedure**

1. Perform one of the following steps depending on the operating system you are using:
   - If you are using Windows 8, on the Start page, click **TSAPI Test**.
• If you are not using Windows 8, click **Start** > **All Programs** > **Avaya AE Services** > **TSAPI Client** > **TSAPI Test**.

2. From the Telephony Services Spy for Win32 window, select **Options** > **Log To File**... .

   Windows displays the Log to File dialog box.

3. On the Create Trace File dialog box, accept the default for Log Trace Messages (enabled).

4. In the Trace File Name field, type a name for the trace file (for example, c:\cstatrace.txt), or, choose a location by clicking **Browse**.

5. The default extension assigned to trace files is .trc, but you can use any filename and extension.

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** (the Log to File option will have a check mark).

2. Uncheck 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/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 the TSAPI Spy with Windows Server 2003
About this task
When using a standard Windows Remote Desktop Connection to start the TSAPI Spy on a Windows Server 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 a Windows Server 2003-based server:

Procedure
1. Click Start > Run.
   The Run dialog box appears.
2. Enter 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 cstattrace.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 files examination**

The figure on page 72 depicts 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.
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 deliverables. This naming convention is not a formal standard, it is simply a guideline for reading file names.

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

**Where:**

<table>
<thead>
<tr>
<th><code>&lt;api&gt;</code>-</th>
<th><code>&lt;type&gt;</code>-</th>
<th><code>&lt;target&gt;</code>-</th>
<th><code>&lt;version&gt;</code></th>
<th><code>&lt;build&gt;</code>-</th>
<th><code>&lt;suffix&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Refers to the name of the API. For example, <code>tsapi</code> or <code>cvlan</code></td>
<td>Refers to the type of deliverable. Can be <code>client-</code>, <code>sdk-</code>, or <code>client-sdk</code> (for ISOs).</td>
<td>Refers to the name of the operating system.</td>
<td>Refers to the software version.</td>
<td>Note: This number changes frequently. It is often represented in this document by <code>x</code> instead of an actual build number.</td>
<td>Refers to the file or package type.</td>
</tr>
</tbody>
</table>

**Examples**

- TSAPI Windows client - `tsapi-client-win32-6.3.3-170.zip`
- TSAPI Linux client - `tsapi-client-linux-6.3.3-94.bin`
- TSAPI Windows SDK - `tsapi-sdk-win32-6.3.3-170.zip`
- TSAPI Linux SDK - `tsapi-sdk-linux-6.3.3-94.bin`
- CVLAN Windows client and SDK - `cvlan-client-win32-6.3.3-70.zip`
- CVLAN Linux client and SDK - `cvlan-client-linux-6.3.3-94.bin`

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

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

<table>
<thead>
<tr>
<th><code>&lt;api&gt;</code>-</th>
<th><code>&lt;type&gt;</code>-</th>
<th><code>&lt;target&gt;</code>-</th>
<th><code>&lt;version&gt;</code></th>
<th><code>&lt;build&gt;</code>-</th>
<th><code>&lt;suffix&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tsapi</code>-</td>
<td><code>client</code>-</td>
<td><code>linux</code>-</td>
<td><code>6.3.3</code></td>
<td><code>-170</code></td>
<td><code>.bin</code></td>
</tr>
<tr>
<td><code>tsapi</code>-</td>
<td><code>client</code>-</td>
<td><code>win32</code>-</td>
<td><code>6.3.3</code></td>
<td><code>-170</code></td>
<td><code>.zip</code></td>
</tr>
<tr>
<td><code>tsapi</code>-</td>
<td><code>sdk</code>-</td>
<td><code>linux</code>-</td>
<td><code>6.3.3</code></td>
<td><code>-170</code></td>
<td><code>.bin</code></td>
</tr>
</tbody>
</table>
### File naming conventions

