

Administrators Guide

telisca Single Sign-On



Version: 3.1.0

SUPPORT@TELISCA.COM
TEL. +331 46 45 05 12

HELP

Open a ticket with your logs on <http://support.telisca.com> for a prompt and efficient response!

Server: MENU>Support>Zip Logs

Summary

1	PRESENTATION PRODUCT	4
1.1	OVERVIEW	4
1.2	USER SELECTION.....	4
1.3	PHONE SELECTION.....	4
1.3.1	<i>Automatic</i>	4
1.3.2	<i>Manual</i>	5
1.3.3	<i>Predefined (PC mapped to Phone)</i>	5
1.4	USER PROFILES.....	5
1.5	ADDITIONAL FEATURES.....	5
1.5.1	<i>Accidental login</i>	5
2	PRE-REQUISITES, INSTALLATION.....	7
2.1	ARCHITECTURE.....	7
2.2	TSSO SERVER-SIDE FEATURES	7
2.3	CUCM REQUIREMENTS.....	8
2.4	PC REQUIREMENT	8
2.5	LAN DATA FLOW.....	9
2.6	SERVER REQUIREMENT	9
3	ADMINISTRATION	10
3.1	ADMINISTRATION INSTALLATION	10
3.2	GLOBAL PARAMETERS	10
3.2.2	<i>Automatic phone detection settings</i>	11
3.2.3	<i>Trace settings</i>	11
3.2.4	<i>TSSO configuration password</i>	12
3.2.5	<i>Server side features settings</i>	12
3.2.6	<i>PC id to link PC and IP Phone</i>	13
3.3	PROFILE	13
3.3.1	<i>Common settings</i>	15
3.3.2	<i>Auto login modes</i>	17
3.3.3	<i>Auto logout modes</i>	21
3.3.4	<i>Treatments after login</i>	24
4	CUCM CONFIG	25
4.2	LDAP CONFIGURATION	28
4.3	HELP TEXTS.....	29
4.4	ASSOCIATION PC-PHONE	30
4.5	MONITORING	31
5	DEPLOYMENT	32
5.1	CLIENT INSTALL TAB	32
5.1.1	<i>Installation file: TSSOClient.msi</i>	32
5.1.2	<i>Configuration file: TSSO_cfg.txt</i>	34
5.2	TSSO CLIENT COMMAND LINE PARAMETERS	35
5.2.1	<i>Remote config file</i>	35
5.2.2	<i>-autologin</i>	35
5.2.3	<i>-hide</i>	35

5.2.4	<i>Profile name -pProfileName</i>	35
5.3	UPDATE PROFILE USED	36
5.4	USER CONFIGURATION FILE: USERCONFIG.XML	36
5.5	LOG FILES FOR SUPPORT AND DEBUG	37
5.5.1	<i>Server side logs</i>	37
5.5.2	<i>Client side logs</i>	37
6	TSSO USER INTERFACE	39
6.1	OPENING TSSO	39
6.2	ENTERING THE CUCM USERID	39
6.3	PHONE SELECTION.....	39
6.3.1	<i>Automatic IP Phone detection</i>	39
6.3.2	<i>IP Phone detection by directory number</i>	40
6.3.3	<i>Fixed mode: PC/Phone association</i>	41
6.4	LOGIN PROCESS.....	41
6.5	THE IP PHONE IS ALREADY LOGGED	41
6.6	EXITING FROM TSSO.....	42
6.7	TSSO USER SETTINGS.....	42
6.8	USER PROFILE CONFIGURATION.....	43
6.8.1	<i>Selecting a profile to use</i>	43
6.8.2	<i>Creating a new PC/Phone association</i>	44
7	APPENDIX	45
7.1	MULTIPLE LOGIN BEHAVIOR	45
7.2	SETTING USER PROFILE FROM REGISTRY	46

1 Presentation Product

1.1 Overview

Telisca SSO (TSSO) is a Single Sign-On application for Cisco Extension Mobility.

When opening a Windows session, TSSO logs your CUCM profile on your Phone without requiring you to enter a PIN code. Depending on your configuration, the process can be made completely invisible to the user.

TSSO may also log your profile out when closing the session, either on demand or at a defined time of day.

Several automatic User and Phone detection modes can be configured:

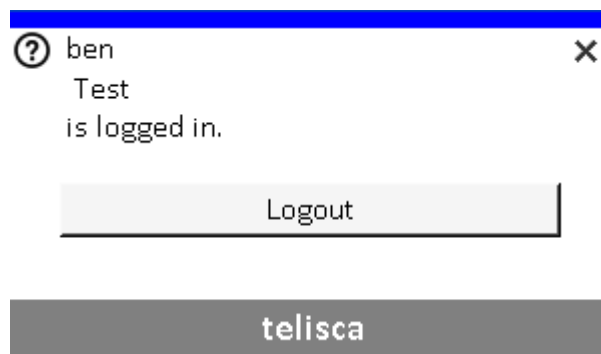
- use the Windows login as the CUCM UserID
- search it in a LDAP or Active Directory
- ask the user to enter it once.
- If the computer is connected to the LAN through the IP Phone, TSSO can automatically detect it.
- the user can also enter the logged-out IP phone directory Number.
- the user will be able to log into the last IP Phone used
- a correspondence table between PC and IP Phones can be used too.

When login or logout is completed, TSSO can launch an application such as a Call Center agent's banner or Lync.

1.2 User selection

TSSO can use the Windows login as CUCM userID if CUCM is synchronized on the Active Directory.

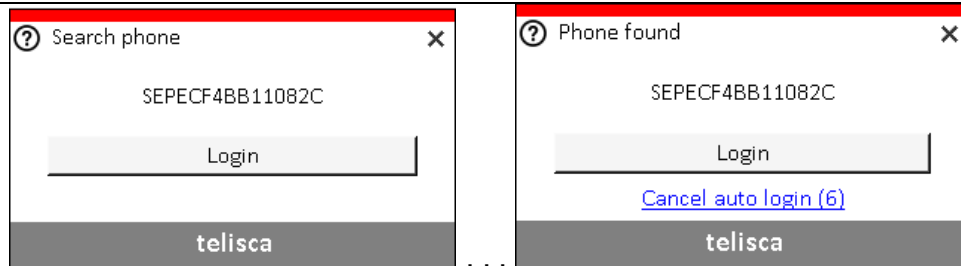
TSSO can also search the CUCM userID in LDAP or Active Directory using the Windows login as a search criteria. Finally, the user may enter his CUCM's userID the first time.



1.3 Phone selection

1.3.1 Automatic

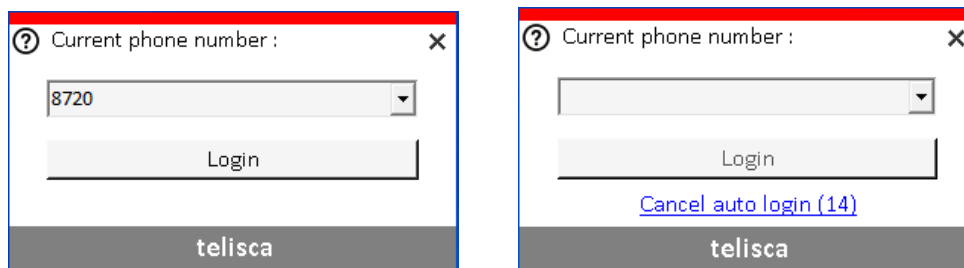
If the computer is connected to the LAN through the IP Phone, TSSO can automatically detect the IP Phone's name. This is done by capturing CDP broadcast from the IP Phone. The average time to detect the IP Phone is 30 seconds.



1.3.2 Manual

If the PC is not connected to the IP Phone switch or when running TSSO on a virtual PC environment, the user may enter the IP Phone's directory number displayed on the Phone (which is usually logged out).

Next time the user opens a Windows session, he will be able to log in directly on the last IP Phone used. TSSO keeps track of the last seven phones used.



1.3.3 Predefined (PC mapped to Phone)

This feature requires the use of the telisca server. The PC to Phone association can be defined on the server or locally on the client by the administrator. When TSSO starts, it sends the Mac Address or Hostname of the local PC to the server, which replies with the associated phone's mac address.

1.4 User profiles

It is possible to create different configuration profiles with different settings: phone selection modes and other parameters. TSSO can then be launched with a particular profile as a parameter or changed via the client with an administrator password.

1.5 Additional features

1.5.1 Accidental login

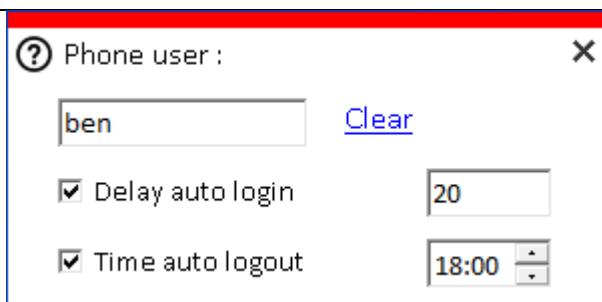
When trying to log on a phone that is already logged in, TSSO will prompt the user on the PC. If the current user is already logged in when the Windows session is opened, TSSO displays, "already logged in".

