Configuration — Secure Portable Office Client
Avaya VPN Gateway

8.0
NN46120-301, 03.03
June 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Preface 5
- Who should use this book 5
- Related documentation 5
- Product names 6
- Avaya SPO Technical Support 6

Chapter 2: New in this release 7
- Features 7
  - Application virtualization 7
- Other changes 7
  - Supported operating systems 7
  - Web Browser 8
  - CD-ROM deployment 8

Chapter 3: Introduction 9
- Features 9
- SPO Client Compatible Devices 9
  - Portable Media Only Deployment 10
  - SmartCard solution 10
  - CD-ROM and DVD Deployment 11
- Supported operating systems 11
- Accessing applications using SPO Client 11

Chapter 4: Downloading and Installing Secure Portable Office Client 15
- Downloading SPO Client 15
- Installing SPO Client 16
  - Installing MSI image 16
  - Installing U3P image 17
  - Installing CD-ROM, CD-R, CD-RW, or DVD 18
- Portable Applications Installation 19
  - Installing portable applications from public websites 19

Chapter 5: Configure Secure Portable Office Client 21
- Configuring SPO 21
- Dashboard 24
  - File menu 25
  - View menu 26
  - Tools menu 27
  - Help menu 28
  - User Preferences 29
- System Tray 37
- Enabling auto-start application for U3P 38
- Removing Secure Portable Office from U3 USB 38

Chapter 6: Ceedo Licensing 41
- SPO application virtualization license 41
- Ceedo (SPO application virtualization) license basic 41
- Activating Ceedo Enterprise from Within the Ceedo Environment 42
- Importing Ceedo license 43

Chapter 7: Authenticating Secure Portable Office Client 45
Authentication with Avaya VPN Gateway Server **45**
Authentication methods **45**
Software Upgrade and Package **46**

Chapter 1: Preface

This document provides information on how to configure and deploy the Avaya Secure Portable Office client.

Who should use this book

This guide is intended for Secure Potable Office (SPO) client users and the administrators who deploy or maintains the SPO feature. It assumes familiarity with how to configure the Avaya VPN Gateway.

Related documentation

For full documentation on installing and using the features available in the VPN Gateway software, see the following manuals:

- *Avaya VPN Gateway 8.0 Command Reference* describes each command in detail. The commands are listed for each menu, according to the order they appear in the Command Line Interface (CLI).
- *Avaya VPN Gateway 8.0 Application Guide for SSL Acceleration* provides examples on how to configure Secure Socket Layer (SSL) Acceleration through the CLI.
- *Avaya VPN Gateway 8.0 CLI Application Guide for VPN* provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway 8.0 BBI Application Guide for VPN* provides examples on how to configure VPN deployment through the Browser-Based Interface (BBI).
- *Avaya VPN Gateway 8.0 VPN Administrators Guide* — VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway 8.0 VPN Users Guide* describes the initial setup procedure, upgrades, operator user management, certificate management, troubleshooting and other general operations that apply to both SSL Acceleration and VPN.
- *Avaya VPN Gateway 3050/3070 Hardware Installation Guide* describes installation of the VPN Gateway 3050 and 3070 hardware models.
- *Avaya VPN Gateway 8.0 Configuration - Secure Portable Office Client Guide* gives the feature list and provides general information about Secure Portable Office (SPO) based VPN client.

- *Avaya VPN Gateway 8.0 Troubleshooting guide* describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).

- *Avaya VPN Gateway 8.0 Release Notes* lists new features available in version 8.0 and provides up-to-date product information.

The preceding manuals are available for download.

Product names

The software described in this manual runs on several different hardware models. Whenever the generic terms *Avaya VPN Gateway, VPN gateway, or AVG* are used in the documentation, the following hardware models are implied:

- Avaya VPN Gateway 3050 (AVG 3050)
- Avaya VPN Gateway 3070 (AVG 3070)

Similarly, all references to the old product name–iSD-SSL or iSD–in commands or screen outputs can be interpreted as applying to the preceding hardware models.

Avaya SPO Technical Support

Contact your IT support help desk or VPN administrator for additional help with implementation of the Secure Portable Office (SPO) feature.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Configuration — Secure Portable Office Client, (NN46120-301)* for release 8.0.

- Features on page 7
- Other changes on page 7

Features

See the following sections for information about feature changes:

Application virtualization on page 7

Application virtualization

Release 8.0 provides application portability by deploying the virtualized applications to an Secure Portable Office (SPO) enabled drive for running on any Windows XP or Vista host. You can carry the personal computer (PC) client applications on the Universal Serial Bus (USB) drive, launch applications from the SPO client, and run on any PC supported by SPO.

You can select a virtualized or a native work space as in previous releases for your applications. For more information about virtualization, see Configuring SPO on page 21.

Other changes

See the following for information about changes that are not feature-related:

- Supported operating systems on page 7
- Web Browser on page 8
- CD-ROM deployment on page 8

Supported operating systems

In native mode, Release 8.0 supports Windows XP and Vista 64 bit Operating System (OS). For more information, see Supported operating systems on page 11.

Web Browser

Supports Mozilla Firefox version 3.0 and later.

CD-ROM deployment

You can deploy the SPO client on CD-ROM and DVD in native and virtualized mode. For deploying SPO client in virtualized mode, the CD-ROM and DVD must have write permissions. The SPO client deployment in CD and DVD provide low cost portable VPN client. For more information, see CD-ROM and DVD Deployment on page 11.

Chapter 3: Introduction

This chapter provides the feature list and general information about Secure Portable Office (SPO) client. The SPO client provides VPN access from portable storage such as USB compliant flash memory and CD ROM.

The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. The SPO client can be deployed and managed from the AVG server thus simplifying SPO client maintenance and updates.

Features

The SPO Client has the following features:

- Supports Layer 3 access using Net Direct
- Supports client-side logging for remote troubleshooting
- Status monitor provides real time information of connection status.
- Application Portability. This enables end users to add their own applications to the USB flash drive and add them to the SPO menu.
- Removes information from the browser cache upon exit, logout, or removal of the USB flash drive.
- Provides access list for the applications authorized by the IT administrator–based on extended profiles.
- SPO client is automatically updated to the latest version when the user connects to the AVG.
- Supports server-side logging for SPO VPN users.
- Applications requiring layer 3 network access can be linked to Net Direct enabling Net Direct autolaunch when the application is started.
- Supports software management menu. The AVG server maintains the software applications required by the SPO Client and any portable applications. The software is stored in a special directory per VPN in AVG server.

SPO Client Compatible Devices

The SPO client can run from any portable media including generic USB compatible flash memory drive and CD ROM. In addition, the SPO client can be deployed on USB flash drives with integrated SmartCard. The deployment with a SmartCard enables the USB flash drives

to function as a portable VPN solution and as a form of hardware based two factor authentication.

Portable Media Only Deployment

In this deployment mode, the SPO client is installed on any compatible USB compatible flash memory drive that is compliant with USB V1.1 or higher. All data resident on the device can be overwritten during the SPO client installation if the format option is chosen. This can be obtained by any third party vendor and initialized.

SmartCard solution

The SPO client can be installed in the flash memory partition of PC/USB compatible devices with integrated SmartCard. In this mode the SPO client user is authenticated by the AVG using a digital certificate installed in the SmartCard. This provides strong, two factor authentication.

- The USB flash drive is a unique and tamper evident device, that is the flash is in molded case.
- The USB flash drive has 2 GB of flash memory and should be 2.0 compliance.
- Strong two-factor authentication, SmartCard-based PKI technology
- Lockdown mode when incorrect password attempts exceed a pre-configured value
- Secure file Storage
- Autorun functionality and secure CD partition modifications
- On-the-fly hardware encryption

Limitation

The SPO application virtualization mode supports SmartCard based certificate management using Virtualized Aladdin PKI Client software only when E-Token NG-FLASH 72 KB (Java Virtual Machine) is used. The E-Token NG-FLASH 64 KB (Siemens CardOS) cannot be used to manage client certificates from SmartCard using Virtualized PKI Client software. This is due to the incompatibility with generic USB CCID driver (usbccid.sys). The E-Token NG-FLASH 64 KB. It can work only with proprietary SmartCard reader driver and they are not available in Windows operating systems. Application virtualization does not support virtualization of drivers. Hence, Aladdin PKI client must be installed in the host PC to manage the client certificates if E-Token NG-FLASH 64 KB is used for SPO Client.

CD-ROM and DVD Deployment

You can deploy the SPO client on CD-ROM and DVD in native and virtualized mode. For deploying SPO client in virtualized mode, the CD-ROM and DVD must have write permissions. The SPO client deployment in CD and DVD provide low cost portable VPN client.

Supported operating systems

The SPO client supports the following operating systems (OS):

- Windows (2000, XP, Vista, and 7) 32 bit OS in virtualized and native environment.
- Windows (XP and Vista) 64 bit OS in native environment.

Accessing applications using SPO Client

After the user credentials are exchanged between the SPO software client and the AVG server, the user receives a configuration file from the AVG server. The list provides a set of application and web links enabled for secure access. The following provides examples of applications and link types that can be provided:

- Web-based applications
  - Web email (Outlook Web Access and Lotus iNotes)
  - Intranet server access
  - Business application like BizSphere
- Corporate policy enforcement applications-TunnelGuard
- Thin clients-WTS and Citrix
- Virtual Desktop
- Full Network (Layer 3) access using Net Direct
  - Business applications like SAP, Oracle, and PeopleSoft
  - Voice over IP applications like MCS and LCS
- Applications supported by port forwarding
- Portable applications support
  - Portable Firefox
  - ClamWin Portable: anitivirus to go

- Example portable applications from http://portableapps.com/apps

• Web browsers:

- Internet Explorer

- Mozilla Firefox version 3.0 and later

The access list menu can be a system tray icon (Figure 2: System Tray on page 14) or a window dashboard (Figure 1: Dashboard on page 13). If it is displayed as system tray icon, a temporary balloon pops-up from the icon. This shows the user status (connected or disconnected) and the list of available applications. The system tray icon contains a link to check the connection status, disconnect the service, and close the application.

