Phone: +372 699 9099
E-mail: support@prominion.eu

Last updated on:	21.06.2019
Responsible	Prominion

Taking SAP Contact Center End-User Applications into Use

Contents

1. Introduction

Each SAP Contact Center application has its specific requirements, see the following sections:

1.1. Communication Desktop (CDT)

Prerequisites

- Software prerequisites: Microsoft Windows 7 or 10 operating system and Internet Explorer 11.
- Make sure that there are no 3rd party Internet Explorer add-ons, such as Google toolbar, installed on the workstation. These 3rd party software can block CDT from opening, or affect the sound quality. If you are using Microsoft Skype, see Using CDT and Microsoft Skype Simultaneously.
- Configure the Internet Explorer security settings as defined, and see also settings affecting the UI appearance.
- Make sure that there are no 3rd party Internet Explorer add-ons, such as Google toolbar, nor other VoIP solutions, such as Skype, installed on the workstation. These 3rd party software can block CDT from opening, or affect the sound quality.

Procedure

- Install the terminal component on the client workstation. See the chapter Installation of Client Components.
- Configure Microsoft Internet Explorer software:
  - Add the SAP Contact Center website to the trusted sites.
  - Adjust the Internet Explorer security settings so that the system works but the maximum security is ensured, see the chapter Internet Explorer Configuration.
- Make sure that there are appropriate audio devices, and optionally a video camera installed on the client workstation.
  Note
  Make sure that the power saving setting of the operating system does not turn the USB device off when it is inactive (see the settings MyComputer > Properties > Hardware > Device Manager > Universal Serial Bus controllers > USB Root Hub-Properties > Power Management).
  If the settings are available in BIOS, make sure the USB legacy settings are enabled and the USB mouse and keyboard are supported.
- To start the CDT, browse to the address http://[customername].ipcallcenters.eu/, and enter username and password.

Using CDT and Microsoft Skype Simultaneously

Both CDT and Microsoft Skype use the same Human Interface Device (HID) addresses to control the USB audio device. If both are running simultaneously, Microsoft Skype may impair CDT audio stream.

System can be configured to reserve USB audio device specially for CDT. This scenario is supported only with Jabra and Sennheiser devices listed on Compatibility List.

Reserving USB Audio Device for CDT

To reserve the audio device specifically for CDT, install terminal_HS_USBHS.msi headset driver. By default, the reservation feature is turned on. If you wish to disable it registry needs to be modified.

For Jabra devices: (DWORD)

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SAP\CCTRAXPXY\HID_USE_JABRA_SPECIAL_COMMANDS

For Sennheiser devices: (from SP10 and upwards)
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SAP\CCTRAXPXY\HID_USE_SH_SPECIAL_COMMANDS

1.2. Online Monitoring

Prerequisites

- Microsoft Windows Vista, or Windows 7 or 10 operating system; Internet Explorer11.
- The Scalable Vector Graphics (SVG) plug-in is required for viewing certain reports of the Online Monitoring application.
  IE versions 9.0 and later include a SVG viewer, and no separate installation is required, but to enable the viewer, make sure that the monitoring site is not in the compatibility mode. Most cases can be corrected by choosing in *IE -> Tools -> Compatibility View* Settings, and remove the selection *Display Intranet Sites in Compatibility View*.
- Make sure that the *mctabuff* component is installed on the computer, see Installation of Client Components.
- See also the settings affecting the UI appearance.

Procedure

To start the Online Monitoring, browse to the http://[customername].ipcallcenters.eu/monitor or choose in CDT -> File -> Online Monitoring (if the link is enabled by administrator in System Configurator).

1.3. Reporting

Prerequisites

You must have appropriate role defined for your Windows user account.

Procedure

1. Start the Internet Explorer and browse the page http://[customername]rep.ipcallcenters.eu/
2. To open the set of reports, click the appropriate folder. The folder name is defined during installation. If several time zones are configured to the system, the folders of other zones can be found on this same site.
3. Language selection in SAP Contact Center does not effect Reporting but it follows the Internet Explorer (IE) language. To change the language, define it in IE -> Tools -> Internet Options -> Languages.
   Note the following exception:
   - If the chosen IE language is not supported by SAP Contact Center, English is used. The list of supported languages is available in Communications Desktop application's *Settings* view.
   - Language selection does not effect the Reporting Services -related items above the actual report, such as search parameters and the *View Report* button. They follow the language option used in the Microsoft SQL Server software. If the IE language is not supported by the SQL software, the installation language is used.
   - Only the reports are available in different languages; the items saved in the database and displayed in the reports, such as Outbound campaign comments, are available as they are entered in the database.

2. Installation of Client Components

2.1. Client Components

Client components are required for using Communication Desktop (CDT).

As of SAP Contact Center version SP07 (7.0.7.0) the client workstation components can be installed and updated automatically, if that is enabled on the server-side. The feature requires Internet Explorer version 8, or later.

