

**Setting Up SSO in Your Workstation**

**Identity and Access Management (IAM)**

|  |
| --- |
| **Document Version: v1**  **Version Date:** 09 September 2019  **Document Owner**: EY IAM  **Document Classification:** CONFIDENTIAL |

|  |
| --- |
| This document contains proprietary information. All information contained herein shall be kept CONFIDENTIAL. None of this information shall be divulged to persons other than P&G and EY employees authorized by the nature of their duties to receive such information, or individuals or organizations authorized by P&G or EY in accordance with existing policy regarding release of company information |

**Document Information**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version(s)** | **Date** | **Status** | **Revised by** | **Comments** |
| 1.0 | 5/29/2020 | Complete | Aldrin Castro  Benjamin Pedralvez |  |

Where significant changes are made to this document, the version number will be incremented by 1.0. Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number will be increased by 0.1

**Reviewed by (EY):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Group – Division** | **Signature** | **Date** |
|  |  |  |  |  |

**Owner (EY):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Group – Division** | **Signature** |
|  |  |  |  |

**Approved by (P&G):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Group – Division** | **Signature** | **Date** |
|  |  |  |  |  |

The signatures above indicate an understanding of the purpose and content of this document by those signing it. By signing this document, they agree to this as the formal Phishing SOP document.

Contents

1. [**Process Introduction 3**](#_Toc42141036)
2. [**Roles and Responsibilities 3**](#_Toc42141037)
3. [**Pre-Requisites 3**](#_Toc42141038)
4. [**Setting Up SSO for Users of PG-Issued Computers 4**](#_Toc42141039)
5. [**Setting Up SSO for Users of Non-PG-Issued Computers 5**](#_Toc42141040)

# Process Introduction

This job aid presents the detailed step by step procedure on how to setup the single sign on solution in your workstation for both PG and non-PG computers.

# Roles and Responsibilities

The following are the persons or teams involved in supporting the SAP SSO process from end-to-end.

1. **The User** – the primary recipient of technical support.
2. **Global Help Desk Team (L1)** – the first responders to the situation. They are commonly referred to as “L1 (Level 1)” or the “PG Employee Care”. Their main goal is to resolve the ticket as soon as possible or transfer it to the appropriate resolver group who has the expertise for the specific issue. In this case, if the issue is SSO-related, they should transfer the ticket to the SAP SSO analyst (Level 2 Support) upon presentation of the initial troubleshooting steps done and detailed screenshots of the persisting error.
3. **Level 2 Support (L2)** – refers to the SAP SSO analysts or “specialists”. They are the first point of contact of the user for any SAP SSO-related incidents whether in SNOW or in the ION email. The SAP SSO analyst also has the added task of managing the [ssoapp.im@pg.com](mailto:ssoapp.im@pg.com) mailbox.
4. **Other IAM Teams** – refers to other teams who have a different skill set that are required to resolve a specific issue.

# Pre-Requisites

Here are the pre-requisite access and applications that must be installed or requested prior to setting up SSO. Please be advised that if the user is unable to follow the procedures on the KB Articles that will be mentioned below, the user may contact the PG Employee Care for assistance:

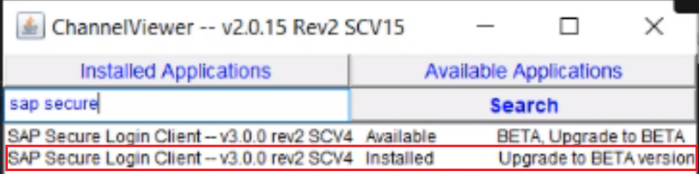
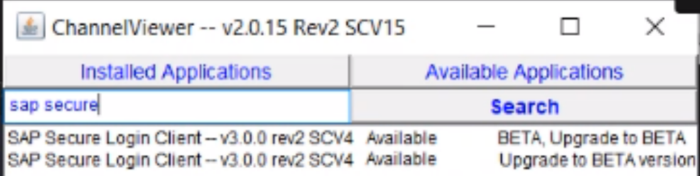
* Chat: [gethelp@pgemployeecare.com](mailto:gethelp@pgemployeecare.com)
* Email: [gethelp.im@pg.com](mailto:gethelp.im@pg.com)