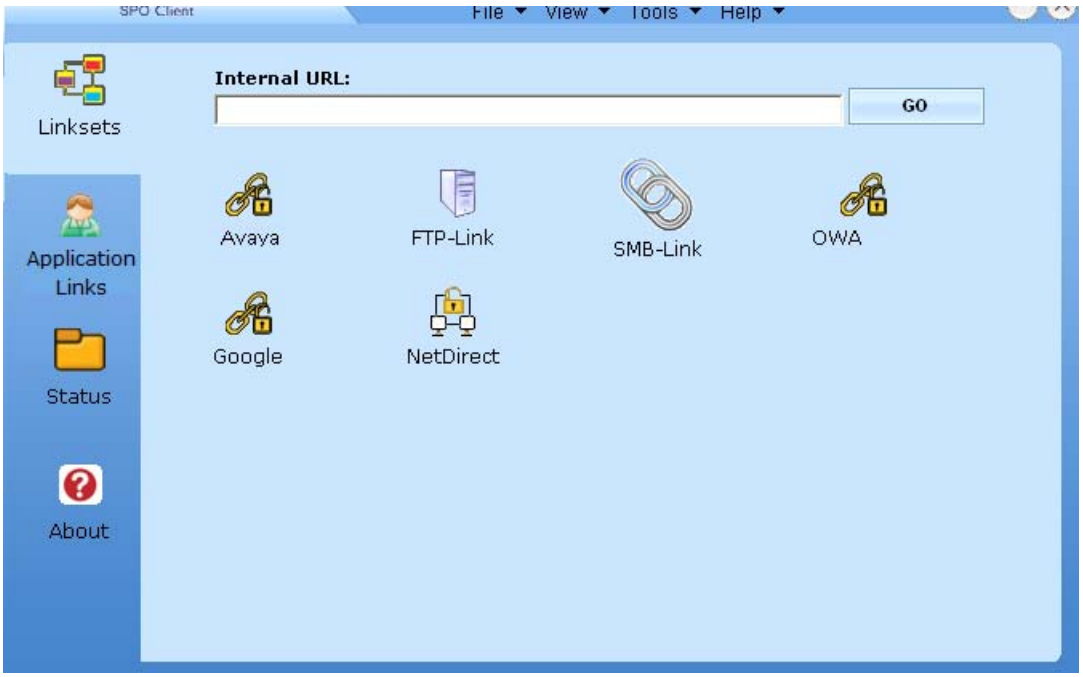


Figure 1: Dashboard

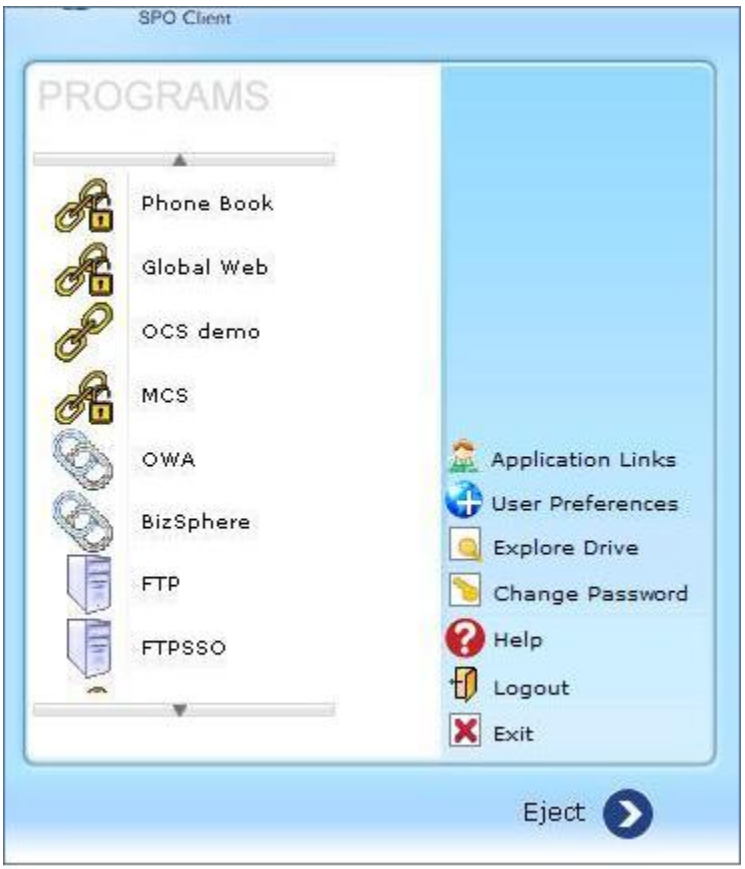


Figure 2: System Tray

Chapter 4: Downloading and Installing Secure Portable Office Client

This chapter explains the downloading and installation processes for the Secure Portable Office (SPO) client. The SPO client can be posted on a web server or on the AVG portal for end users to download and install. You need to download the SPO software images from the portal/server before you install them in the USB flash drive, U3PUSB device, or CD-ROM.

There are three SPO client images available which support different forms of portable storage. They are:

- MSI image for use on USB 1.1 or higher flash memory devices
- U3P image for use on U3 type flash memory
- ISO image for use on CD ROM.

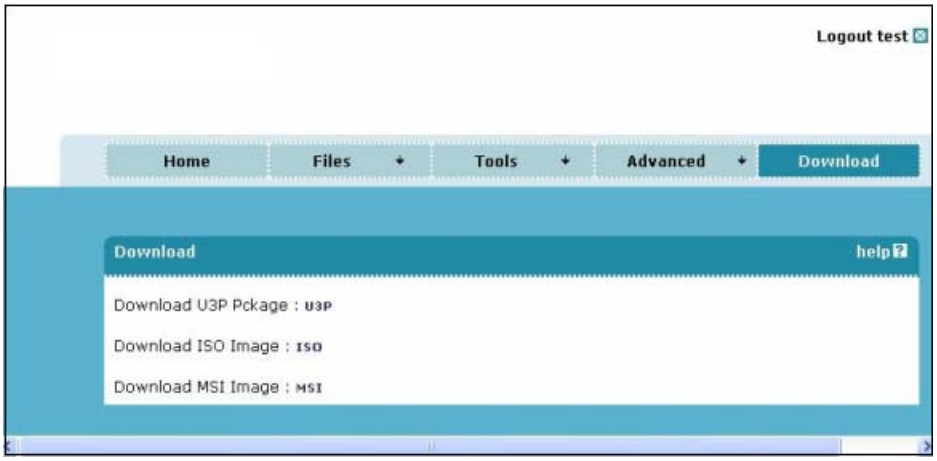
Note:
In this document the term CD-ROM refers to CD-ROM, DVD, CD-R, and CD-RW as appropriate.

Downloading SPO Client

This section explains the steps to download the MSI, ISO, or/and U3P images software from the portal:

1. In the available web browser, the user should enter the domain address (for example https://vpn.example.com).
2. To log in, the remote user should enter his or her user name and password in the Username and Password fields, respectively.
3. Click **Login**.
4. Click on the **Download** tab in the portal to download the MSI, ISO, or U3P image.

Note:
The Download tab is only available in the portal when the System Administrator has enabled the SPO access.For information on how to enable the SPO in groups using CLI, see *Avaya CLI Application Guide, (NN46120-101)*. For information on how to enable the SPO in groups using BBI, see *Avaya BBI Application Guide, (NN46120-102)*.



5. Double click on the software image that matches USB flash drive (MSI), U3P USB, or CD-ROM (ISO) image.
6. Download MSI and u3p files directly to appropriate USB flash drive.

Note:
If you have downloaded the U3P image, rename the .zip file to .u3p format before installing.

Installing SPO Client

This section explains the steps to install the SPO client software in USB flash drive, CD-ROM, and U3P USB device.

Installing MSI image

To install the MSI image, use USB flash drive 256 MB. Recommended using 1 GB or larger. The following procedure explains the steps to install an MSI image onto a generic USB flash drive.

1. Double-click on **Download MSI Image : MSI**.

   SPO Client Setup Wizard appears.
2. Click **Next**.

   SPOClient Setup Wizard with Banner text appears.
3. Select **I accept the terms in the License Agreement** and click **Next**.

   SPO client Wizard with installation folder location appears.
4. Select the USB flash drive for installation and click **Next**.

SPO Client Setup Wizard with installation mode appears.

5. Select the SPO Client software installation mode.

   The two different modes are **Fresh install** and **Format and Install**.

   - Select **Fresh install** if you want to install the SPO client software without formatting.

     A new folder is created for installation.

   - Select **Format and Install** if you want to format the device before installation.

     The format option will remove all previously installed files and data from the target device.

6. Click **Next**.

   SPO Client Setup Wizard with installation ready message appears.

7. Click **Install** to install the SPO application on the USB flash drive.

   SPO client application Setup Wizard with installation complete message appears after successful installation.

8. Click **Finish** to complete the MSI installation.

Installing U3P image

The following procedure explains the steps to install an U3P image into a U3 USB device.

1. Launch the U3 launch pad from the system tray.



2. Go to **Add Programs** and click **Install from my Computer** link.
3. Navigate to the downloaded U3P file.

   U3 Add graphic wizard appears.
4. Click **Next**.

   Installation process begins.
5. Click **Next**.
6. Click **Done** to exit the Add Program Wizard.