Also, if using the telisca server, it is possible to add a prompt screen on the phone that is about to be used. TSSO will wait for a validation "Allow? Yes/No" coming from the device before logging in.

If a user has multiple device profiles, TSSO will select the one most appropriate to the IP Phone detected (same model series, or number of buttons).

The user can optionally set a delay to log in automatically on the last previously logged IP Phone.

It is possible to give the user the ability to configure an automatic logout time. TSSO then calculates the appropriate login duration left and redefines it in Extension Mobility.



Phone user :

ben [Clear](#)

Delay auto login 20

Time auto logout 18:00

TSSO is able to monitor when the IP Phone is actually logged in and launch an executable (for instance a Call Center agent's banner). This is useful since the time of login on the IP phone may be variable and some application will fail if the login is not completed.

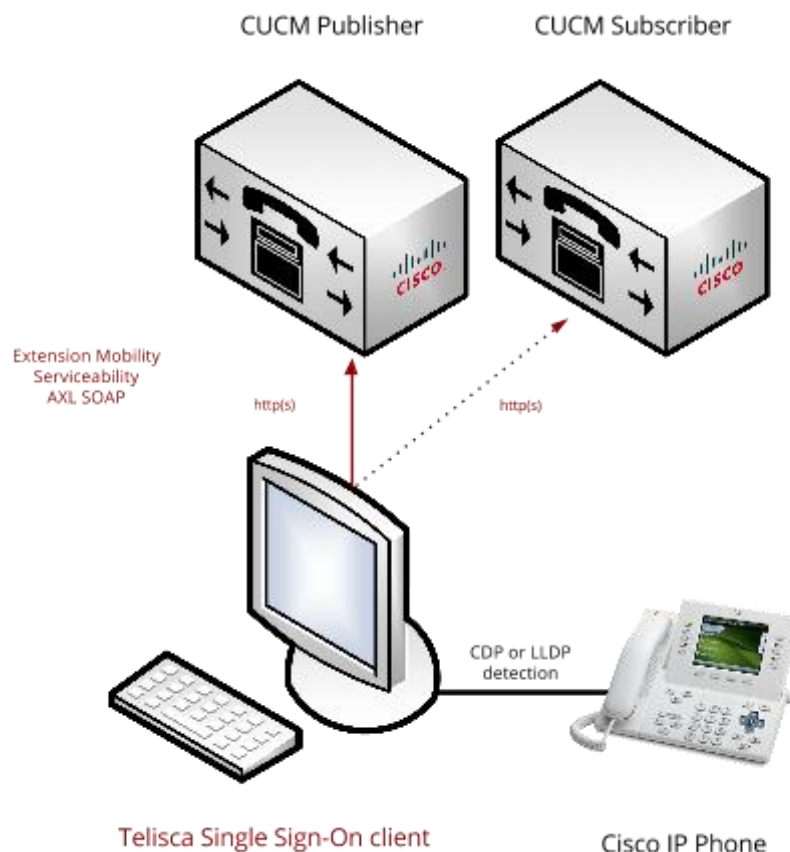
When closing the Windows session or during system shutdown, TSSO is closed which initiates an immediate logout, asynchronously. On crash, power failure, locked session, or hibernation of the computer, however, the application is not closed normally and therefore the IP Phone is not logged out

2 Pre-requisites, installation

2.1 Architecture

TSSO is an application that runs on the PC or on a Citrix virtual machine. It can be deployed on the PC by simply copying it or running it from the network if the IP Phone detection option is not enabled.

TSSO takes advantage of CUCM Extension Mobility API and uses an authentication proxy user for Extension Mobility.



Since CUCM 6.1, the performance of login/logout has increased and it is possible to execute a login/logout even if the CUCM Publisher is stopped. Also TSSO can be configured to support a primary and backup CUCM server. The number of logins/logouts per minute is directly related to the size of the cluster (without loss of performance due to the use of the API). TSSO can also operate in load balancing mode with multiple CUCM servers.

To automatically detect the IP Phone on which the PC is connected, TSSO relies on the "pcap" library to access the network layer and retrieves the name of the IP Phone to which the PC is connected.

If the name of the IP Phone is granted by entering the telephone number of the IP Phone, the TSSO relies on CUCM "AXL" API.

2.2 TSSO Server-side features

The web server component of TSSO can be used to generate the configuration file for the clients only and then disconnected. However, having the telisca server permanently running provides additional capabilities.

- Checking login status by CTI
- Fixed PC/Phone association
- Statistics of phones association
- Confirmation of logout on phone

2.3 CUCM Requirements

TSSO is supported on CUCM 10.5, 11, 11.5, 12, 12.5, 14.

Extension Mobility service must be activated on CUCM.

Extension Mobility Service Parameter advanced setting "Validate IP Address" should be set to "false," which is the default value.

For some optional features, AXL SOAP Service must be activated on CUCM.

If the option to confirm other users' logout on IP Phone is set, CTI Manager Service must be activated on CUCM.

If IP Phone automatic detection mode is used, the CDP or LLDP protocol should be enabled on the PC Port.

2.4 PC requirement

TSSO is compatible with:

- Windows 8
- Windows 10
- Windows 11

It requires .Net Framework to be installed. Any of the following versions is supported: 2.0, 3.0, 3.5, 4.0, 4.5, 4.6 & 4.7.

TSSO can run on a TSE or Citrix virtual terminal.

It can be installed by

- MSI silent installation (rezone auto-detection)
- executable files copied locally
- launched from a LAN drive or URL (if permitted by the PC security settings)

TSSO communicates with CUCM via https.

If using automatic phone detection, security software (firewall or antivirus) must allow incoming CDP/LLDP packets.

2.5 LAN data flow

TSSO connects directly to the CUCM cluster, Extension Mobility, and AXL SOAP.

If the optional module to push a logout of another user on the IP Phone is installed, then TSSO communicates with the IPS Framework server, which pushes to the IP Phone by JTAPI (that uses SCCP).

Source	Destination	Protocol	IP port
TSSO	CUCM Publisher or Subscriber	Extension mobility Web Service	8080
TSSO	CUCM Publisher or Subscriber	AXL SOAP	8443
TSSO	IPS Framework (optional)	http Get	80
IPS Framework (optional)	IP Phone	Push via SCCP	2000
IP Phone	IPS Framework (optional)	http Get	80

2.6 Server requirement

For standard configuration, no server is required to run TSSO.

A **server** may be required for specific features:

- when the phone detection is based on the directory number entered by the user, it is possible to ask to confirm from the IP Phone itself, before login out the previous user,
- to define fixed PC to Phone association,
- to wait for CTI event after login, to launch external application,
- to provide usage reports.

Windows servers supported:

- Windows Server 2012 R2 Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

Minimum configuration: 1 vCPU, 4GB RAM, 70GB disk

Virtual Machine VMware vSphere, Hyper-V or Cisco UCS, Cisco UCS-E
Cloud ready

3 Administration

3.1 Administration installation

TSSO client configuration file is created from a web-based administration. You may install the administration on a server with Microsoft IIS.

The purpose of the administration is to provide a client SETUP package which will include the required MSI and an encrypted setup file which will be deployed to the PC or downloaded from a defined URL.

The SETUP will ask for the license file TSSO_lic.xml. Telisca can provide you an evaluation license. Contact us on <http://www.telisca.com/contact>.

The administration is installed in IIS default directory (c:\inetpub\wwwroot). Two virtual directories are created: /IPSCFG and /TSSO.

To open the administration, launch the following URL from your browser:

[http://\[COMPUTER_RUNNING_THE_ADMINISTRATION\]/](http://[COMPUTER_RUNNING_THE_ADMINISTRATION]/)

or via the full URL: <http://xxx.xxx.xxx.xxx/IPSCFG/admin> (https supported)

A login/password may be requested. You should enter a Windows login which is part of the "Administrators" or "teliscaAdmin" group on the local server or Network domain.

3.2 Global parameters

In this first tab, you can configure the main settings of TSSO.

The screenshot shows the 'Global parameters' configuration page in the Telisca administration interface. The page is titled 'Home / TSSO / Global parameters'. The configuration fields are as follows:

- URL to download TSSO config:
- IP Phone detection protocol:
- IP Phone name prefix:
- Trace level:
- Logs files retention (days):
- TSSO configuration password:
- TSSO configuration file encryption >= v2.4:
- Enable TSSO server:
- Mode Extension Mobility Cross Cluster:
- telisca IPS Framework host / CTI Server:
- Backup server host:
- Connect to CTI Server using SSL:
- CTI Server port:
- CTI server timeout (s):
- CTI Server network connection timeout (s):
- Delay of logout Popup on IP Phone(s):
- Maximum login wait by CTI delay (s):
- Keep alive delay (s):
- Additional delay after logout before login (s):
- PC id to link PC and IP Phone:

At the bottom of the page, it indicates 'CUCM Version 12' and 'TSSO AXL Version 12'.