The following are the required access and applications that the user must have before setting up SSO:

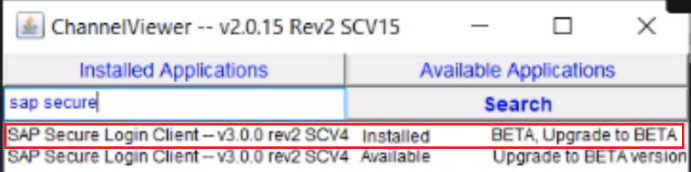
1. Access
   1. **Intranet Access** – This is the first and foremost access that the user needs to have prior to setting up SSO in his/her workstation. The user may refer to this published KB Article for instructions on how to request for intranet access – [KB0012126](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=7a5b88f1db4c9c14072b24f405961921).
   2. **Administrative Credentials** – Installation of the SAP Secure Login Client (SAP SLC) especially for users of non-PG-issued computers require an administrative access. The user should make sure to secure one when installing the SAP SLC application. For users of PG-issued computers who are installing via the ChannelViewer application, this may not be required.
2. Applications
   1. **Ping ID** – This is needed when entering credentials on the SAP SLC application. The user may refer to the following KB Articles for reference – [KB0011915](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=35848942db598f843c56fb651d9619f8) and [KB0012031](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=0dea9ededb5183081eaafba31d96195e).
   2. **Pulse Secure** – This is needed to secure the session of the user. The SAP SLC application of the user will not work if the user is not connected to Pulse Secure. The user may refer to this published KB Article for instructions on how to install and setup Pulse Secure in his/her workstation – [KB0546119](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=95588e70dbe1c0d4dcc82ad94b961983) and [KB0053227](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=1e6227c5dbdd5b4833445478dc961943).
   3. **SAP Logon version 750 and above** – The SAP GUI is needed to access the SAP systems of P&G. It is highly recommended that the user asks the PG Employee Care Help Desk to install the SAP GUI application on his/her workstation.

# Setting Up SSO for Users of PG-Issued Computers

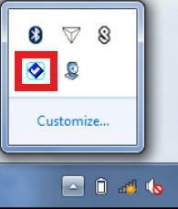
1. Make sure the user is connected to the PG network (i.e., PG Go Wireless wifi or Pulse Secure).
2. Close SAP Logon and other related applications.
3. Open ChannelViewer and then type “**SAP Secure**” then press Enter or click the **Search** button.
4. If you see any installed **SAP Secure Login Client** application, click it, then click **Remove**. This is to ensure that we have a clean installation of the application. Wait until it finished removing.

 🡺 

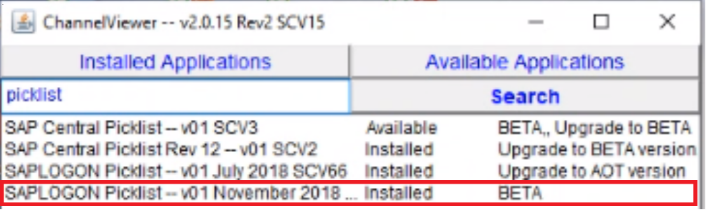
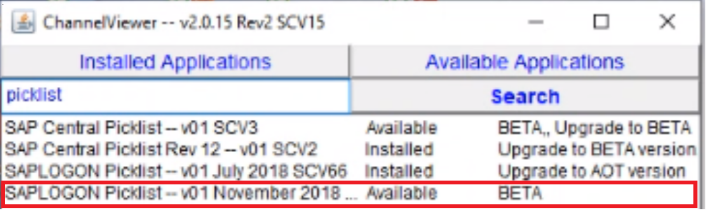
1. After it is removed, click now the **SAP Secure Login Client** – the one with the “BETA” version, then click **Install**. Wait until it finished installing. This may take about 3-5 minutes.