   Installation process completes.
7. Go to U3 launch pad.

Installing CD-ROM, CD-R, CD-RW, or DVD

The following procedure explains the steps to install SPO client software CD-R, CD-RW, or DVD:

1. Insert empty CD-ROM, CD-R, CD-RW, or DVD into the CD-ROM, CD-R, CD-RW, or DVD drive.
2. Open the web browser and login to the AVG.

3. Download the ISO image from the portal and write onto the CD-R, CD-RW, DVD.

   The Client application runs after writing the ISO image into the CD-ROM, CD-R, CD-RW, or DVD disk.

4. Re-insert CD-ROM.

   The SPO client application automatically runs.

For more information about installation process, see Downloading and Installing Secure Portable Office Client on page 15.

Portable Applications Installation

Portable applications are the software programs that can be stored on any storage device like USB flash drive (generic or U3P format). Therefore, the user can add their favorite software applications like web browser, email client, office suite, calendar/scheduler, instant messaging client, antivirus, and so on a USB flash drive to be used on multiple computers. The portable applications can be downloaded into the USB flash drive from portable application websites like http://portableapps.com/, http://www.portablefreeware.com/, and http://www.u3.com/ if you have a U3 capable USB flash drive.

Portable Applications can be downloaded to the USB flash drive in two ways:

- Public website
- AVG Server

Note:

For information on downloading Portable Applications on AVG server see *Avaya Administrator Guide*, (NN46120-105).

Installing portable applications from public websites

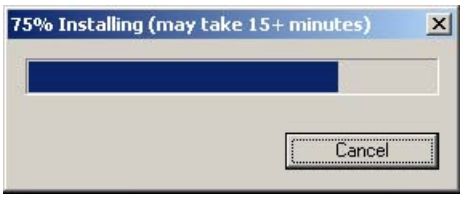
You can download the portable application from the website mentioned above into the USB flash drive and create a link for it in the User Links section of the Dashboard. For information on how to create user links, see Application Links on page 33.

You can install the portable applications up to 10 MB.

1. Open the Web browser.
2. Type the protocol and IP address http://portableapps.com/ to install the portable application.
3. Press **Enter**.
4. Click **Download**.
5. Download the application into the USB flash drive.



6. Click **Install**.



The software is installed on the USB flash drive.

Note:
To view the list of installed applications, click on the **Status** tab on Dashboard.

Chapter 5: Configure Secure Portable Office Client

This section explains the configuration processes of SPO Client. There are two options for configuring SPO feature. One option is configuration by the end user after they have installed the client. The other option is pre-configuration by the AVG administrator so that the end users does not have to do the configuration themselves. There are also SPO client customizing options that the AVG administrator can use.

Following topics are discussed:

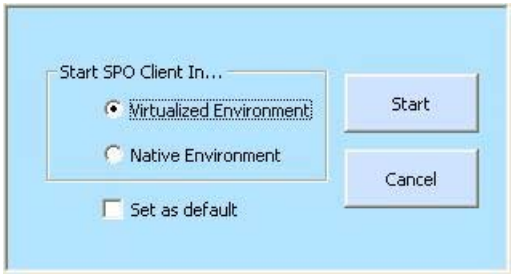
- Configuring SPO on page 21
- Dashboard on page 24
- System Tray on page 37
- Enabling auto-start application for U3P on page 38
- Removing Secure Portable Office from U3 USB on page 38

Configuring SPO

After the SPO client is installed, if not preconfigured, it must be configured by the end user. The following procedure explains the steps to configure the SPO Client. When choosing the virtualized environment, ensure application images are created with a tool while installing the application on a computer before the virtualization takes place.

1. Double-click the executable file in the following location: `<usbdevice>://AutoRun.exe or <usbdevice>://SPOClient/StartSPO.exe`.

   Start SPO Client In dialog appears.



Note:

The SPO Client launches in native mode if you access the executable file directly from the following location: `<usbdevice>://SPOClient/SPO Client.exe`.

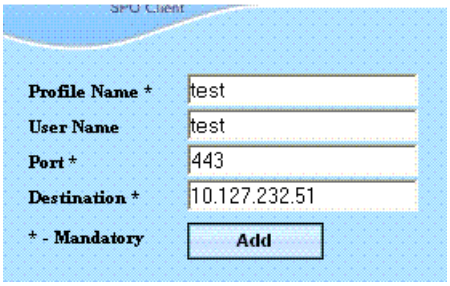
2. Click **Virtualized Environment** if you want to work within a virtual workplace from the USB or click **Native Environment** to run applications from the web server. The SPO Client can be launched from a read-only media only in native mode. Click the **Set as default**. If you want to save this environment to open automatically the next time you run SPO. Click **Start**.
3. If you are logging on SPO for the first time you will receive a **Ceedo Trial Version** license reminder window alerting you to import the license before the expiry date.

   For more information, see Importing Ceedo license on page 43.



Or

The SPO VPN dialog box appears.



4. To create a new profile for the SPO Client, enter the profile name, user name, port, and destination.

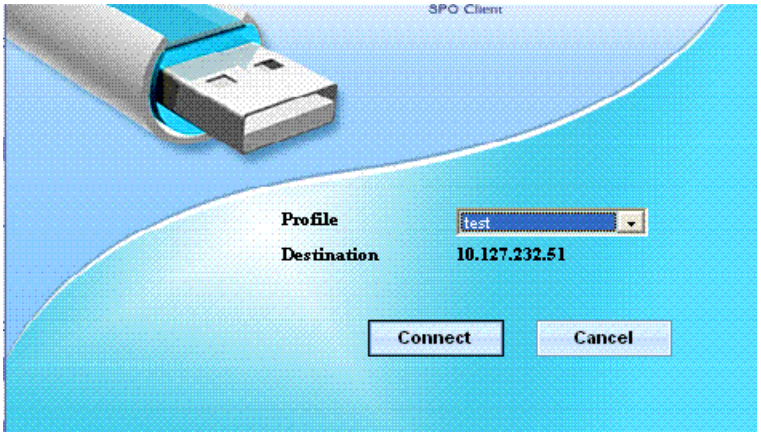
   The profile name and the user name are alphanumeric fields with not more than 30 characters.

Note:

Destination can be domain name or the IP address of the VPN Gateway provided by your system administrator.

5. Click **Add**.

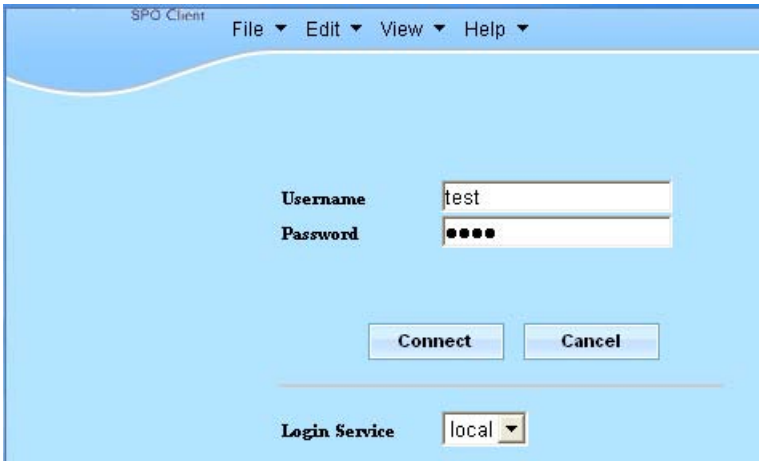
   Login splash screen appears.



Note:

The security warning messages appear if the server certificate is invalid. To hide the security warning messages, in SPO user interface, select **Preferences > Autohide warning messages**.

6. Click **Yes**.



7. Enter the password and click **Connect**.
8. In the **Login Service** list, select the authentication method to connect to the server.

   If default value is selected, all the authentication methods that are defined for the user are selected one after the other.

9. Click **Connect**.

When the authentication method is successful, Banner Text appears.



Note:

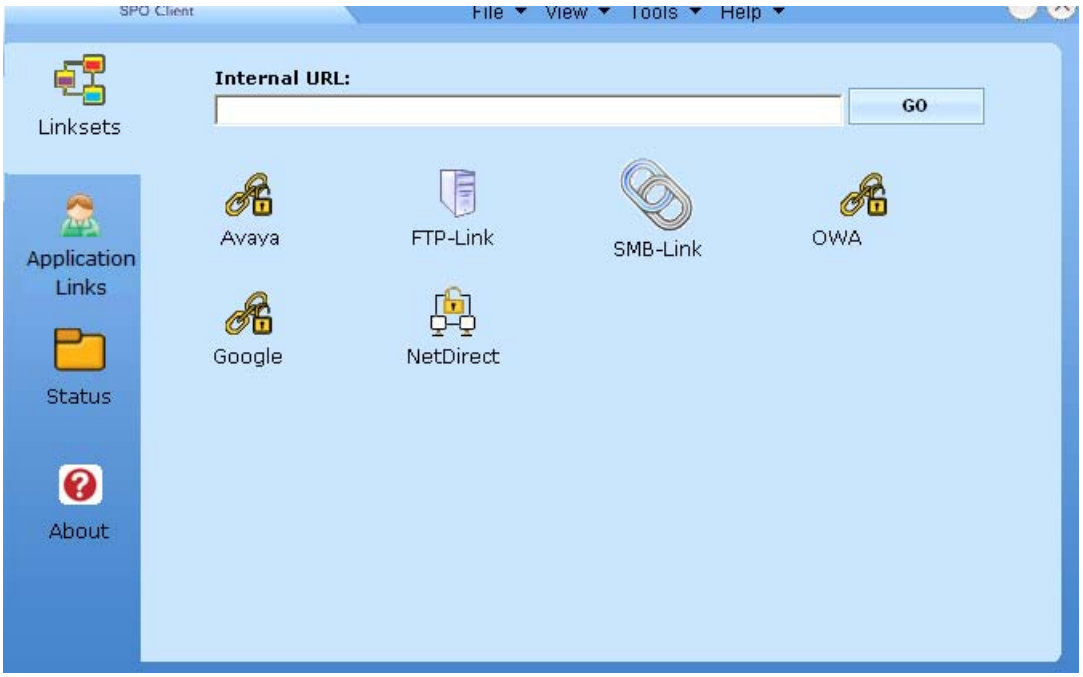
This can be customized by the System Administrator as per the requirements.