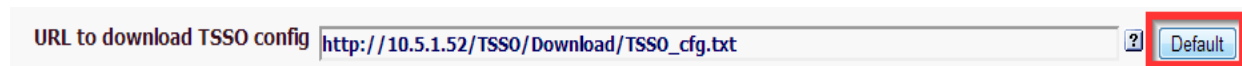
The TSSO Global Parameters tab in administration
**EMCC mode only present if you have the correct TSSO license*

3.2.1.1 URL to download TSSO configuration

Enables TSSO configuration to be updated on clients after TSSO is deployed. The file is downloaded from the URL two seconds after TSSO starts, then **every 4 hours**.

The default URL is the default path on the web server where telisca administration is running:

`http://TELISCA-SERVER/TSSO/Download/TSSO_cfg.txt`



Related information: [launching TSSO with a remote configuration file](#)

3.2.2 Automatic phone detection settings

3.2.2.1 IP Phone detection protocol

Which types of packets will be monitored by TSSO for automatic detection of the connected phone. (Default: CDP)

Note: *Cisco Discovery Protocol (CDP): PC Port and Link Layer Discovery Protocol (LLDP): PC Port should be enabled on the IP Phone.*

Note: *If this mode of detection is selected, you should not activate the Span Port option of the IP Phone. Indeed, in this case, you would receive the CDP and LLDP of the other IP Phones on the same VLAN network.*

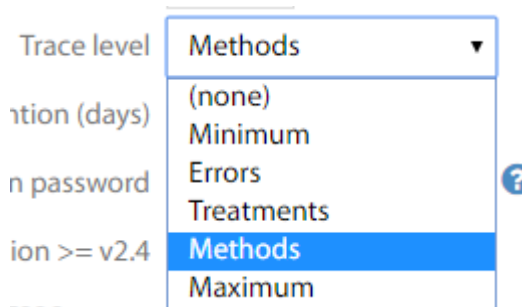
Important Note: *If using automatic detection, the firewall and antivirus software must be configured to allow incoming CDP/LLDP network packets.*

3.2.2.2 IP Phone name prefix

Allows TSSO to ignore CDP/LLDP network packets not coming from phones when using automatic detection of the phone. (Default: SEP)

3.2.3 Trace settings

3.2.3.1 Trace level



Select the level of details in the client's generated log files.
 Default for production is Methods for troubleshooting use Maximum.
 TSSO creates the log files TSSO_yymdd.log (**one file per day**).
 See: [How to access the logs files](#)

3.2.3.2 Logs files retention (days)

The log files (on the client machines) will be deleted after this number of days. (Default: 15 days)

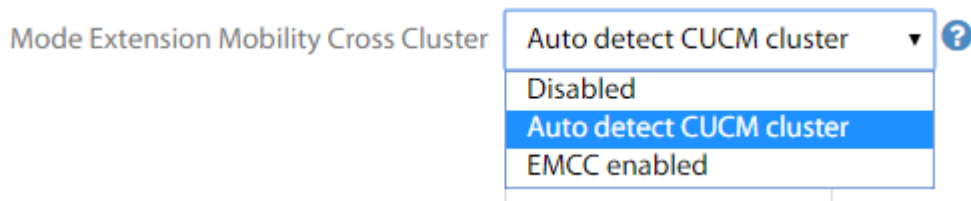
3.2.4 TSSO configuration password

Secret administrator password to change settings and access info on local TSSO clients. See [TSSO Client Admin Access](#)

3.2.5 Server side features settings

These settings are only needed if using [server side features](#) of TSSO.

3.2.5.1 Mode Extension Mobility Cross Cluster



In a multi CUCM cluster environment, it is possible to detect automatically the user's home cluster and the IP phone's cluster. This is useful when using the same configuration file for different clusters, for instance on Citrix or VMare Horizon environment.

"Auto detect CUCM cluster" on this option, TSSO will determine which cluster the user belongs to and log then into their correct cluster.

"EMCC enabled" with this option, the TSSO client will login/logout the user into any cluster, so either the visiting or home cluster, will depend on their location.

3.2.5.2 telisca_IPS Framework host / CTI Server

By default the current telisca server, enter the address (IP or DNS) here.

3.2.5.3 TSSO backup server host

When using telisca servers in Fault Tolerance, you can specify the address of the backup telisca server here. When TSSO cannot reach the primary telisca server, it will try on the backup one.

3.2.5.4 Connect to CTIS server using SSL

Encrypts the http communication between the TSSO clients and the telisca server(s).

3.2.5.5 CTI Server Port

Telisca CTI server port: allows you to change the port used by the telisca servers. The port number will automatically change depending on if SSL is selected or not. (Defaults: http: 8081 , https (ssl): 8444)

3.2.5.6 CTI server timeout

TSSO server timeout during communication between the TSSO client and the server. This parameter defines the maximum waiting time for a response from the primary server before the client tries to connect to the standby server (and vice-versa). (Default: 3 seconds)

3.2.5.7 CTI Server network connection timeout (s)

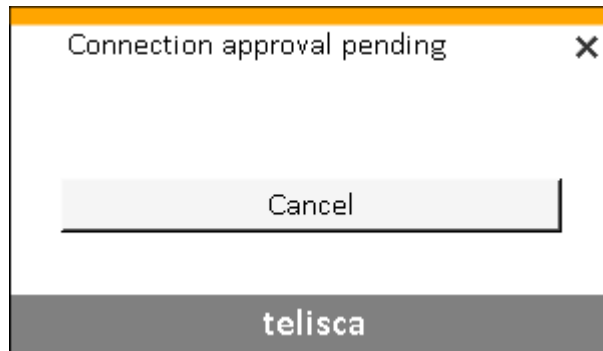
When using the CTI server, this parameter defines the maximum connection time with the CTI server. (Default: 3 seconds)

3.2.5.8 Delay of logout Popup on IP Phone (s)

If the option to [prompt the user on the IP Phone](#) is used, this option allows you to define how long to keep the message displayed before closing. (Default: 60 seconds)

If the message closes automatically on the phone TSSO will consider this as a negative response and won't allow the user to log in on the device.

0 will leave the popup opened on the phone until a user selects Yes or No.



3.2.5.9 Maximum login wait delay (s)

How long TSSO will wait for a response from CUCM to confirm the logon command was successful.

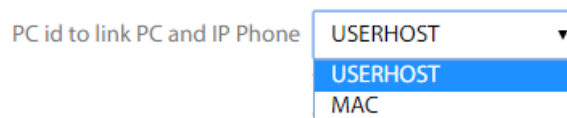
3.2.5.10 Additional delay after logout before login

TSSO waits (10 seconds by default) for the phone to be effectively logged out before launching the login process. This allow for CUCM to send the logout command and for the phone to restart before the new login.

3.2.6 PC id to link PC and IP Phone

If using pre-defined mapping of computers and phones. Allows you to define the identifier of the computer:

- USERHOST: computer name
- MAC: mac address of the computer



TSSO will use this information from the computer to find the associated IP Phone

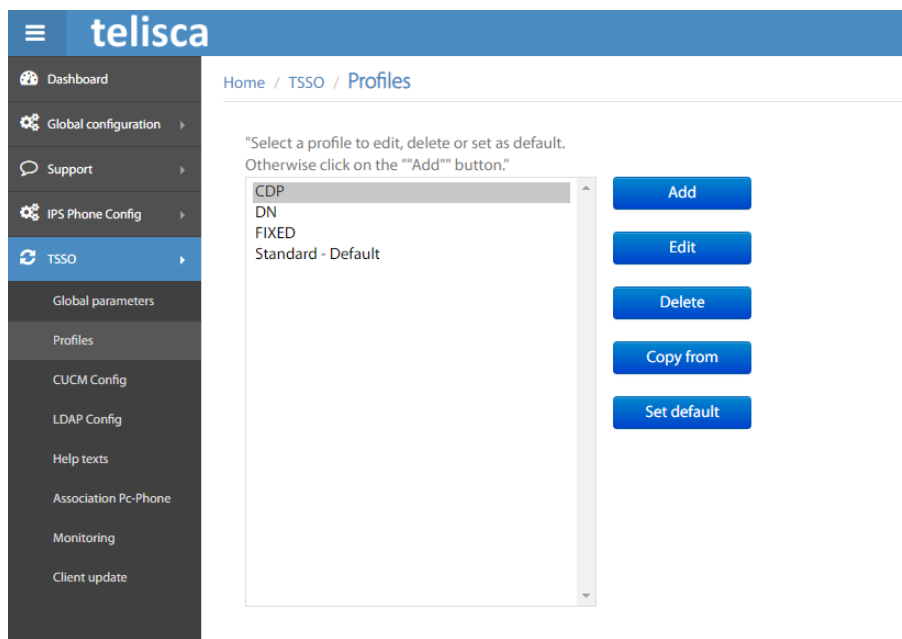
3.3 Profile

In this tab, the administrator can create different profiles for different users.