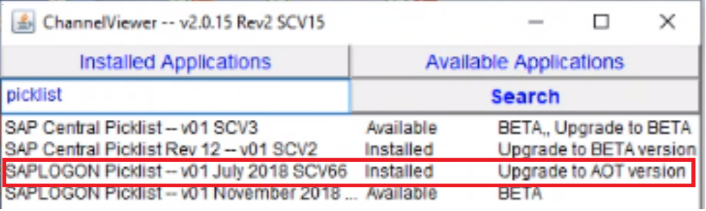
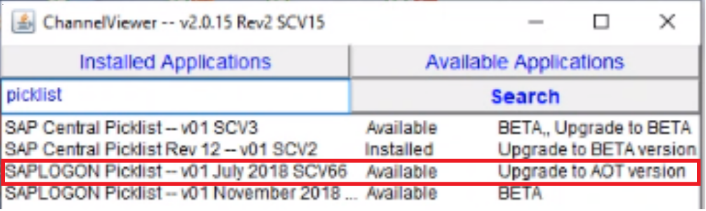
1. You should be able to see now the SAP SLC icon from the taskbar notification tray.



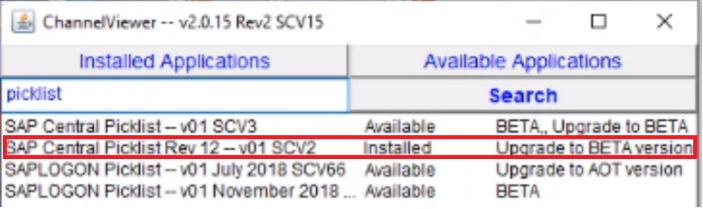
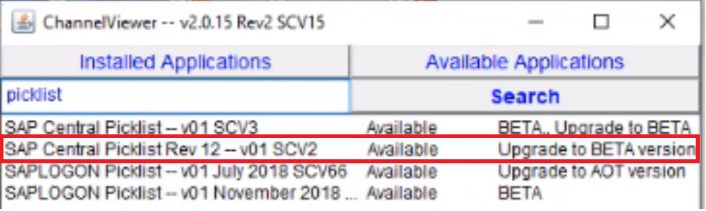
1. If you are not able to see the SAP SLC icon on the taskbar notification tray, that means the installation is not successful. For this, please try manually installing the SAP SLC application instead. You can refer to this published KB Article for guidance - [KB0546118](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=15650270dba1c0d4dcc82ad94b961972).
2. After SAP SLC is installed, type “**picklist**” now on the ChannelViewer application then press Enter.
3. If you see **SAPLOGON Picklist – v01 November 2018** is installed, click it then click **Remove**. Wait until finished.

 🡺 

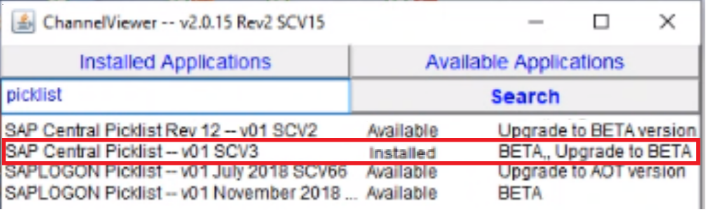
1. If you see **SAPLOGON Picklist – v01 July 2018** version is installed, click it then click **Remove**. Wait until finished.

 🡺 

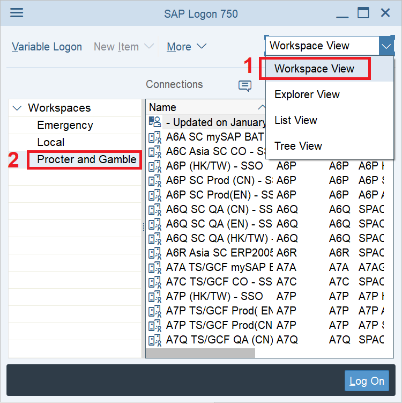
1. If you see **SAP Central Picklist SCV2** version is installed, click it then click **Remove**. Wait until finished.

 🡺 

1. Lastly, click the **SAP Central Picklist – v01 SCV3** version – the one with the word “BETA”, then click **Install**. Wait until finished. This may take about 3-5 minutes.



1. After installing the picklist, open now the SAP Logon. Select **Workspace View**. Double-click **Procter and Gamble** to refresh the list. You will then see the P&G picklist appearing in your SAP GUI. Advise the user now to try double-clicking his/her SAP system to check his/her access.