10. Click **OK**.

    Dashboard and system tray application are displayed. This contains all the linksets the end user is authorized to access.

Dashboard

This section explains the various menu options and tabs available in the dashboard. The Internal URL navigation bar is used to navigate any internal URL that administrator did not configure in the linksets links.



Following menu options are available in dashboard:

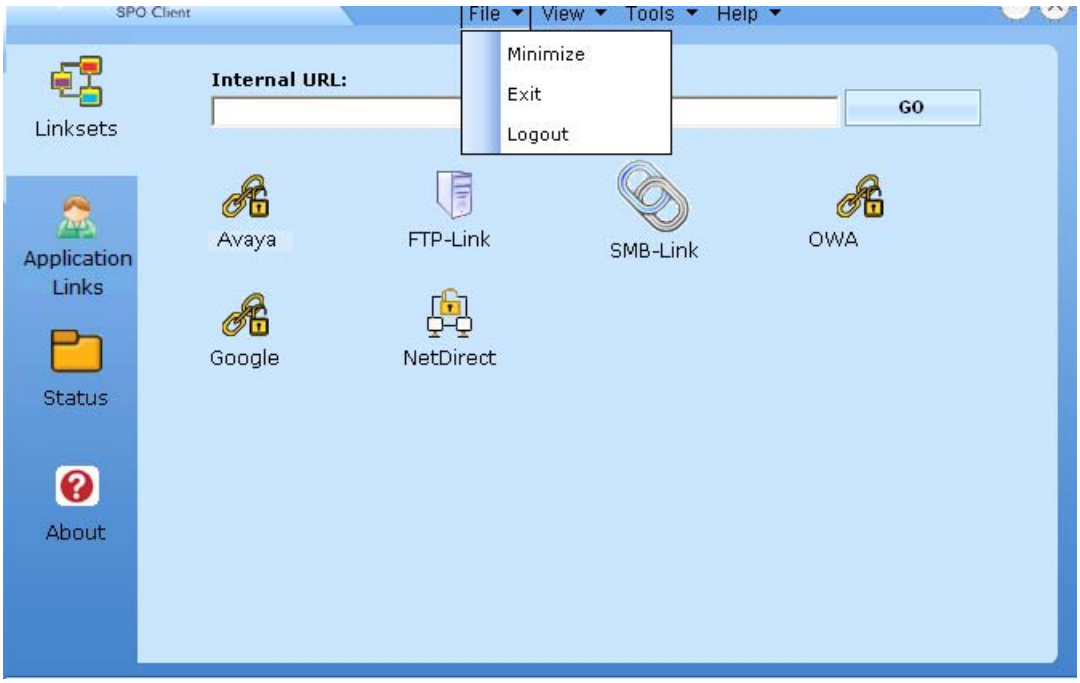
- File menu on page 25
- View menu on page 26
- Tools menu on page 27
- Help menu on page 28

Following tabs are available in dashboard:

- Linksets
- User Links
- Status
- About

File menu

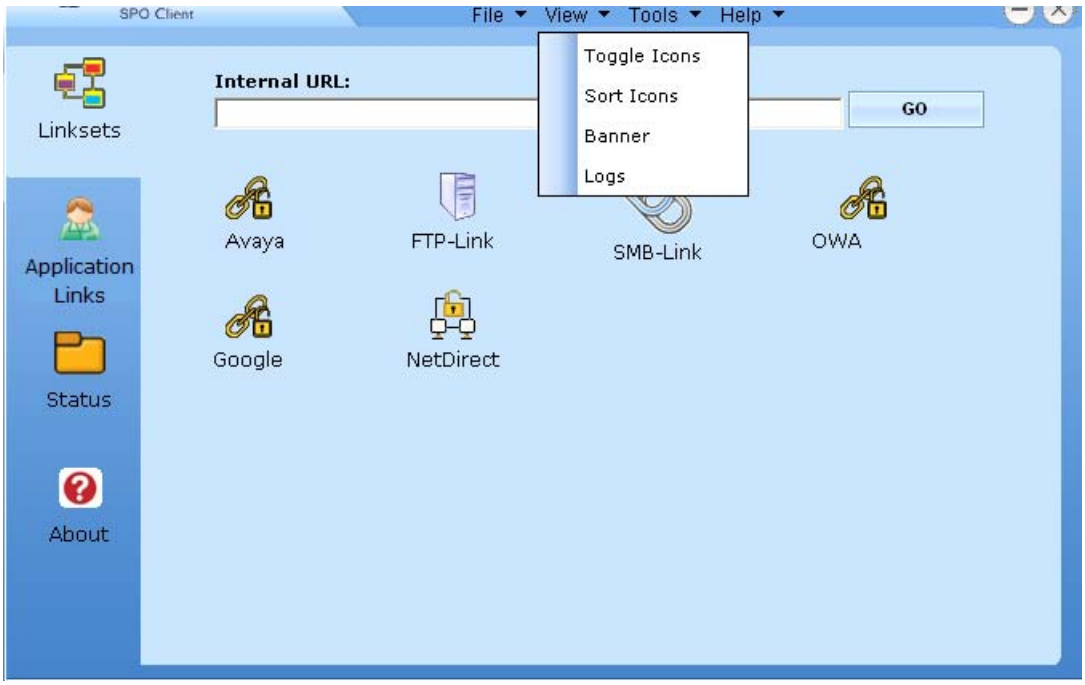
This section explains the following functions of the file menu:



- Minimize - minimizes the application in the system tray and removes them from the windows taskbar.
- Exit - logs out from the AVG server by closing all open windows that were started by the SPO application.
- Logout - logs out from the AVG server and closes all the open applications/windows and goes back to initial login screen.

View menu

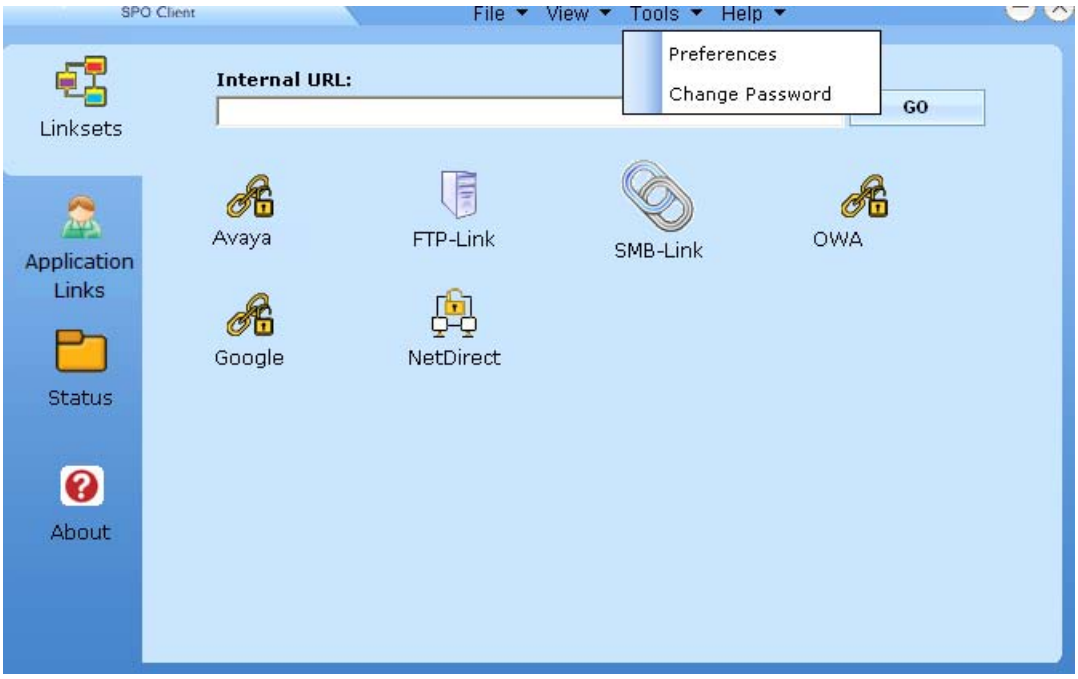
This section explains the following functions of the view menu:



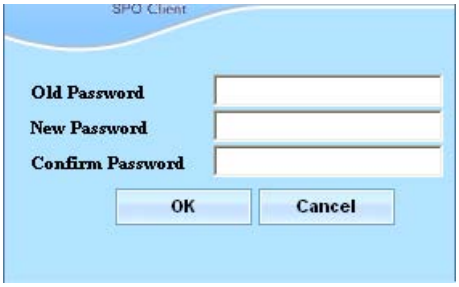
- Toggle Icons - removes the icons from the dashboard links. Clicking again brings the icons again.
- Sort Icons - sorts the icons alphabetically within the linkset. Clicking again sorts the icons in original format.
- Banner - Navigates to the SPO client banner screen.
- Logs - Navigates to the SPO client log file.