Users can be assigned a profile in 3 ways:

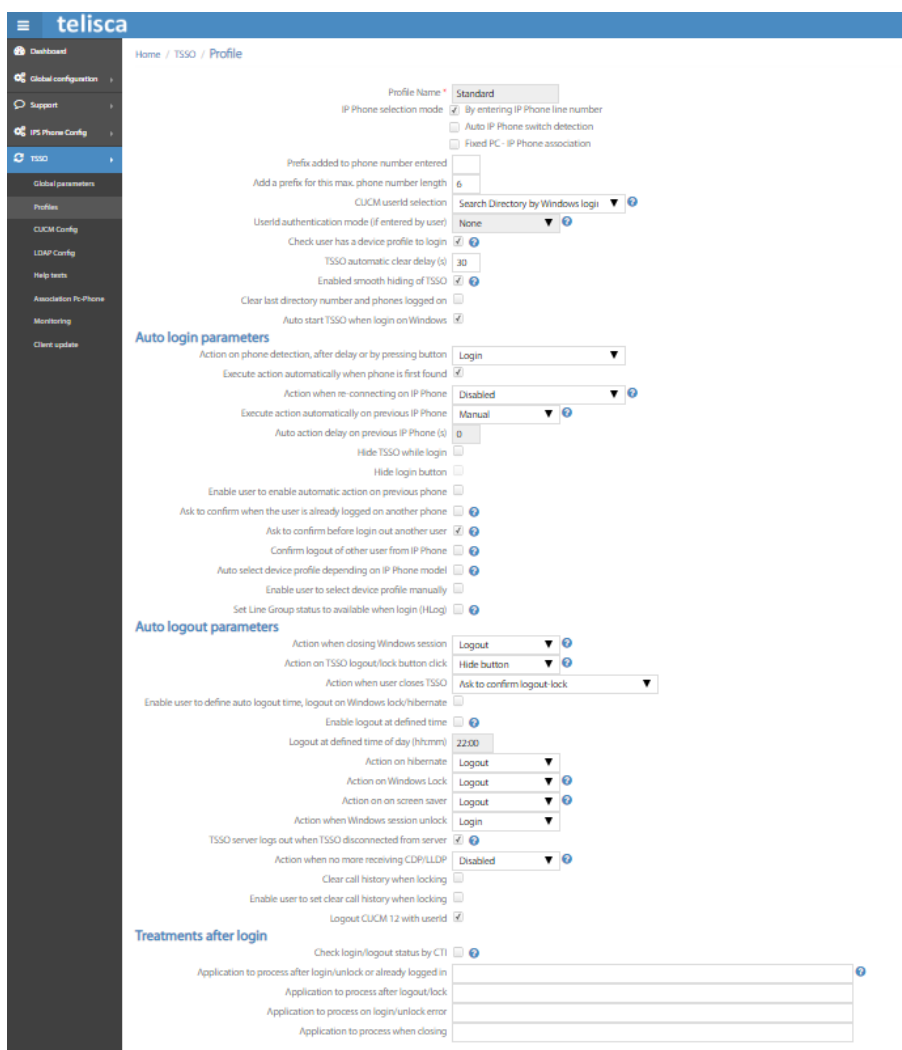
1. [Launching the client app with a parameter](#)
2. [Select the desired profile in the client app interface](#)
3. [Use a registry key](#)

There must be at least one profile defined which will be used as the default by TSSO.



Create, modify, copy, delete, change the default profiles here

Select a profile and click Edit:



The TSSO user profile definition screen

[See here](#) for how to use a specific profile on TSSO client.

3.3.1 Common settings

3.3.1.1 Profile Name

Name for the configuration profile (examples: static users, hot desk users...)

3.3.1.2 IP phone selection

Check one or several modes for selecting the IP Phone to use.

3.3.1.3 By entering IP phone line number

Will prompt the user to enter the DN seen on the phone screen.

3.3.1.4 Auto IP Phone switch detection

TSSO will use the computer's network card to detect the phone connected to it. This requires the use of [INSTALLPCAP parameter](#) during installation.

3.3.1.5 Fixed PC- IP phone association

TSSO will do a lookup in [an association table](#) to find the IP Phone matching the local [computer identifier](#). This is useful in virtualized environment if you don't want the users to have to manually select the phone to use (by typing the DN).

3.3.1.6 Prefix added to phone number entered

When using "By entering IP phone line number" this setting will add a prefix to the number typed in by the user. Useful when users are used to use short numbers rather than full extensions.

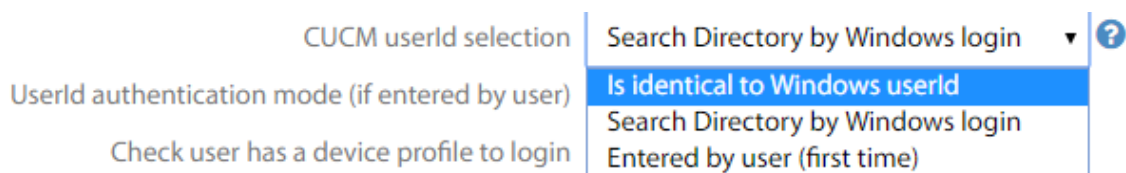
3.3.1.7 Add a prefix for this max. Phone number length

How many digits of the directory number entered by the users are going to be added after the prefix. e.g. if users types 01213 036 677 and the maximum allowed number is 4, and the prefix is 123 the result will be 123 6 677.

3.3.1.8 CUCM userID selection

These settings define how TSSO is going to identify the user to log onto a phone. Three options are possible depending on CUCM/AD are synchronised, if an external database contains a correspondence between Windows usernames and CUCM Users or if the user has to enter his name manually.

3.3.1.9 is Identical to Windows userId



If the CUCM userID is synchronized with the Windows login, TSSO can use the Windows session's login for Cisco Extension Mobility. It should be noted that TSSO uses an authentication proxy and it is thus not necessary to know the user's PIN code.

3.3.1.10 Search Directory by Windows login

CUCM userID selection Search Directory by Windows login ?

UserID authentication mode (if entered by user) Is identical to Windows userID

Check user has a device profile to login Search Directory by Windows login

Entered by user (first time)

If the CUCM userID is different from the Windows login, TSSO can use the Windows session's login to carry out a request on a LDAP directory or Active Directory to get the corresponding CUCM userID. The Administrator will have in this case to fill the parameters of the "[LDAP Configuration screen](#)."

3.3.1.11 Entered by user (first time)

CUCM userID selection Entered by user (first time) ?

UserID authentication mode (if entered by user) None ?

Check user has a device profile to login None

TSSO automatic clear delay (s) PIN code

Enabled smooth hiding of TSSO Password

PIN code or Password

Lastly, it is possible to ask the user to enter the CUCM userID when using the software for the first time. This userID is saved in the user settings in the user's personal directory (AppData).

User config with "Entered by User" and no authentication

Note: the authentication on CUCM is not case sensitive, whatever the username source typed/retrieved/Windows, it will match the CUCM User ID in any case.

3.3.1.12 UserID authentication mode (if entered by user)

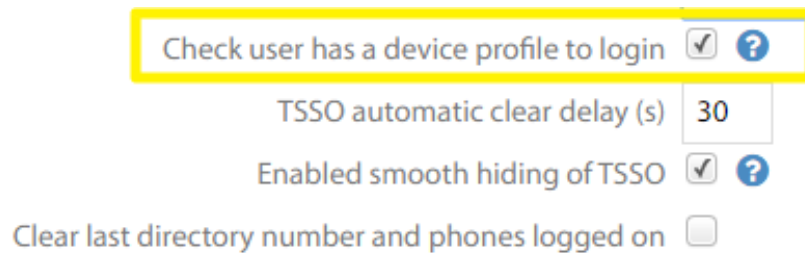
When using the username typed by users, we can prevent impersonation by asking the user to authenticate themselves by entering once their CUCM PIN, Password or both. The authentication is saved into the user configuration file and is not needed afterwards even when CUCM credentials change.

3.3.1.13 Check user has a device profile to login

If enabled TSSO will search for a device profile for this user before initiating a login command:

- If the user doesn't have a device profile: TSSO will not initiate a login process and assume he is already logged in, then launches [the application defined in launch app on login](#).
- If the user has a device profile: TSSO initiates the login process for this device profile and [launches the applications on success or failure](#).