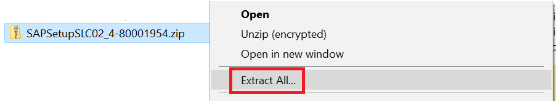


1. The user should then enter his/her SAP SLC credentials to be able to access his/her SAP systems.
   1. For Dedicated Personal Workstation Users:
      1. Username = shortname
      2. Passcode = intranet password and Ping ID
   2. For Shared Workstation Users:
      1. Username = shortname
      2. Passcode = intranet password only

# Setting Up SSO for Users of Non-PG-Issued Computers

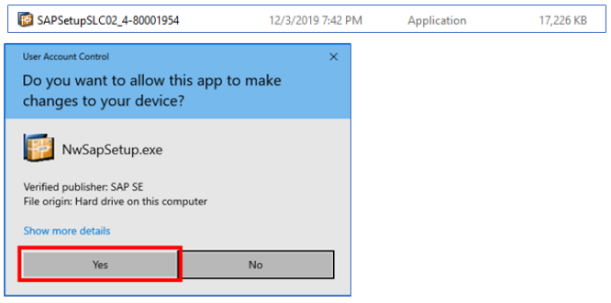
Please refer to these published KB Articles for reference – [KB0546118](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=15650270dba1c0d4dcc82ad94b961972) and [KB0546120](https://pgglobalenterprise.service-now.com/pgsp?id=pg_kb_article&sys_id=0468cca11bfbccd4fdac960abc4bcb56).

1. Download the SAP SLC installer and the SAP SLC root certificate file from the PG Knowledge Article. You will be asked to enter your P&G credentials in Service Now.
   1. [SAP SLC installer](https://pgglobalenterprise.service-now.com/sys_attachment.do?sys_id=3256c6f4dba1c0d4dcc82ad94b9619ea)
   2. [SAP SLC root certificate file](https://pgglobalenterprise.service-now.com/sys_attachment.do?sys_id=a3073641db21ccd48f8e22d4059619ec)
2. After downloading, unzip and extract both files.

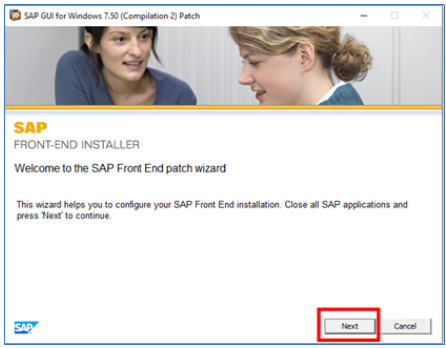


**Installing the SAP SLC Installer**

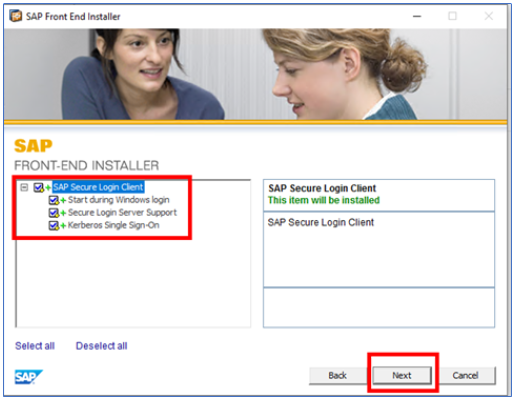
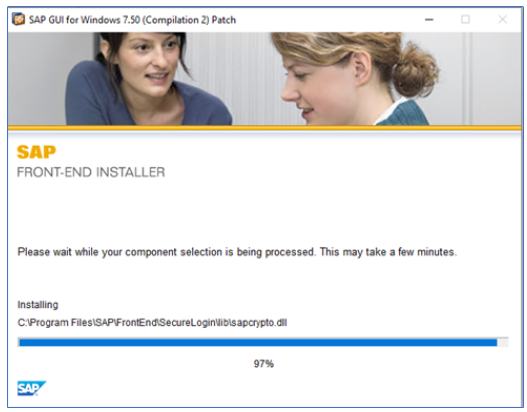
1. Double click the SAP SLC setup installer to run the program and wait for the popup to appear. Click the **Yes** button.