Tools menu

This section explains the following functions of the Tools menu:

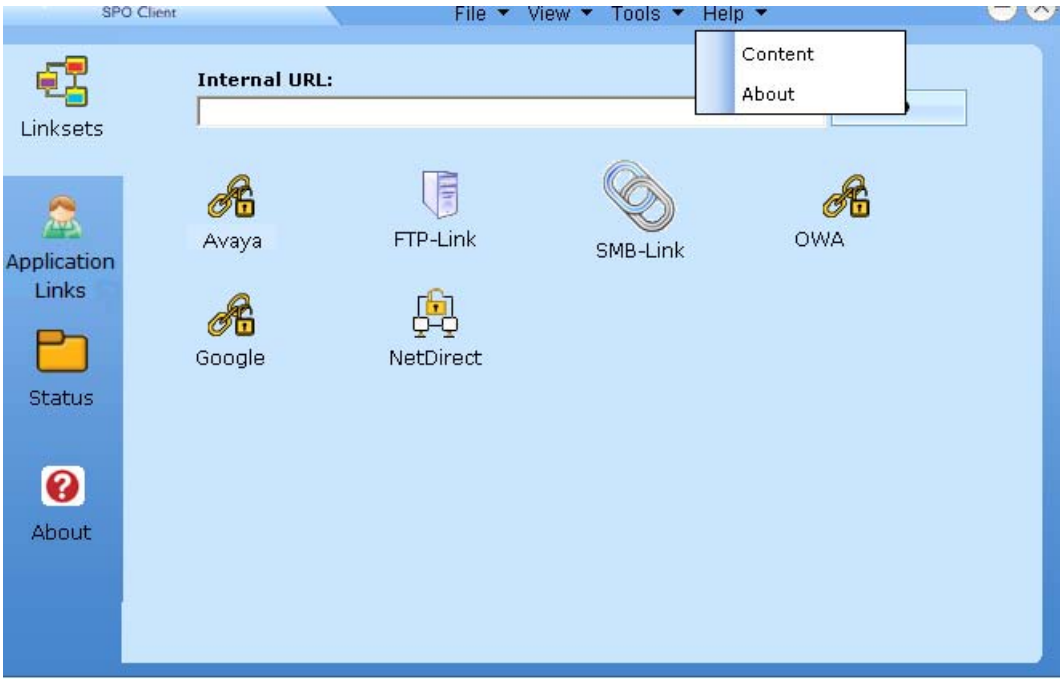


- Preferences - This option has multiple user preferences. These are stored on the local USB flash drive. For more information about the preferences, see User Preferences on page 29.
- Change Password - This option pops up a dialog for changing the password for the current user. This option is only available if login service is Local.



Help menu

This section explains the following functions of the Help menu:



- Content - takes to the SPO Client windows help file. Also it supports "F1" shortcut for help file.
- About - takes to the About tab in the left side tabs.

User Preferences

This section explains the various preferences given to a user. To access these preferences navigate **Tools->Preferences**.

Following are the user preferences:

- General on page 29
- Logs on page 31
- Profile on page 32
- Application Links on page 33
- Web browser on page 35
- Language on page 36

General

This section explains the various general preferences for a user. The following screen shows the different preferences.



You can set the following general preference for a user:

- Save user profile: It saves the user changes on the profile. For example, when a user creates a profile with username test and saves the profile and connects to the server and when the user is in login screen, if the user changes the username to testuser, the testuser will be saved in the configuration file. When the user tries to connect next time the username appears as testuser.
- Suppress security warning dialog: If this option is enabled, it tries to auto click the security warning dialogues if there are un-trusted SSL certificate that cannot be verified by the host from AVG server.
- Allow multiple web instance: Suppose there is one link for "OWA - outlook web access", when a user clicks the OWA link, a new web browser opens and shows the content. After Allow multiple web instance is disabled, and user clicks the same link again while the previous opened web browser for that link is still active, the old windows is brought to foreground. When Allow multiple web instance is enabled, every time user clicks the link, new web browser window opens for the link.
- Automatically connect to the server: With this option enabled the SPO client will automatically attempt to connect to the previously connected AVG server. This simplifies the connection process for the end user.
- Rotate log files: After the log file has reached 500 KB, log file starts deleting the old entry and add on the new entries into the log file.

Note:

This option should not be used if there is more than one connection profile configured on the SPO client.

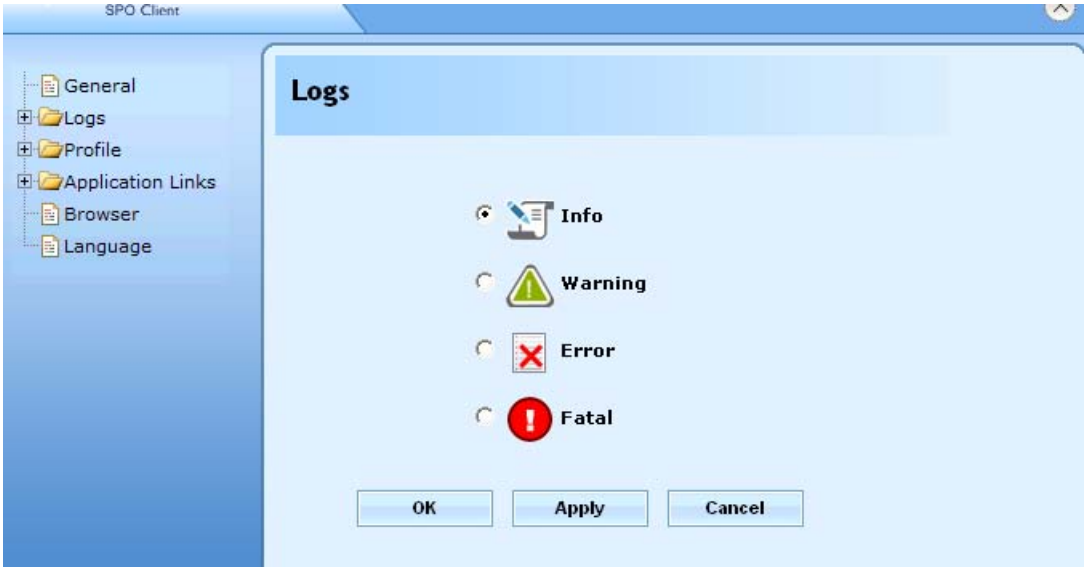
- Autofill RSA soft token for RSA authentication: If the authentication method is RSA, and the user uses the RSA soft token, by selecting this option, the user is prompted to enter PIN, instead of passcode.
- Reset the SPO startup environment settings: Removes the user selected default settings for either Virtualized Environment or Native Environment as chosen in the Set SPO Client window.

  Reset the SPO startup environment settings: is automatically selected if the default settings is not selected during startup.

Logs

This section explains how the user can change log levels. The following screen shows the criticality of the log files.

For information on client log messages, see Appendix Syslog Messages in *Avaya Troubleshooting Guide*, (NN46120-700).



The following log levels are available:

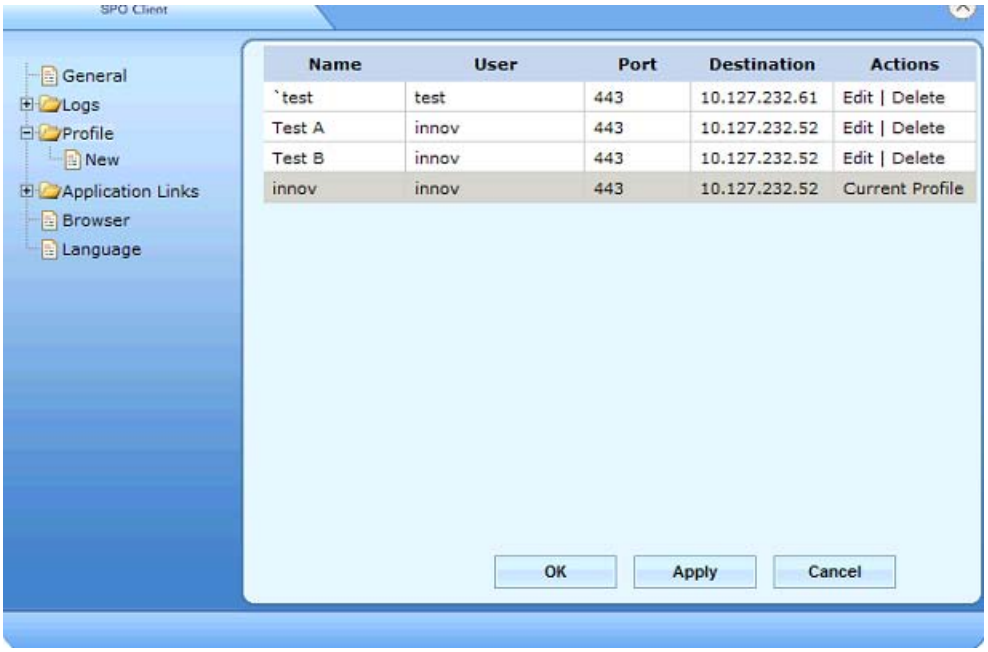
- Info
- Warning
- Error
- Fatal

The Options has View Log, to open log file with default text editor and Clear Log to clear the log file.