<table>
<thead>
<tr>
<th><code>&lt;api&gt;</code>-</th>
<th><code>&lt;type&gt;</code>-</th>
<th><code>&lt;target&gt;</code>-</th>
<th><code>&lt;version&gt;</code></th>
<th><code>&lt;build&gt;\(^1\)</code></th>
<th><code>&lt;suffix&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>tsapi-</td>
<td>sdk-</td>
<td>win32-</td>
<td>6.3.3</td>
<td>-170</td>
<td>.zip</td>
</tr>
<tr>
<td>cvlan-</td>
<td>client-</td>
<td>linux-</td>
<td>6.3.3</td>
<td>-70</td>
<td>.bin</td>
</tr>
<tr>
<td>cvlan-</td>
<td>client-</td>
<td>win32-</td>
<td>6.3.3</td>
<td>-70</td>
<td>.zip</td>
</tr>
</tbody>
</table>

\(^1\) 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 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 server (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 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 Communication Manager. Up to 64 links can be administered on Communication Manager.

**CVLAN**  
CallVisor/LAN - 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 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 Application Enablement Services platform.

**PEM**
Privacy Enhanced Mail - 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**
Selecting an appropriate path for a call. When a routing application is started, it sends route registration requests, which contain a device ID, to Communication Manager. Routing requests instruct 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. Communication Manager does not route these calls. Also referred to as adjunct routing.

**SDK**
Software Development Kit. An SDK is a package that enables a programmer to develop applications for a specific platform. Typically, an SDK includes one or more APIs, documentation, and, in some cases, programming tools.

**Tlink**
A Tlink is a service identifier that is created when the administrator adds a TSAPI Link in AE Services OAM. A Tlink refers to a switch connection between a specific switch and a specific AE Server.

**TLS**
Transport Layer Security. TLS 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. TSAPI is a C- language based API for third-party call and device control, and based on CSTA standards.
# Index

## A
- AE Services
  - documentation ................................................. 4
- Alternate Tlinks ................................................... 32
- ASAI test utility .................................................. 54
- Avaya CT Windows SDK ........................................ 44, 52

## B
- backward compatibility .......................................... 7

## C
- client certificate authentication ............................... 23, 34
- Client certificate authentication .................................. 61
- CVLAN
  - installing Linux Client ....................................... 52
  - installing Linux SDK .......................................... 52
  - installing Windows Client .................................... 50
  - installing Windows SDK ....................................... 50

## E
- Errors
  - reported by TSAPI Spy ......................................... 69

## I
- Installing CVLAN Linux Client and SDK .................... 52
- Installing CVLAN Windows Client and SDK ................ 50
- Installing TSAPI Linux client ................................ 31
- Installing TSAPI Linux SDK ................................... 44
- Installing TSAPI Windows client ............................. 17
- Installing TSAPI Windows SDK ............................... 41

## L
- Location of default CA certificate ............................. 57

## O
- operating system requirements .................................. 14

## R
- Removing
  - TSAPI Windows SDK ......................................... 44, 52
  - Removing TSAPI Linux client ............................. 39, 45
  - Removing TSAPI Linux SDK ............................... 45

## S
- server certificate authentication ............................. 34
- Software
  - downloading .................................................. 9
  - support ....................................................... 7

## T
- TSAPILIB
  - tracing client messages with TSAPI Spy .................. 64
- TSAPI Linux client, removing ................................ 39, 45
- TSAPI Linux SDK, removing .................................. 45
- TSAPI Spy
  - client library model .......................................... 68
  - TSAPI Test, verifying installation .......................... 20
  - TSAPI Win32 client, verifying installation ................. 20
  - TSAPI Windows client, installing .......................... 17
tslib.ini configuration file ........................................ 25
tslibrc configuration file .......................................... 32
- TS Spy
  - error records .................................................. 69
  - file logging ................................................... 66
  - trace records .................................................. 68
- TS Spy menu options .............................................. 64

## V
- Verifying installation of CVLAN client ...................... 54
- videos ................................................................... 6