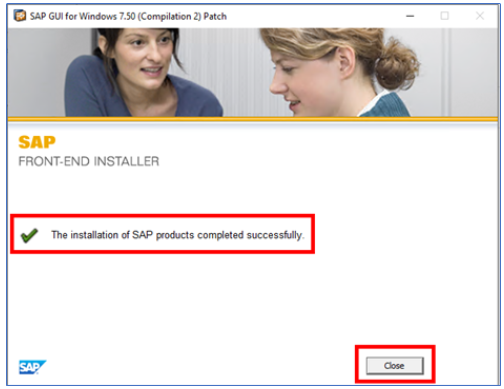
1. The installer will appear. Click the **Next** button.



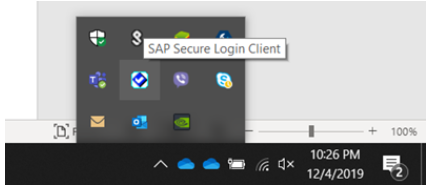
1. Select all that’s related to Secure Login Client. Click on **Next** then wait for the installation to be completed.

 🡺 

1. Click on **Close** button once the installation of SAP SLC is completed.



1. Verify if the SAP SLC has been installed by searching for SAP SLC application on the mini tray of windows in the lower leftmost corner of the screen.

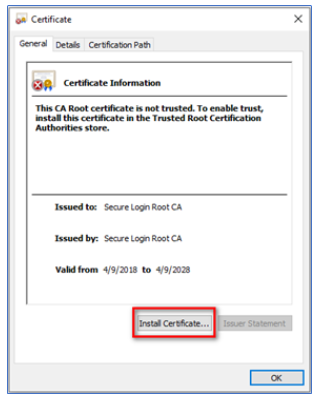
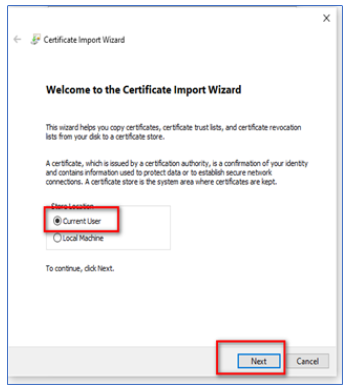


1. Next would be trusting the certificate (SLS root).

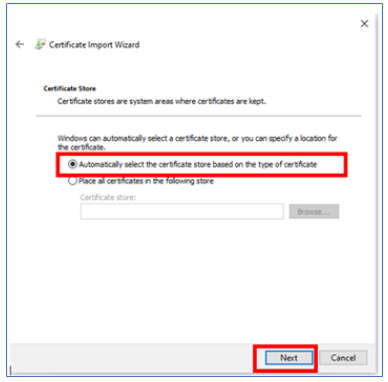
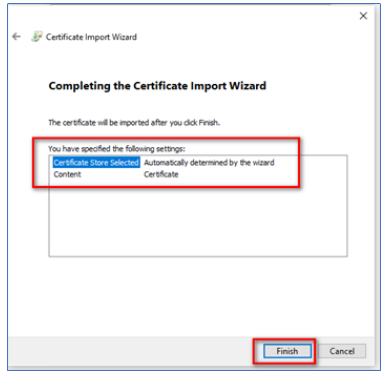
**Trusting the SLS Root Certificate**

1. Double click on the **SLS Root** certificate that you have downloaded and unzipped then click on the **Install Certificate** button. After that, select **Current User** then click the **Next** button.

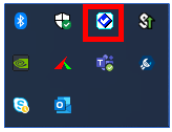
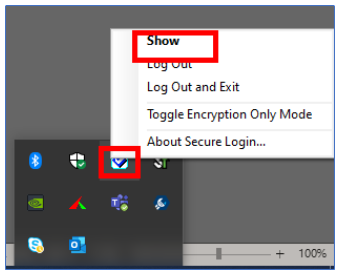


 🡺

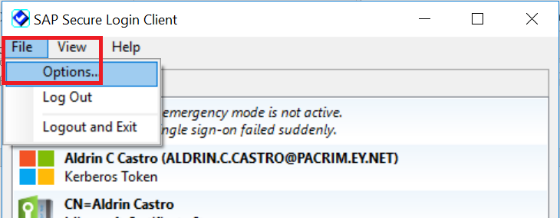
1. Select the first option then click **Next** then click **Finish**.