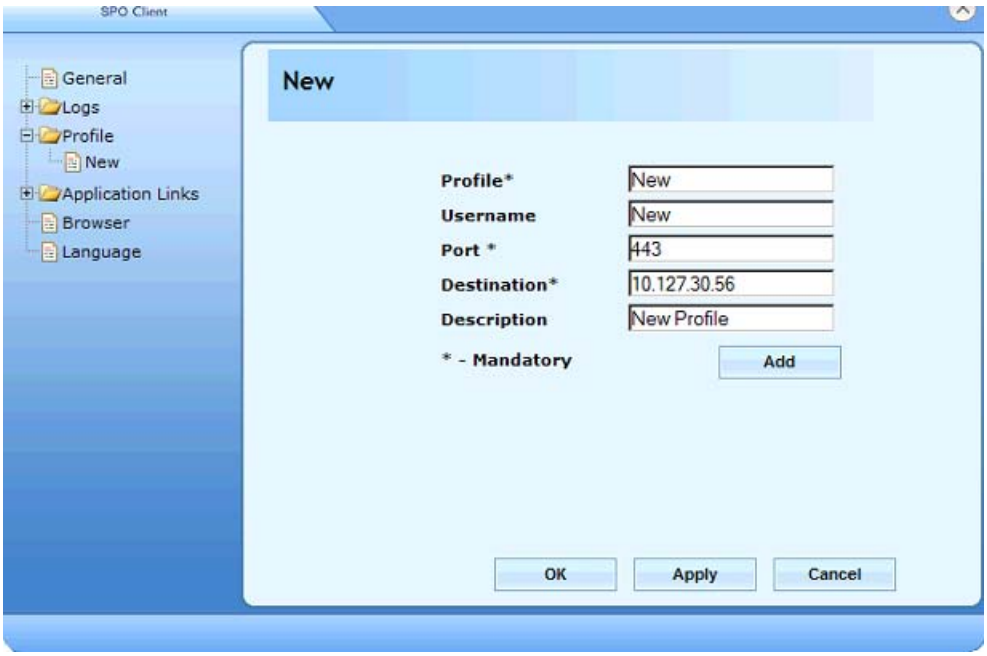


Profile

This section explains how to add and edit the profiles for the SPO client. The following screen shows a sample profile.



The current profile is greyed out, therefore cannot make any changes to this profile. However, other profiles are edit-able by the user. User can also add a new profile by clicking on New option.



For information on how to create a user profile see Configuring SPO on page 21.

Application Links

This section explains the Application Links option. These are the local links and not from the server. These are customizable links that are available only for the SPO user.

User can copy any application in the USB flash drive and create a link for it. These links are shown in the Application Links tab in the Dashboard application.

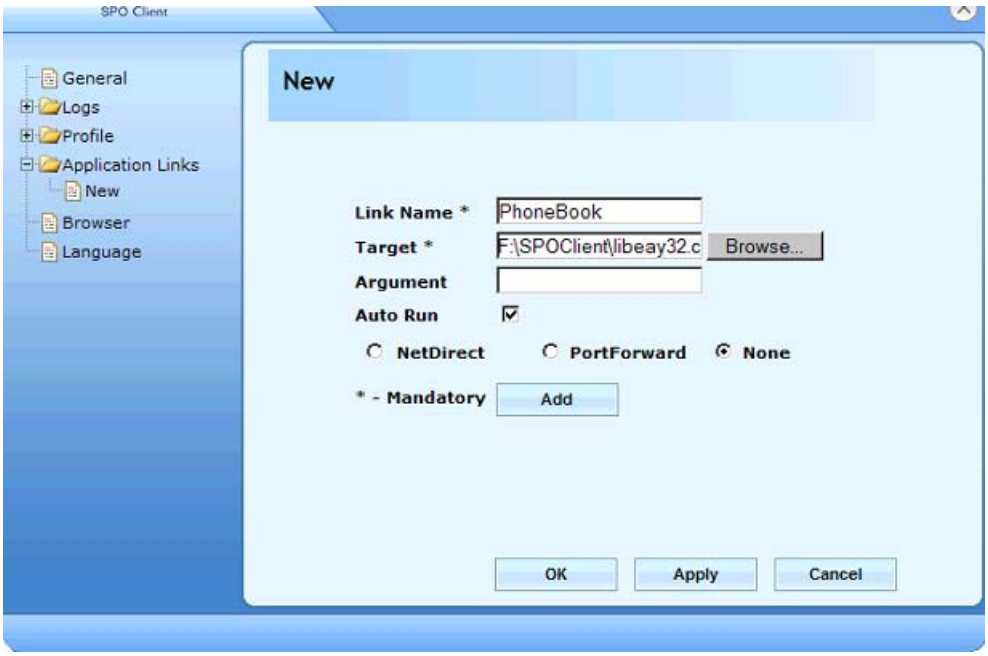
Using the application links, the user can create a link. This link can be shortcut to the windows installed application on the local machine or portable application available in the USB flash drive. When loading these application links in the USB, the links are validated. Only if the link is valid, it is shown in the application under application links application. Otherwise, the links are not loaded in the SPO client.

In virtualized mode, you can add shortcuts to the virtualized applications. The shortcuts to the virtualized applications are visible on SPO interface if they are running in the virtualized mode.

The following procedure explains the steps to add a new link:

1. Under **Application Links**, click **New**.

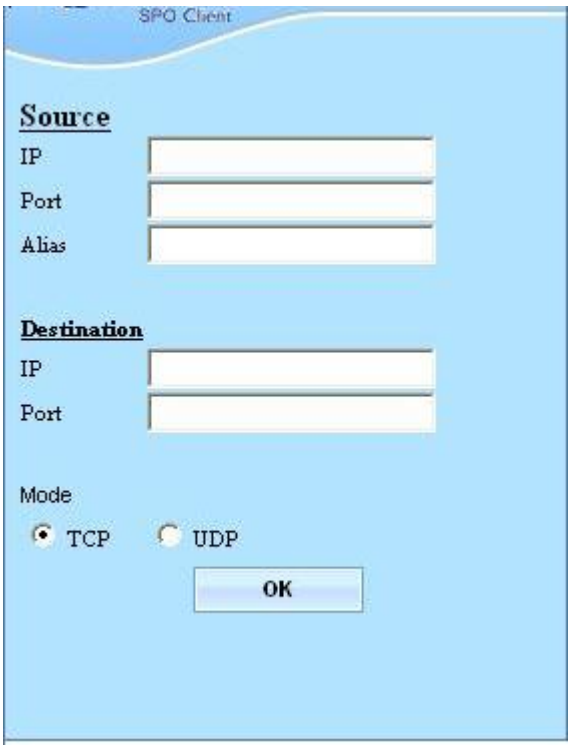
   Links screen is displayed.



2. Enter the name for the link that you want to create.
3. Enter or browse for the destination file and select the application for which you need to add shortcut in user linksets.
4. Select **Auto Run** if you want to navigate to the dashboard screen during authentication.
5. Select **NetDirect** or **PortForward** as prerequisite if you require to start Netdirect or PortForward.

Note:
The NetDirect or PortForward gets started if you make it as a prerequisite.

When you select **PortForward** as a prerequisite, the following dialog box appears for the PortForward configuration.



a. Enter the Source IP, Source Port, Alias, Destination IP, Destination Port.

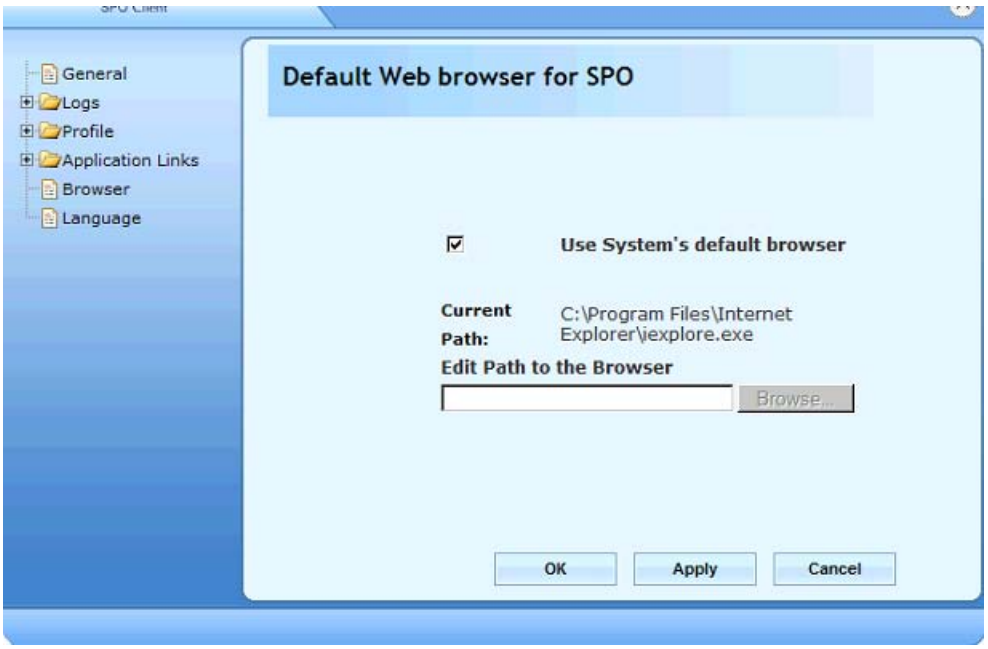
b. Select the **TCP** or **UDP** mode.

c. Click **OK**.