If disabled, TSSO simply attempts to log the user in and [launches the applications on success or failure](#).



3.3.1.14 TSSO automatic clear delay (s)

TSSO appears when launching or when clicking on the icon of the notification taskbar. It is hidden after a defined lead time (in seconds). When the automatic login is enabled, you should take care that this auto hide lead time is higher than the automatic login delay.

3.3.1.15 Enabled smooth hiding of TSSO

By default TSSO is hidden gradually (while becoming transparent). In a Citrix environment, it is advised to disable this option to reduce the server and network load.

3.3.1.16 Clear last directory number and phones logged on

When the user is successfully logged on, the tssso client will remove the directory number, so when they next log on they will need to add this value back in.

3.3.1.17 Auto start TSSO when login on Windows

When TSSO is executed the first time it sets the Windows registry, in CURRENT_USER to start TSSO automatically. Default: enabled.

The registry key is checked every time TSSO.exe is executed, the entry is then created/deleted if necessary depending on this setting.

The registry key is:

```
[HKEY_USERS\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"TSSO"="C:\Program Files (x86)\telisca\TSSO\TSSO.exe"
```

3.3.2 Auto login modes

This section is to tweak the behavior of TSSO when logging a user in extension mobility.

Depending on what license you have, the first option is slightly different.

3.3.2.1 TSSO + IPSLOCK option

Auto login parameters

Action on phone detection, after delay or by pressing button Login

Execute action automatically when phone is first found Login

Action when re-connecting on IP Phone Unlock

Execute action automatically on previous IP Phone Login+Unlock

Manual

3.3.2.2 Action on phone detection, after delay or by pressing button

You can choose what action to use when tssso client detects phone: login, unlock or login+unlock.

3.3.2.3 TSSO only

Auto login parameters

Execute action automatically when phone is first found

Action when re-connecting on IP Phone Disabled

Execute action automatically on previous IP Phone Manual

Auto action delay on previous IP Phone (s) 0

Hide TSSO while login

Hide login button

Enable user to enable automatic action on previous phone

Ask to confirm when the user is already logged on another phone ?

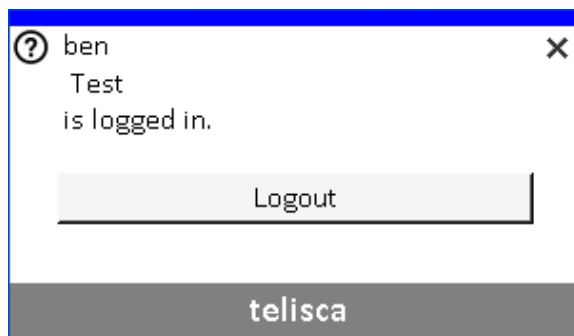
Ask to confirm before login out another user ?

Confirm logout of other user from IP Phone ?

Auto select device profile depending on IP Phone model ?

Enable user to select device profile manually

Set Line Group status to available when login (HLog) ?



Auto login enabled

3.3.2.4 Execute action automatically when phone is first found

With this selected, the login will take place on the phone when its first found.

3.3.2.5 Action when re-connecting on IP Phone

When a phone that was previously used is connected to the PC, this option defines what TSSO should do:

- **Disabled**
TSSO does nothing when the PC gets plugged into a known phone, when opening TSSO user gets a prompt asking him if he wants to login.
- **Login**
TSSO initiates a login on the phone automatically.

3.3.2.6 Execute action automatically on previous IP Phone

If the user has a dedicated IP Phone and logs in occasionally on another IP Phone, one can select an automatic login on the last IP Phone used.

- **Disabled**
Won't try to connect automatically on the last phone.
- **Manual**
The user is prompted to log in on last IP Phone.
- **Automatic**
TSSO tries to log the user on the last IP Phone automatically without asking.

3.3.2.7 Auto action delay on previous IP Phone (s)

When using "Auto login on previous IP Phone" option above, it is advisable to allow the users a chance to cancel the auto login (unless they really never use a different phone). This option displays a countdown on the TSSO client to cancel the auto login.

Default is 20 seconds.

3.3.2.8 Hide TSSO while login

After selecting to login via the client, the window will disappear rather than showing the user the logon process.

3.3.2.9 Hide login button

You can remove the login button so that the user cannot manually login. You would only select this option if you had the 'Execute action automatically when phone is first found' selected and login for both re-connecting and previous phones selected too.

3.3.2.10 Enable user to enable automatic action on previous phone

It is possible to let the user delay and set the automatic lead time to log in. The value entered in "Auto login delay on previous IP Phone(s)" above then becomes the user's pre-filled value.

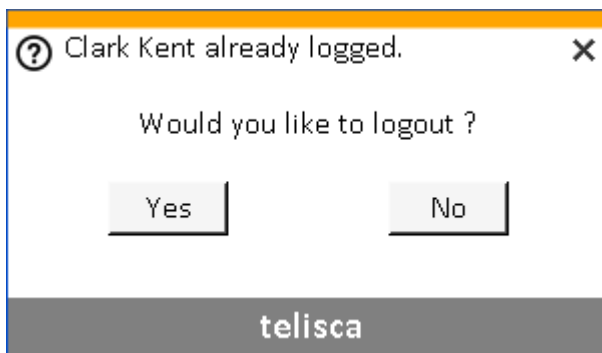
User config on TSSO client

3.3.2.11 Ask to confirm when the user is already logged on another phone

If the current user is already logged on another IP phone, then ask to confirm if he wants to logout before login on the new IP phone.

3.3.2.12 Ask to confirm before login out another user

If your [CUCM doesn't handle multiple logins](#), you can set TSSO to log you out of your current phone before logging you in onto the new one.



Logout another user prompt

3.3.2.13 Confirm logout of other user from IP Phone (Server feature)

Confirm logout of other user from IP Phone itself. Relies on the CTI component of the telisca server. The TSSO client waits ([timeout setting](#)) for the confirmation coming from the device before attempting a login.



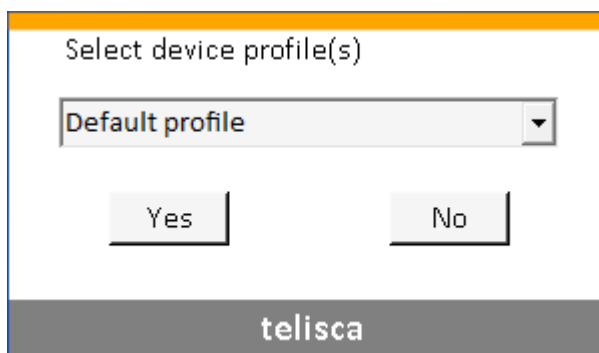
The other user is asked if he wants to be logged out

3.3.2.14 Auto select device profile depending on IP Phone model

When the user has multiple device profiles, TSSO will try to guess which device profile to use depending on the IP Phone model selected. Based on the available profile with the most similar phone model series and number of buttons.

3.3.2.15 Enable user to select device profile manually

If a user has multiple device profiles for the same model of phone, then during the log on process once phone has been selected the user can then select which device profile to log on with.



3.3.2.16 Set Line Group status to available when login (HLog)

If the line is part of a Line Group, this option will set the user HLog flag in CUCM to enable/disable receiving calls from the group.

3.3.3 Auto logout modes

Defines the behavior of TSSO for logging the users out of extension mobility.

3.3.3.1 Action when closing Windows Session

When the Windows session is closed, TSSO is stopped and the user is logged out using Extension Mobility. Default: enabled

3.3.3.2 Action on TSSO logout/lock button click

When the user is logged in, he has a choice of logging out by default, unless we hide the logout button with this option. Default: disabled.



Do not hide logout by default

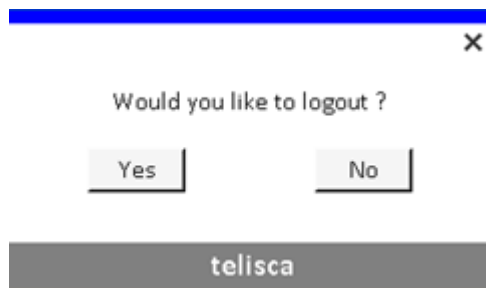


With hide option checked

3.3.3.3 Action when user closes TSSO

Defines what TSSO should do when the [user quits TSSO](#).