If there is a need for a clean install, the following terminal components are available:

Terminal Component	Description	Note
`terminal_Proxy.msi`	The client end service that communicates with the CDT application.	Works as a proxy between the terminal core component and the user interface. CDT requires that terminal Proxy is installed. **Note** Install Proxy before other terminal components.
`terminal_Core_7.0.x.x.msi`	Actual terminal component	CDT requires that also terminal Proxy is installed **Note** If the auto-update is in use, do not install the MSI package.
`mctabuff.msi`	Installs a ClientCOM ActiveX component required for Online Monitoring and telephony integration with third parties.	Not included in the complete terminal package. Downloads automatically if that is allowed in IE settings.

2.2. Installing Client Components on One Workstation from MSI

Note

- Install MSI packages so that CDT or any other phone client component is not running while you do it, restarting the computer is not required. To see other options for the MSI package installation, run the .msi in the command line with the parameter /?.
- Install the terminal_Proxy.msi and terminal_Core.msi packages before installing the device adaptors.

Procedure

We recommend installing separate components

1. Double-click the terminal_Proxy.msi package.
2. Double-click the terminal_Core.msi package.

- If a handset is used, install the driver: double-click the desired one of handset driver packages.
- If the agent will use video calls, double-click the wvp.msi package to install the video component.
- If the agent uses Online Monitoring or needs link to the third party telephony applications, double-click the mctabuff.msi package.

2.3. Installing Client Components with Group Policies

With the following procedure you enforce that the package is installed on all workstations of the organizational unit when the client logs on:

Procedure

On the Active Directory server with the *Active Directory Users and Computers* tool:

1. Start -> Group Policy Object Editor -> Computer Configuration -> Software Installation.
2. Browse the installation directory and the folder for the MSI packages. The directory is created during installation process, make sure you are authenticated to access it.
3. Choose one MSI package from the list. You can deploy several packages at a time, but to select the right options for each package, we recommend deploying one package at a time.
4. Choose the *Deployment* tab and the following options:
    - *Deployment type*: Assigned.
    - *Install this application at logon:* Choose.
    - *Installation user interface options*: Basic.
5. Choose OK.
6. If the package you are installing has already been installed on the workstation with a group policy, select the Upgrades tab.
    - Select the option *Uninstall the existing package*, then install the upgrade package.
    - Choose OK.

3. Internet Explorer Configuration

Some SAP Contact Center applications require that the Microsoft Internet Explorer software is installed on the workstation, and its security settings are set accordingly.

Note
Make sure that there are no 3rd party Internet Explorer add-ons, such as Google toolbar, nor other VoIP solutions, such as Skype, installed on the workstation. These 3rd party software can block your SAP Contact Center application, or affect the sound quality.

Note
Delete Internet Explorer temporary files regularly, and always when upgrading the system, with Tools -> Internet options-> Delete. Accumulated temporary files may impair software functions, such as CDT Diagnostic View.

3.1. Configuring IE Security Settings with Group Policies

Define the settings with the *Group Policy Object Editor* software on the Active Director server.

Note

The following procedure is supported at least on the Internet Explorer 6.0. Configure the IE 7.0, 8.0, 9.0 and 10.0 settings individually on each workstation, or follow the basic principle of the procedure below.

Procedure

1. First create a *Trusted Sites Zone* template.

    1. Choose User Configuration -> Administrative templates -> Windows components -> Internet Explorer -> Internet Control Pane -> Security Page.

    2. Double-click the option *Trusted Site Zone Template*.

    3. Click the *Enable* button.

    4. Choose the security level *Medium*.

    5. Choose the option *Site to Zone Assignment List Properties*.

    6. Choose the *Enabled* option.

    7. Click the *Show* button. The dialog window appears.

8. Click the *Add* button and add the Website address or name to the *Value Name* list and *2* to the *Value* list. The value 2 defines that the site is a trusted site.

2. Then adjust the actual security settings:

1. Select the *Trusted Sites Zone* template you created above.

2. Change the settings that prevent the application from working, see the settings on the one workstation procedure.

3. After adjusting settings, remember to *Refresh* policies to deploy them to the selected organizational unit.

3.2. Configuring IE Security Settings on One Workstation

Set the following security settings in the Internet Explorer software.

Procedure

1. Choose Tools -> Internet Options -> Security -> Trusted sites.
2. Add the site to the trusted sites:
   1. Choose *Sites*.
   2. If HTTPS is not in use in the website, remove the selection from the *Require server verification (https:) for all sites in this zone* option before adding new sites to the list.
   3. Add to the list of trusted sites the address "**.ipcallcenters.eu*", and choose *OK (Close)* to return to the *Internet options* dialog window.
3. Define security settings:
   1. Choose again the Trusted sites option and *Custom level* to set the custom security settings.
   2. Reset the settings to the *Medium* level and then set the following individual settings as required for each IE version.
4. To view Reporting, allow *Access data sources across domains* in the security settings.

Note

Defining other settings may cause malfunction. For example, if the setting *ActiveX controls and plug-ins: Only allow approved domains to use ActiveX without prompt* is enabled, CDT may not start.