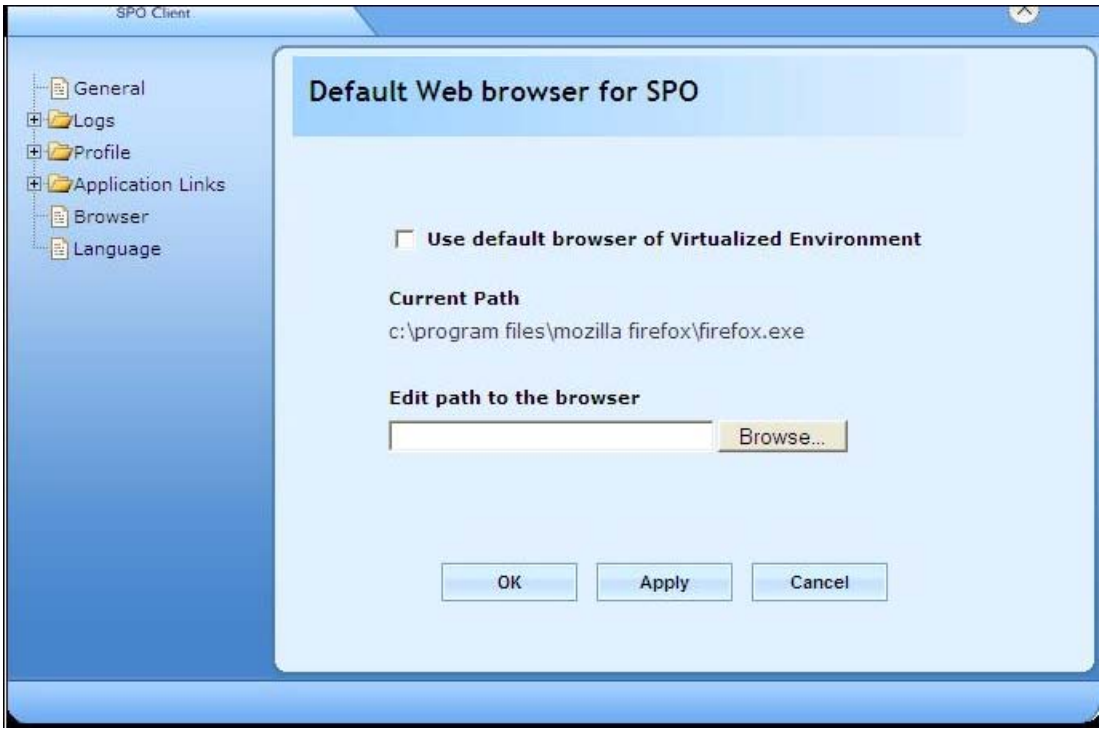
6. Click **Add** to add a new link.
7. Click **OK** and **Apply** to apply the changes.

Web browser

You can add or edit a default web browser by either copying the link or by clicking Browse and searching for the executive file. If you are accessing web browser in native mode, the following dialog appears:

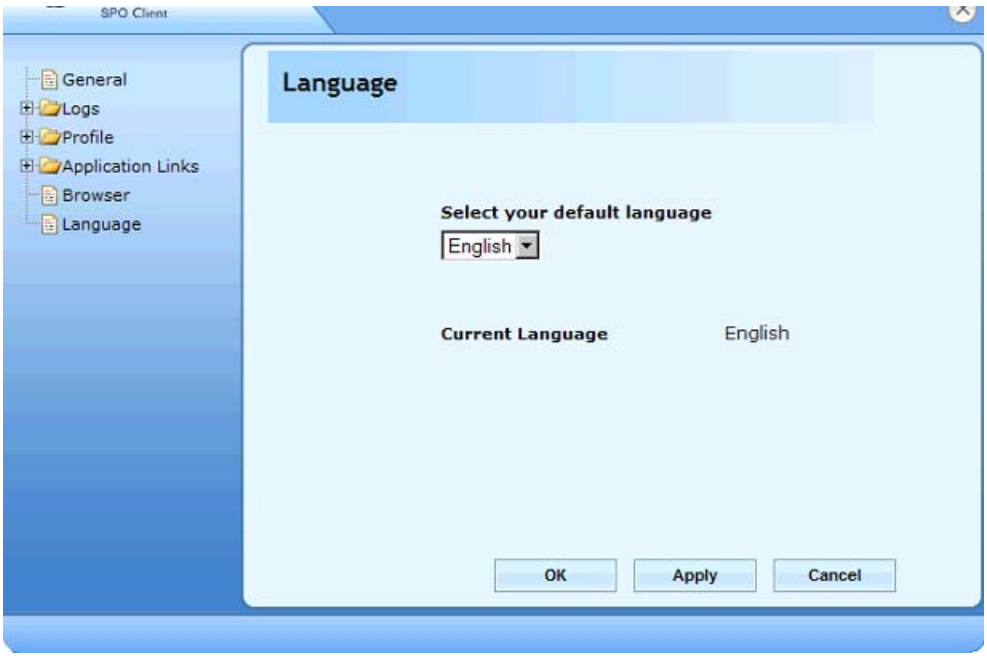


If you are accessing web browser in virtualized mode, the following dialog appears:



Language

Currently English, German, and French languages are supported. But user can add their language by copying one of their language file in the path `<usbdrive>/SPOclient/Lang` and changing the caption text.

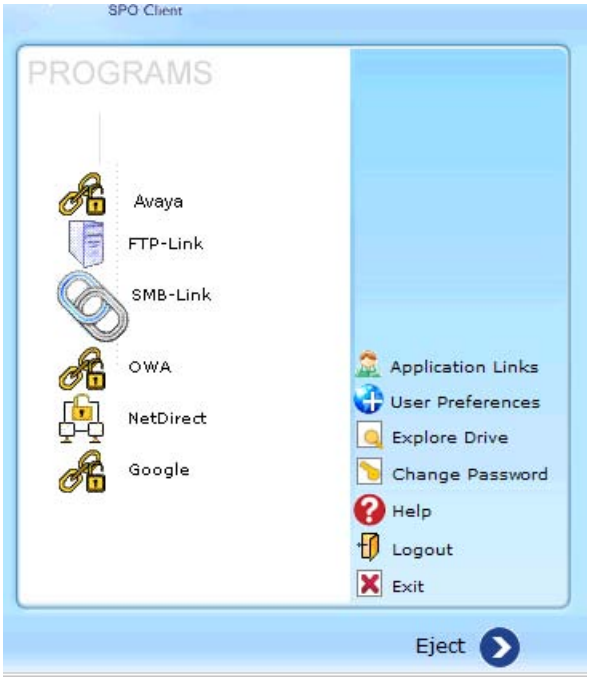


System Tray

System tray menus are similar to the dashboard links and menus except, ExploreDrive and eject option. ExploreDrive opens an explorer window with the USB flash drive with browse option. The eject option ejects the USB flash drive from the windows after performing logout and closing all the open windows and SPO client application. The following screen shows the system tray with links and menus.

Note:

Even though many links are available in the linksets, only the first 16 links are shown in the system tray menu.



Enabling auto-start application for U3P

This section explains the steps to enable the auto-start SPO application when U3 USB device is plugged in to your computer.

1. Go to U3 launch pad.
2. Click **Settings** at the right hand side of the launchpad.
3. Select **Program Settings** .
4. Select the U3 SPO client.
5. Select **Start on Insertion** check box to enable the SPO auto-start application when U3 USB is plugged into the computer.

   Now when you un-plug the U3 USB and re-plug it in the computer the SPO application is auto-started.

Removing Secure Portable Office from U3 USB

This section explains the steps to remove the SPO application from the U3 USB device:

1. Go to U3 launch pad.
2. Click **Settings** at the right hand side of the launchpad.

3. Select **Program Settings** .
4. Click **Remove Program** to remove the SPO client from the U3 USB device.



5. Click **Yes** to remove the SPO application and when the application is removed, click **Close** to exit the window.

Chapter 6: Ceedo Licensing

The AVG SPO Application requires Ceedo license. This chapter provides general information about Ceedo License, and also explains how to import and activate the Ceedo license.

The AVG SPO Application Virtualization mode ships with 45-day Ceedo ™ temporary license. The license is activated only after first use of the SPO Application Virtualization mode.

Note:
To activate AVG SPO Application Virtualization mode, you need both AVG SPO license and Ceedo licenses. If you use Native SPO mode, only AVG SPO license is required.

SPO application virtualization license

You can get the SPO application virtualization license in the following ways:

- Request your administrator to contact Ceedo to acquire pool of activation code, and to provide you the activation code.
- You can contact Ceedo directly and acquire license

Ceedo (SPO application virtualization) license basic

The Ceedo™ license mechanism binds the Ceedo license to the hardware identifiers of the USB drive on which Ceedo is installed. If the Ceedo is installed on a USB drive, the hardware identifiers are the Vendor ID, Product ID, and serial number of the drive. In this case, each Ceedo license is unique to the drive for which it was issued.

Starting from Ceedo version 3.0, Ceedo introduced automatic activation mechanism. You can purchase a Ceedo license either from within Ceedo software or without — the hardware identifiers are not transmitted to Ceedo servers at this stage. After making a complete payment for the purchased license, you receive activation code automatically. Using this activation code you can activate your Ceedo installation immediately.