- **Do nothing**
TSSO simply closes
- **Automatic logout**
TSSO will log the user out of his current phone
- **Ask user to confirm logout**
Prompts the user with a choice before closing (default):

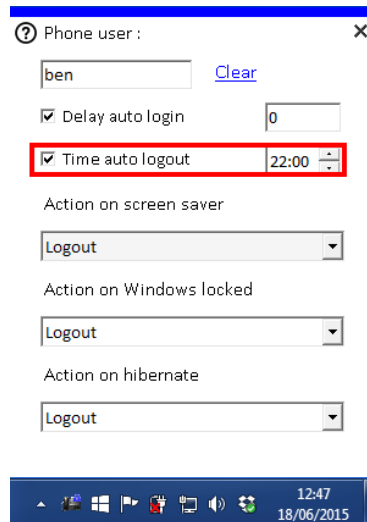


3.3.3.4 Enable logout at defined time

When logging in in with Extension Mobility, it is possible to specify the login duration. Default: disabled

3.3.3.5 Enable user to define auto logout time, logout on Windows lock/hibernate

The user may choose to enable this option and define the automatic logout time. The entered value is then used as the default value. Default: disabled



User config screen

Note: If this option is enabled and the user is already logged in when TSSO is launched, TSSO logs the user out and in again in order to be able to define an adequate login lead time.

3.3.3.6 Enable logout at defined time

This function is used in TSSO to make it possible to define the time of an automatic logout, even if TSSO is not running or the PC is disconnected at that time. Default:22:00

3.3.3.7 Action on hibernate

TSSO logs the user out when the PC goes in hibernation.

3.3.3.8 Action on windows lock

TSSO will logout when the windows session is locked (Win+L) and on Windows Screensaver.

3.3.3.9 Action on screensaver

TSSO will logout when the windows session is locked (Win+L) and on Windows Screensaver.

3.3.3.10 Action when windows session unlock

TSSO logs the user onto the phone when PC unlocked.

3.3.3.11 TSSO server logs out when TSSO disconnected from server (server feature)

Will logout a user if he disconnects from the network. It requires the telisca server. TSSO sends a heartbeat to the telisca server, when the heartbeat stops, telisca server issues a logout command to the callmanager for this user.

3.3.3.12 Action (by WiFi) when no more receiving CDP/LLDP

Logs a user out automatically when taking away a laptop that was connected physically to a phone and is still connected to the network via WiFi. This is available when using phone automatic detection. As soon as TSSO stops receiving the phone's network packet (assuming the user has removed his laptop from the desk), it will try to send a logout command to CUCM via WiFi.

3.3.3.13 Clear call history when locking (IPSLock)

When the phone is locked the call history is cleared.

3.3.3.14 Enable user to set clear call history when locking

The user can turn on this feature manually.

3.3.3.15 Logout CUCM 12 with userId

If the version of CUCM is greater than 12, this option allows to transfer the userId in the Extension Mobility query logout.

3.3.4 Treatments after login

What TSSO will do after a successful login, allows for third party applications integration. After initiating the login, TSSO will periodically check if the login is effective. A similar process occurs for the logout. TSSO then displays the state of the user's IP Phone. This functionality can be useful to start launching a Call Center Agent Desktop. Indeed, the Agent Desktop must be launched after Extension Mobility login is completed so that the directory number can be monitored. If the user is already logged in, the Agent Desktop will be also launched.

Treatments after login

Check login/logout status by CTI ?

Application to process after login/unlock or already logged in	<input type="text"/>
Application to process after logout/lock	<input type="text"/>
Application to process on login/unlock error	<input type="text"/>
Application to process when closing	<input type="text"/>

3.3.4.1 Check login/logout status by CTI (server feature)

Gets the current extension mobility status by CTI, this requires the telisca server to be configured for CTI and to be running at all times. The status of being logged in or out is verified by default using RIS queries on TSSO or can be done by CTI with this option for more reliable results.

3.3.4.2 Application to process after login/unlock or already logged in

Only opens an application when the user is actually logged on his phone. (e.g. Agent Banner, Lync...).

3.3.4.3 Application to process after logout/lock

Will launch an application when the user is logged out of his phone. (e.g. command to close down applications).

3.3.4.4 Application to process on login/unlock error

Opens an application when there is an error during the login process. (e.g. batch file for error reporting).

3.3.4.5 Application to process when closing

Can launch an application when TSSO exits.

4 CUCM Config

This tab is to define the CUCM communication information used by the TSSO client.

Non EMCC option:

Home / TSSO / CUCM Config

Fault tolerant mode: Primary/Backup

Primary CUCM host: 10.2.112.10

Backup CUCM host:

CUCM application user: appMDN

CUCM password:

Confirm password:

Login status refresh delay (mn): 15

AXL query timeout (s): 7

Test userId: [] Test DN to test: []

Test userId: [] Test DN to test: []

EMCC option:

Home / TSSO / CUCM Config

Fault tolerant mode: Primary/Backup

Select cluster: 1

Primary CUCM host:

Backup CUCM host:

CUCM application user: appMDN

CUCM password:

Confirm password:

Load userId's cache

Period to reload userId's cache (h): 4

Login status refresh delay (mn): 15

AXL query timeout (s): 7

Test userId: [] Test DN to test: []

Test userId: [] Test DN to test: []

Within the EMCC option, you can define all of the clusters your TSSO client will be able to log into, so for each cluster you will need to stipulate:

Primary & backup CUCM host

CUCM application user & password

On a daily basis's the user id's are cached from the CUCM cluster, but if you wanted to manually force a load, select the 'load userId's cache' button.

4.1.1.1 Fault Tolerant Mode

This screen makes it possible to define the primary CUCM server (generally the Publisher) and the backup server (generally a Subscriber) allowing login via the Extension Mobility Web Service API. Indeed, since CUCM 6.1, it is possible to log in even if the Publisher is no longer functional. In the same way, the AXL requests are always accessible without the Publisher.

Note: that the hLog function will not work when the Publisher is down.

4.1.1.2 Primary / Backup

Fault tolerant mode

Select cluster

Primary CUCM host

Backup CUCM host

Primary must be the Publisher, Backup is a Subscriber. IP addresses or DNS can be used.

In a multi-cluster environment, you can define the publishers and subscribers hosts of each cluster.

4.1.1.3 Load Balancing

Fault tolerant mode

Select cluster ?

Primary CUCM host

Other CUCM server

Other CUCM server

Other CUCM server

Other CUCM server

Other CUCM server

Other CUCM server

Other CUCM server

Primary must be the Publisher following addresses are the subscribers.

For write operations TSSO does it on the Publisher. For Read operation, TSSO picks up one of the "other CUCM server" address at random and then goes through each one in sequence.

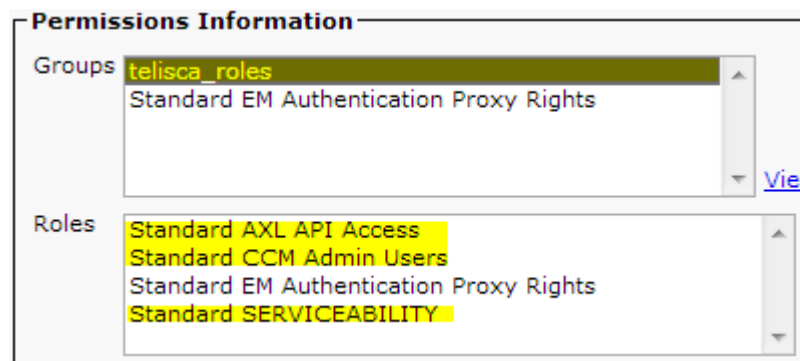
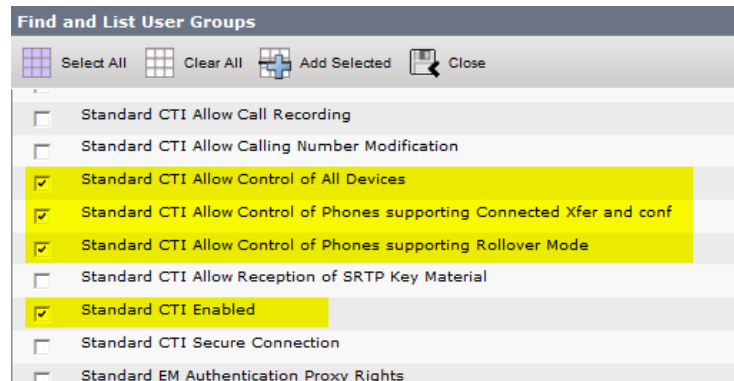
4.1.1.4 CUCM Application User

TSSO uses an authentication proxy user to log any CUCM user in Extension Mobility. The CUCM Application User (name suggestion "tsso_appuser") must be part of:

- User group: Standard EM Authentication Proxy Rights
- Custom User Group with these roles (name suggestion "telisca_roles")
 - Role: Standard AXL API Access
 - Role: Standard CCM Admin Users

If using CTI enabled features, the application user must also be part of these User Groups:

- Standard CTI Enabled
- Standard CTI Allow Control of all devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode



TSSO Application User permissions with custom User Group "telisca_roles"

Standard AXL API Access

To be able to display the user's last and first names and also to select the most appropriate device profile, the Application User also must execute AXL SOAP read queries.