 🡺

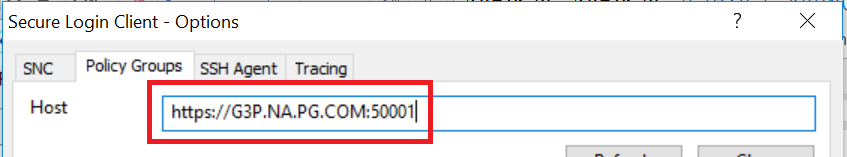
1. Open the SAP Secure Login Client in the tool bar. Right click on the icon and click “**Show**”.

 🡺 

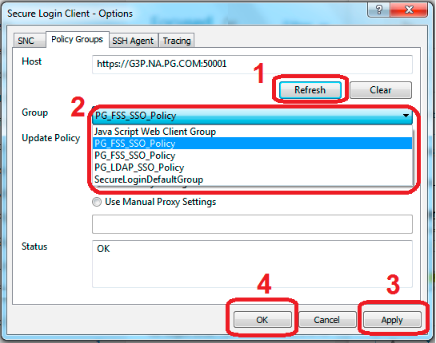
1. A popup will appear, and Secure Login Client will display. Go to **File** on top right corner then select “**Options…**”.



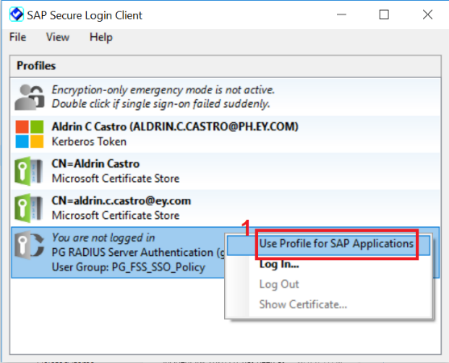
1. Go to **Policy Groups Tab** then input the following host details: [**https://g3p.na.pg.com:50001**](https://g3p.na.pg.com:50001).



1. Click **Refresh** button. The **Group** dropdown box will then become accessible. On the **Group** dropdown box, please select **PG\_FSS\_SSO\_Policy** then click **Apply** then **OK**.