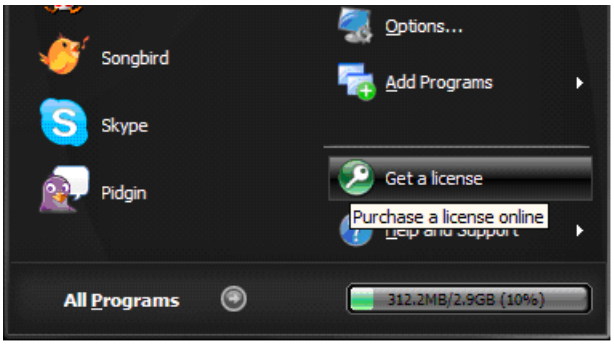
Activating Ceedo Enterprise from Within the Ceedo Environment

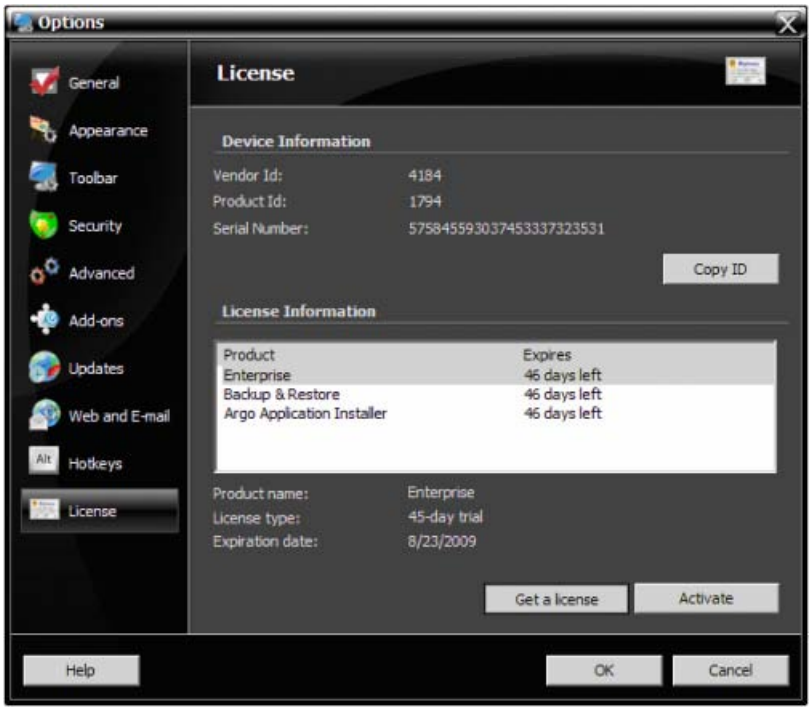
Perform the following procedure to activate Ceedo from within the Ceedo environment.

Procedure steps

1. Click **Get a License** to initiate the license purchase process.

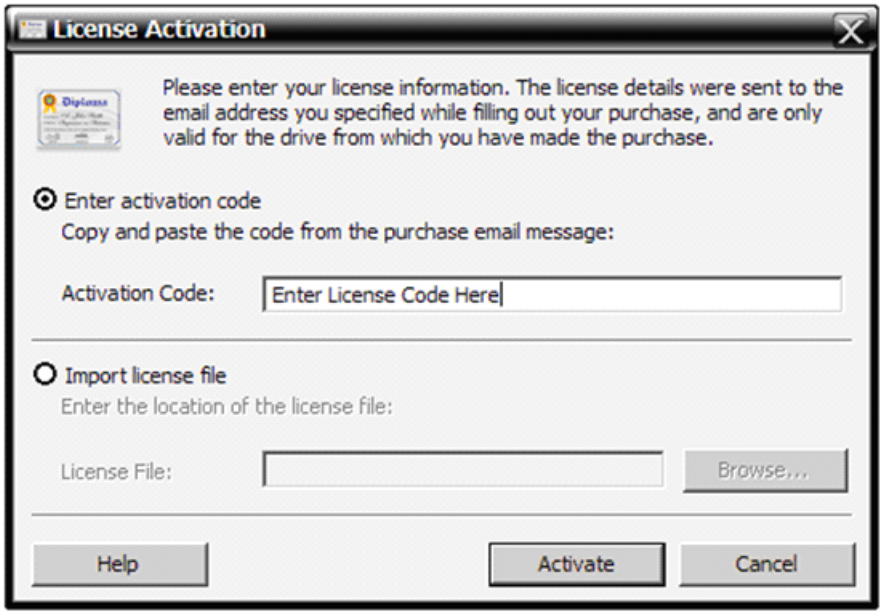
   The **Get a License** button is available in both the Ceedo easy-access menu and the License section of the Ceedo Options panel, as shown in the following figures.





2. After receiving the activation code, open **Ceedo Option**, **License** .

3. Click **Activate**. The **License Activation** dialog box appears, as shown in the following figure.



4. Enter the activation code you received in the **Activation Code** field.

   At this stage, the system sends the hardware information of drive to the server where the license for the drive is generated , and automatically imported into Ceedo.

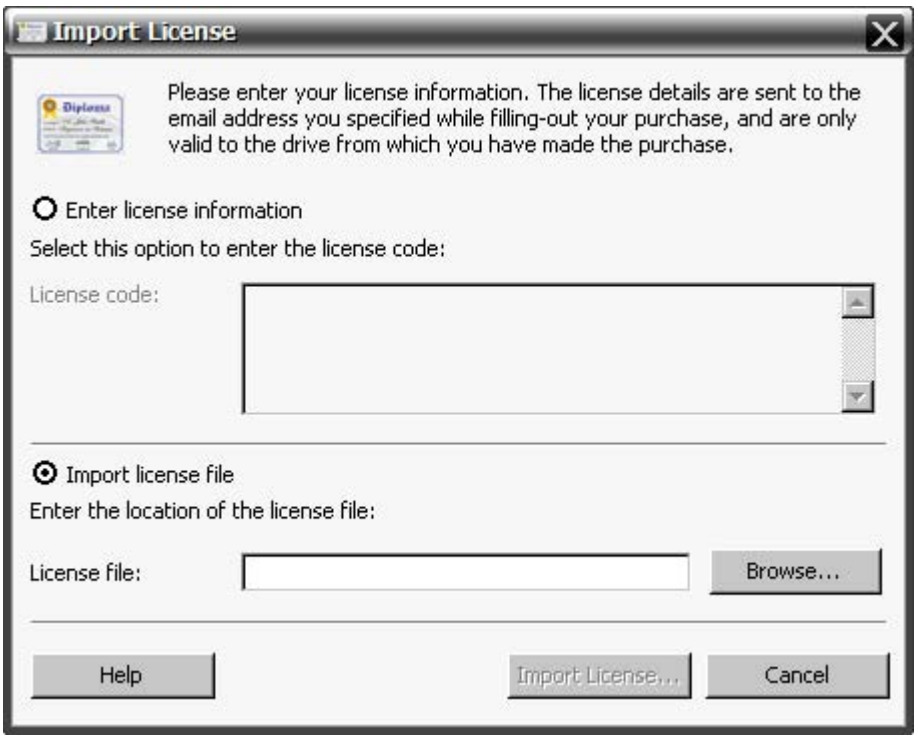
   You can use the activation code for any number of times on the drive for which the license was purchased. Even if you format the drive, the license code still activates Ceedo as long as it is installed on the drive for which the license was purchased. You can use the license to activate multiple images installed on the same drive simultaneously.

Importing Ceedo license

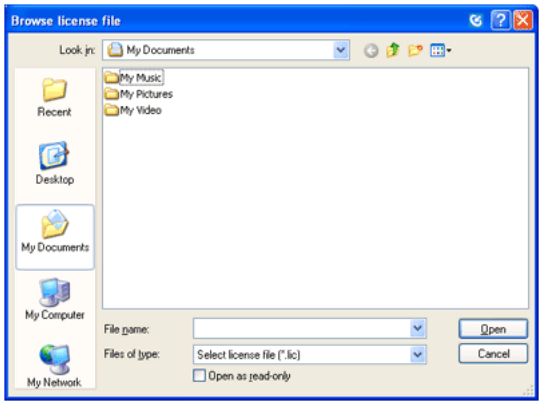
Ceedo trial version license reminder appears if you are logging on SPO for the first time. You can import the Ceedo license from the Invalid License dialog. To import the Ceedo license, perform the following procedure:

1. Click **Import License**.

   The **Import License** dialog appears.



2. Select **Import license file**.
3. In **License file**, enter the location of the Ceedo license file or click **Browse** to locate the file.



4. Click **Open**.

   The Import License dialog appears.
5. Click **Import License**.

   The license is imported.

Chapter 7: Authenticating Secure Portable Office Client

The SPO Client requires authentication with the AVG server. This chapter explains the various authentication options available with the SPO client.

Authentication with Avaya VPN Gateway Server

User needs to authenticate with the SPO client to the Avaya VPN Gateway. This section explains the steps to authenticate the Secure Portable Office (SPO) with AVG server.

1. Insert the USB flash drive into the drive.
2. If authentication method is other than Client Certificate, Splash screen appears.
3. The username in the **Username** field is the Profile username that is given during the creation of the profile.

   This is an alphanumeric field with not more than 30 characters in it.
4. Enter the password in the **Password** field.

   The password is provided by your system administrator.
5. Click **Login**.

   After the SSL link is established between the SPO client and the AVG, the user's login credentials (username, password) are sent for authentication.

Authentication methods

The SPO client can authenticate with all the methods supported by the AVG. The authentication system supports the following methods:

- Username/password to local AVG directory
- Username/password to LDAP, RADIUS
- Dual authentication
- Secure ID

- Client Certificate authentication
- Password change support

For more information about these authentication methods, see chapter Authentication Methods in *Avaya BBI Application Guide (NN46120-102)*.

After the authentication is completed, the SPO needs to be authorized. The SPO client also supports the authorization mechanisms provided by the AVG. The linksets displayed on the SPO client are based on how authorization is configured on the AVG and back end directories.

For more information, see chapter Groups, Access, and Profiles in *Avaya BBI Application Guide (NN46120-102)*.

The SPO solution provides the following authorizations:

- Network control over the applications the user can access based on the end-user identity.
- Display restrictions on applications shown in the system tray and launch pad on the Windows client, based upon the current access privileges for the user.
- Client filter based on SPO. Administrator can configure extended profiles based on client filter access method as **SPO**.

Software Upgrade and Package

The user can upgrade the existing SPO software version to the new software version. Following steps describes the process involved in this upgrade:

1. After the SPO software client authenticates with AVG server, AVG server sends an XML configuration file to the SPO Client.

   The XML file contains the current software version and the MD5 checksum available in the AVG server.

2. The SPO software client validates with the existing software version and initiates the software upgrade.

   Note:
   The upgrade takes place if there is a mismatch in the software version.

3. Once the upgrade is done, the current running client restarts using the new code.

   Note:
   After the upgrade, the user need to login into client again.