You can test the Service Mobility web access by entering a CUCM userID **already logged** into an IP Phone and pressing the "Test" button. You must obtain the name of the IP Phone on which it is logged.

Fault tolerant mode	Primary/Backup				
Primary CUCM host	10.2.112.10	Test userid	mdn	<input type="button" value="Test"/>	DN to test
Backup CUCM host		Test userid		<input type="button" value="Test"/>	DN to test
					<input type="button" value="Test"/> SEP080027851F83

Testing the CUCM configuration with a logged user id with phone selection = detection

If the IP Phone is detected from the directory number entered, then this Application User will also carry out a AXL SOAP request on CUCM.

You can test the access to AXL SOAP by entering the directory number of an IP Phone (Test DN) and pressing the "Test" button. You must first obtain the name of the associated IP Phone.

Fault tolerant mode	Primary/Backup				
Primary CUCM host	10.2.112.10	Test userid		<input type="button" value="Test"/>	DN to test
Backup CUCM host		Test userid		<input type="button" value="Test"/>	DN to test
					<input type="button" value="Test"/> 231105 <input type="button" value="Test"/> SEP080027851F83

Testing the CUCM configuration with a logged user id with phone selection = by DN

Load userId's cache

Period to reload userId's cache (h)	4	?
Login status refresh delay (mn)	15	?
AXL query timeout (s)	7	

Minimizing queries on CUCM

4.1.1.5 Period to reload userID's cache (H)

Set the period for when the cache is reloaded and any changes picked up.

4.1.1.6 Login status refresh delay (mn)

TSSO periodically executes (by default every 15 min) an Extension Mobility API request to check the login state and to update the tray icon's status color. This request is also executed when you open the TSSO user interface and one minute after the specified automatic logout time. It is thus possible to disable this function (by entering the value 0) to minimize the number of requests to Extension Mobility when there are a large number of TSSO running (i.e., several thousand).

4.1.1.7 AXL Query timeout(s)

How long the TSSO client waits for a response to AXL Queries. Can be increased when CUCM slow to respond or network latency issues. Default: 7 seconds

4.2 LDAP Configuration

This tab is used when the CUCM userID selection is "[Search directory by windows login](#)" ie when doing a directory lookup to retrieve the CUCM User ID from the windows login of the user.

Primary AD or LDAP host	192.168.0.103	<div style="margin-bottom: 5px;">Test</div> <div>Test</div>
Backup AD or LDAP host		
AD or LDAP Port	389	
Version	3 ▼	
Timeout (s)	3	
AD or LDAP proxy user	administrator	
AD or LDAP proxy password		
Confirm password		
Organisation unit to search userid	dc=telisca,dc=com	?
LDAP search filter	objectclass=person	
Windows login field in directory	sAMAccountName	
CUCM userID AD/LDAP attribute	IPUser	?

Directory lookup settings to search for CUCM User IDs

This screen makes it possible to define a LDAP directory or Active Directory in order to query it by the Windows userID and find the CUCM userID. It is possible to define a primary server and a backup server. In the event of failure, a second request will be sent to the backup server.

The query timeout, if no user CUCM has yet been found, is 30 seconds. For the following query, the timeout is much shorter (i.e. 3 seconds) to avoid slowing down the login process. If the timeout is reached, the previous CUCM userID found is used.

The administrator must enter a login/password with read rights.

The administrator must enter the main directory search path for the Windows userID.

Lastly, the administrator must enter the attribute containing the Windows userID (search key) and the attribute containing the CUCM userID (result).

Tip: To check your settings and connectivity, you can also use an LDAP or AD client such as:

- AD Explorer <http://technet.microsoft.com/en-us/sysinternals/bb963907>
- LDAP Admin <http://www.ldapadmin.org>

4.3 Help texts

This tab is to customise the tooltips displayed in the TSSO client.

Language / Screen	Help Text
Login screen help(FR)	Veillez saisir ou sélectionner le numéro de ligne{CR}affiché sur le poste téléphonique sur lequel vous souhaitez v
Logout screen help(FR)	Cliquez sur 'Logout' pour désactiver votre profil du téléphone.
Already logged screen help(FR)	Un autre utilisateur est resté connecté sur ce téléphone.
Config screen help(FR)	Modifiez les paramètres souhaités et fermez la fenêtre,{CR}les modifications seront sauvegardées.
Login screen help(EN)	Enter or select the line number displayed on the IP Phone{CR}on which you want to login.
Logout screen help(EN)	Click on 'Logout' to remove your profile from the phone.
Already logged screen help(EN)	Another user is currently logged on this phone.
Config screen help(EN)	Update the parameters and close the window.{CR}The parameters will be automatically saved.
Login screen help(DE)	Enter or select the line number displayed on the IP Phone{CR}on which you want to login.
Logout screen help(DE)	Click on 'Logout' to remove your profile from the phone.
Already logged screen help(DE)	Another user is currently logged on this phone.
Config screen help(DE)	Update the parameters and close the window.{CR}The parameters will be automatically saved.
Login screen help(NL)	Geelieve het nummer getoond op de telefoon waarop uw zich wenst te identificeren,{CR} te noteren of te selecten
Logout screen help(NL)	Klik op 'Afmelden' om uw telefoonprofiel te desactiveren.
Already logged screen help(NL)	Een andere gebruiker is aangemeld gebleven op deze telefoon.
Config screen help(NL)	Wijzig de gewenste parameters en sluit het venster,{CR}de wijzigingen worden bewaard.

The help messages must be changed to adapt to the defined settings. The help messages are available in English, French, German and Dutch.

To insert a line break in your text, add this: {CR}.

To reset a default help message, delete the selected message, save the screen, and reopen it.

4.4 Association Pc-Phone

This tab is used to permanently tie up physical workstations and IP Phones with no user input. It has to be populated if using [fixed Pc-IP phone association](#) mode.

The screenshot shows the telisca web interface for the 'Association Pc-Phone' configuration. The left sidebar contains navigation options: Dashboard, Global configuration, Support, TSSO (selected), Global parameters, Profiles, CUCM Config, LDAP Config, Help texts, Association Pc-Phone, Monitoring, and Client update. The main content area has a breadcrumb trail: Home / TSSO / Association Pc-Phone. Below this is a search section with two dropdown menus: 'PC identity' set to 'Contains' and 'IP phone name' set to 'Contains', each followed by an empty text input field. There are 'Search' and 'Display all' buttons. Below the search section is an 'Import data from file CSV' section with a 'File CSV path' field containing 'Choose File' and 'No file chosen', and an 'Upload' button. Underneath is a table titled 'Associate list PC identity and IP phone' with columns for 'Edit', 'Delete', 'PC identity', and 'IP phone'. The table contains one row with 'M3800' for PC identity and 'SEP9CEBE82444DF' for IP phone. There are 'Add' and 'Export CSV' links above the table.

4.4.1.1 Search

To find which device is associated to which phone. Or list on screen all the associations.

4.4.1.2 Import data from file CSV

You can upload a CSV file containing PC, IP Phone columns and edit each row individually. The PC identity is either the hostname or MAC address depending on [the option selected](#).

Example of the CSV file content:

```
1.2.3.4,SEP5C6A5548
5.6.7.8,SEP541A547B
9.10.11.12,SEP655E558C
```

Note: the association can be individually overridden manually from the TSSO client using the administrator access.

4.5 Monitoring

This tab gives you access to real time users login/logouts, statistics and reports. This tab is visible only when the TSSO Server option is enabled.

The screenshot shows the telisca web interface. The top navigation bar includes a hamburger menu and the 'telisca' logo. The left sidebar contains the following menu items: Dashboard, Global configuration, Support, TSSO (highlighted), Global parameters, Profiles, CUCM Config, LDAP Config, Help texts, Association Pc-Phone, Monitoring (highlighted), and Client update. The main content area shows the breadcrumb 'Home / TSSO / Monitoring'. Under the 'Statistics' heading, the following data is displayed: TSSO licences total :16, Deployed TSSO total :1, Static associate total :0, Dynamic associate total :0, and Logged PC total :0. Below this is the 'Report of association' section, which includes a dropdown menu for 'Associate type' set to 'All' and a blue 'Display' button. The content area below the dropdown is empty.

4.5.1.1 Statistics

Static count displays the number of TSSO clients which have identified a computer and phone in a correspondence table.

Dynamic count means how many times TSSO has associated a phone and computer by automatic detection or by using an entered directory number.

4.5.1.2 Report of association

Date and time displayed represent the time when a phone and computer were identified as linked. It doesn't relate to the time of a logout or login.

5 Deployment

TSSO has a web based administration component and a client component. The administration is used to generate the TSSO configuration file deployed with the clients on the users' computers. This file containing the current settings entered in the administration can be downloaded from the "Install tab".

Note: this file also contains the license information.