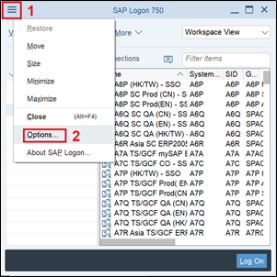


1. Right-click and click **Use Profile for SAP Applications**.



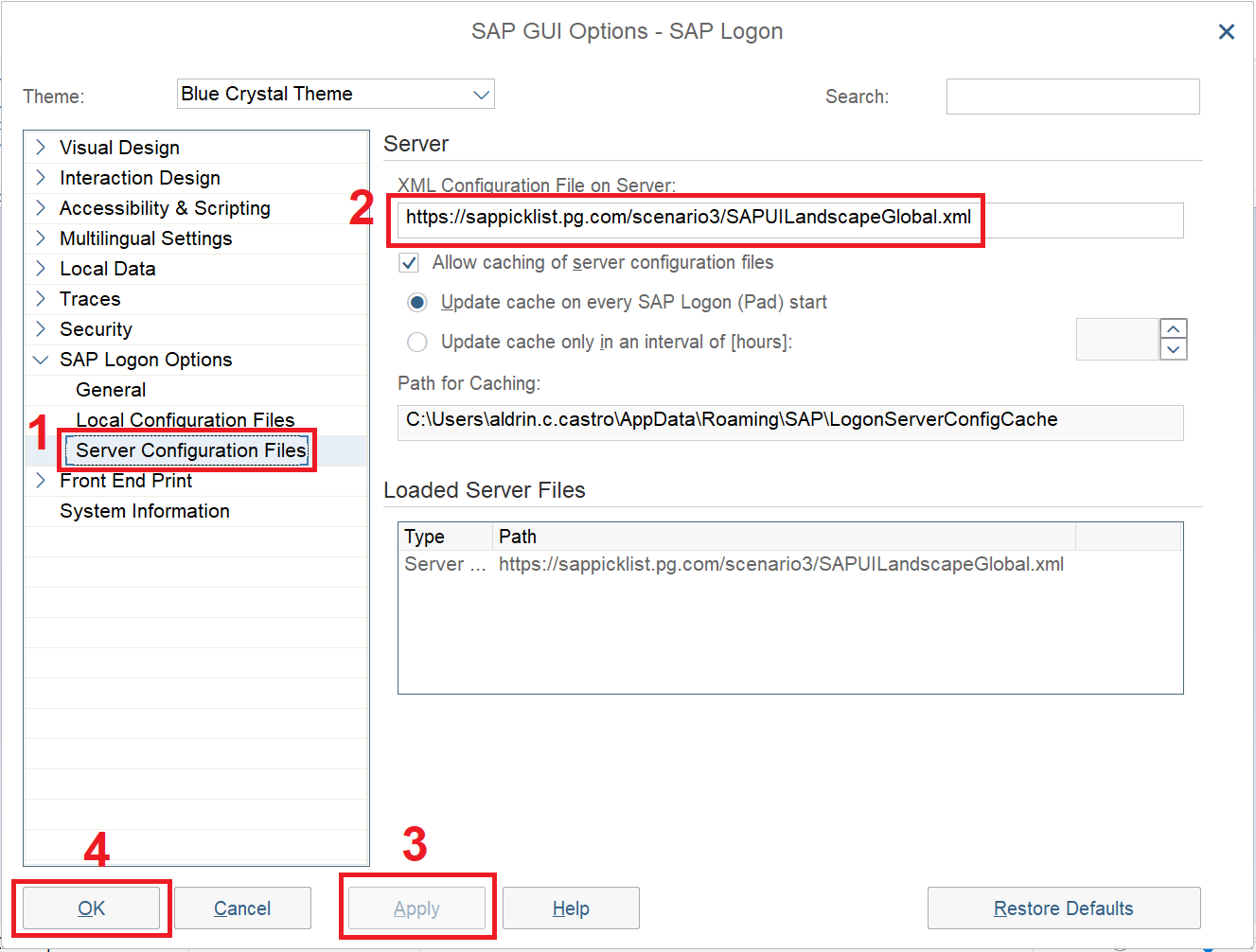
**Configuring the SAP GUI Central Picklist**

1. Click the icon beside the SAP Logon title, then click **Options**.



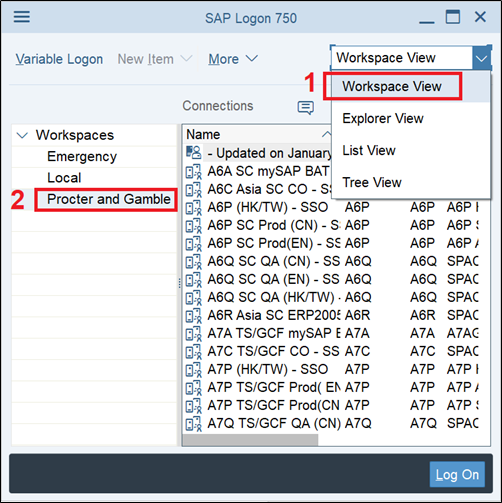
1. Click the **Server Configuration Files** button and then type this link in the **XML Configuration File on Server** textbox:

<https://sappicklist.pg.com/scenario3/SAPUILandscapeGlobal.xml>



Click **Apply** then **OK**. If it is not being accepted, try <http://sappicklist.pg.com/scenario1/SAPUILandscapeGlobal.xml> instead.

1. Close SAP Logon and then open it again to refresh the settings.
2. Select **Workspace View**. Double-click **Procter and Gamble** to refresh the list. You will then see the P&G picklist appearing in your SAP GUI.



1. Advised the user to double-click now his/her SAP system. The user should then enter his/her SAP SLC credentials to be able to access his/her SAP systems.
   1. For Dedicated Personal Workstation Users:
      1. Username = shortname
      2. Passcode = intranet password and Ping ID
   2. For Shared Workstation Users:
      1. Username = shortname
      2. Passcode = intranet password only