Internet Explorer 11

The following settings are the minimum changes required to the *Medium* level of the Internet Explorer security settings for the system to work properly:

- *ActiveX controls and plug-ins*
  - *Automatic prompting for ActiveX controls:* Enable.
  - *Initialize and script ActiveX controls not marked as safe for scripting:* Enable.
- *Miscellaneous*
  - *Allow script-initiated windows without size or position constrains:* Enable.
  - *Use SmartScreen Filter:* Disable.
  - *Use Pop-up Blocker:* Disable.
- *User Authentication*

  - *Choose Automatic logon with current user name and password.* This setting is required if the system servers and workstations are located in different domains.
- *In Tools > Internet options > Advanced > Security > Allow active content to run in files on My Computer: Enable.* This is required for browsing for a folder to save e-mail attachments and for viewing embedded images.

3.3. Appearance of User Interfaces in Internet Explorer

Settings in Microsoft Windows and Internet Explorer affect the appearance of IE applications such as CDT, Online Monitoring, and Reporting. If the UI does not appear as it should, for example, the screen is displayed only partially, or the menu bar is missing, check the following or corresponding settings:

- **Theme:** Control Panel -> Appearance and Personalization -> Personalization -> Theme: We recommend using the Windows Basic or Windows Classic theme.
- **Size of text:** Control Panel -> Appearance and Personalization -> Display: *Size of text* Use the default settings (the option *Smaller*), or in *Set custom text size (DPI)* use 100 % of the normal size, that refers to 96 DPI.
- **IE text size:** Choose Tools -> Zoom and 100%. Alternatively, to adjust the text size, place the cursor on the application UI, press CTRL and scroll with the mouse scroll button, or press CTRL and plus (+) or minus (-) keys.
- **Tabbed browsing:** If you use tabbed browsing, choose in Tools-> Internet Options -> Tabs -> Settings either the option *Always open pop-ups in a new window* or *Let Internet Explorer decide how pop-ups should open*. Do NOT use the option *Always open pop-ups in a new tab*.

3.4. Virus Scanning and Malware Protection Programs

Some virus scanning or malware protecting programs, such as Microsoft Security Essentials (MSSE) or Microsoft Forefront endpoint protection, may impair CDT functions by reserving too much CPU capacity. The following work-arounds have been found to be useful:

- Exclude from scanning:
  - c:\users*\appdata\local\temp\ContactCenter*.log files
  - iexplore.exe
- Optionally exclude from scanning c:\users*\appdata\local\temp\mct*.txt.

4. Installing Audio Devices

Note

Make sure that the power saving setting of the operating system does not turn the USB device off when it is inactive (see the settings MyComputer > Properties > Hardware > Device Manager > Universal Serial Bus controllers > USB Root Hub-Properties > Power Management).

Audio Devices

Typically clients make phone calls with USB sound devices.

The sound device, such as a headset, should be set automatically for the default audio device but if problems occur, check the following settings:

In the workstation operating system:

1. Choose Start -> Control Panel -> Sounds and Audio Devices -> Audio.

2. Choose the USB device option for both *Sound playback* and *Sound recording*.

In the CDT application:

1. Choose Tools -> Settings -> Phone -> Audio
2. Choose the USB device option for the *Audio* and *Ringing tone* options from the drop-down menu.

5. Log Files Saved on Client Workstations

Following log files are saved on the client workstation in the current temporary *%temp%* path and registered in the UTC time. You can view the files with a text editor.

All Contact Center workstation log files starts with "ContactCenter_" and end date value "*YYYYMMDD.log".*

By default, the log level is None (0), no log is written. If another log level is used, the log files are written for each day. Writing logs slightly increases the client workstation CPU load, thus we recommend using low levels in normal use, and reserving 4 and 5 to error situations only. The following levels are available:

- 0 -> None: No log file is created, the default value.
- 1 -> Low: Log file is created with the following data
  - CDT start and close information.
  - Terminal commands received from user interface.
- 2 -> Medium: Log file is created with the following data in addition to the lower level
  - Terminal events received from CEM and sent to user interface.
- 3 -> High: Log file is created with the following data in addition to the lower level
  - Terminal events that reached user interface.
- 4 -> Tracing: Log file is created with the following data in addition to the lower level
  - Opening, closing, and messages passed in audio device, RTP, and secure channels.
- 5 -> Debugging: Log file is created with the all information available

Changing Log Level

The log level can be changed in the System Configurator for the entire system in General Settings -> Log Level, or at the each client workstation in the following way:

1. In the CDT, choose Tools -> Settings.
2. Double-click the lower left corner of the dialog window.
3. Choose the level from the drop-down menu. The log level is applied immediately.

Setting Log Level with URL Parameter

You can also start CDT so that the URL includes a startup parameter that sets the log level. With this method, you can set logging on right from the CDT start. For example, http://1.2.3.4:1080/cdt?arg=loglevel=5.