Last updated on:	21.06.2019
Responsible	Prominion

Internet Explorer Settings

Contents

1. Introduction

To use Communication Desktop, the following security settings in IE must be set correctly.

2. Instructions

Administrators configure these settings so you may not need to configure them yourself. However, in case you have problems opening CDT, it is advisable to check that the necessary IE settings have been configured correctly.

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:

Required Internet Explorer Settings

Version	Settings
Internet Explorer 11	• **ActiveX controls and plug-ins** ○ **Automatic prompting for ActiveX controls**: Enable. ○ **Initialize and script ActiveX controls not marked as safe for scripting**: Enable. • **Miscellaneous** ○ **Access data sources across domains**: Enable. This is required if SAP Cloud for Customer client side integration is used. ○ **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.