5.1 Client install tab

From this tab, the administrator downloads:

- The client installation file
- The users configuration file

The screenshot shows the 'telisca' web interface. The left sidebar has a menu with items: Dashboard, Global configuration, Support, TSSO (selected), Global parameters, Profiles, CUCM Config, LDAP Config, Help texts, Association Pc-Phone, Monitoring, and Client update. The main content area is titled 'Home / TSSO / Client update'. It contains text explaining that TSSOClient.msi setup programs need to be run on the PC, requiring at least .Net 2.0. It provides a command line example: `TSSOClient.msi INSTALLPCAP=1 URLCONFIG="http://xxx.xxx.xxx.xxx/TSSO/Download/TSSO_cfg.txt"`. It also describes two ways to install the system configuration file: copying TSSO_cfg.txt to the same directory as TSSO.exe, or adding a URL parameter. A URL example is provided: `http://xxx.xxx.xxx.xxx/TSSO/Download/TSSO_cfg.txt`. Below the text are two download links: 'Download TSSO config file' and 'Download TSSOClient.msi setup'.

The install tab

Administrators can deploy the installation of TSSO client software across their network using their own set of tools and procedure.

The msi installation file can be installed with the config file in the same folder or using a parameter pointing to a remote location for the config file.

Note! the installation must be done within administrator context, "running as administrator" on one of the sample batch or MSI files from a user session on a local PC may create a broken Start menu shortcut to TSSO or not install the MSI at all. The administrator context can be achieved using appropriate deployment tools.

5.1.1 Installation file: TSSOClient.msi

The installation file is available on the server or via a URL:

```
http://[TELISCA_SERVER]/TSSO/download/TSSOClient.msi
```

TSSO Client installation file download URL

```
C:\inetpub\wwwroot\TSSO\download\TSSOClient.msi
```

Default local path of the client installation file on the server

The MSI file can be launched as-is with the config file TSSO_cfg.txt in the same folder, alternatively it can be executed with some parameters.

```
TSSOClient.msi TARGETDIR="%PROGRAMFILES(x86)%\telisca\TSSO" INSTALLPCAP=0
URLCONFIG="http://X.X.X.X/TSSO/download/TSSO_cfg.txt"
```

TSSO.msi parameters example with the default values

5.1.1.1 Installation file parameters

- **Setup folder, TARGETDIR**

If you want to change the default installation folder.

Values: "[PATH_TO_INSTALL_FOLDER]"

Example: TSSOClient.msi TARGETDIR="D:\apps\tss" (installs tss on D:)

Default: %PROGRAMFILES(%86)%\telisca\TSSO

- **WinPcap driver, INSTALLPCAP**

To force the installation of the [pCap driver](#) used by [automatic detection of the connected phone](#). Disable when the WinPcap driver is already installed on the machine, or when not using automatic phone detection. Will install the Wpcap.dll file in "Windows/System32/" folder.

Values: [0|1]

Example: TSSOClient.msi INSTALLPCAP=1 (will install the winpcap driver)

Default: 1

- **Configuration file URL, URLCONFIG**

Can specify the remote location of a configuration file during installation. **Note:** if a config file is in same folder as TSSOClient.msi, the local config file will override the one specified remotely.

Values: [URL_TO_CONFIG_FILE]

Example: TSSOClient.msi URLCONFIG="http://1.2.3.4/TSSO/download/TSSO_cfg.txt" (will install with a config file located on server with IP 1.2.3.4)

Default: NONE, will pickup the TSSO_cfg.txt in the current folder [see standard installation](#)

- **Launching the client after installation, RUN**

Can force launching the TSSO.exe client as soon as the installation has completed. It is disabled by default since it is usually installed as an administrator for use by a standard user.

Values: [0|1]

Example: TSSOClient.msi RUN=1 (will launch the client after install)

Default: 0

- **Launching TSSO client on Windows login, START**

Execute TSSO.exe client when the Windows session is opened, for all users. It is enabled by default since it is usually installed by an administrator.

Values: [0|1]

Example: TSSOClient.msi START=1 (will launch the client on Windows login)

Default: 1

5.1.2 Configuration file: TSSO_cfg.txt

The config file used by TSSO is named TSSO_cfg.txt. It is encrypted via AES 128 bits. It contains the TSSO license, when upgrading the TSSO license on the server, the new configuration file can update all the clients (for instance for switching from a demo license to a purchased one).

The current config file is by accessible on the telisca server at this location:

```
http://[TELISCA_SERVER]/TSSO/Download/TSSO_cfg.txt
```

Config file location on the telisca server

5.1.2.1 Standard installation

When launching TSSO.msi, the installer will use the TSSO_cfg.txt in the current folder.

5.1.2.2 Remote configuration installation

It is also possible to use a remote config file during installation, using the URLCONFIG parameter with TSSO.msi. When URLCONFIG parameter, make sure there is no TSSO_cfg.txt in the current folder. [See URLCONFIG](#)

5.1.2.3 Original local configuration file

The configuration file used during installation is copied in the default installation folder:

```
%PROGRAMFILES(x86)%\TSSO\TSSO_cfg.txt
```

Default config file location on the user's PC

or into a [custom location](#) if any.

Note: this initial install config file is overridden by [the one downloaded with auto-updates](#).

5.1.2.4 Changing the configuration after installation

If it is required to change the configuration file after the client has been installed. It is possible to launch the TSSO client (TSSO.exe) once with the URL of the new configuration file as a parameter.

```
TSSO.exe "http://[TELISCA_SERVER]/TSSO/Download/TSSO_cfg.txt"
```

Changing the configuration file after installation

From then on, TSSO will use this URL to [auto-update](#) its configuration. It overrides the [auto update URL defined](#) in the administration.

5.1.2.5 Configuration auto update

TSSO can update its configuration by checking a remotely hosted configuration file. TSSO retrieves the remote configuration file:

- 2 seconds after startup
- then every 4 hours

This auto update mechanism can be used in two ways:

1. By entering a [URL in the administration](#)
2. By launching the [TSSO client with a URL as parameter](#)

To stop auto updates it is possible to override the remote config setting by launching the TSSO client once with a special parameter:

```
TSSO.exe download=
```

Stopping configuration auto update on the client

Important: some settings changes that alter dramatically how TSSO behaves will only be taken into account after TSSO restarts the next time. Following this scenario:

1. TSSO collects the new configuration file
2. TSSO applies minor changes live
3. TSSO's next launch
4. TSSO uses all the new settings

5.1.2.6 Remotely downloaded configuration file

The configuration file downloaded from a remote location overrides automatically [the one used during installation](#). It is saved in this location:

```
%LOCALAPPDATA%\telisca\TSSO\TSSO_cfg.txt
or if the above isn't present:
%APPDATA%\telisca\TSSO\TSSO_cfg.txt
```

TSSO uses the configuration file in this location first

5.2 TSSO client command line parameters

Some command line parameters are available on the client, with the following syntax:

```
TSSO.exe [http://[TELISCA_SERVER]/TSSO/Download/TSSO_cfg.txt] [-autologin=1|0] [-hide=1|0]
[-pProfileName]
```

5.2.1 Remote config file

This setting is explained in [changing TSSO configuration after install](#)

5.2.2 -autologin

Autologin=0|1 : disables or enables automatic login. If omitted, uses the mode defined in the configuration file.

5.2.3 -hide

Hide=0|1 : hides TSSO user interface while logging in or out (default, 0). When using a ZERO user interaction configuration, is useful to make the process of logging in completely invisible to the user.

5.2.4 Profile name -pProfileName

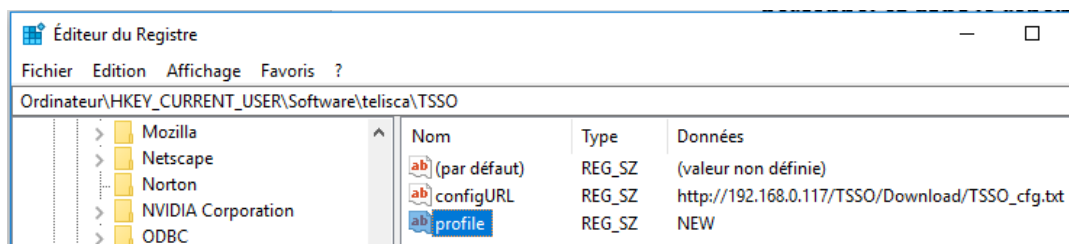
Specifies the profile to use concatenated to -p argument. TSSO will use the default profile if left empty. See [the Profile section](#) for other methods to change a user's profile.

5.3 Update profile used

If you add a new profile in TSSO administration and want some of the PC to use it. You can either change the batch that call TSSO and add the parameter `-p` followed by the profile name. Other PC without the parameter will still use the profile defined as default in the administration.

Otherwise you can change the profile defined in TSSO registry. The new profile will be used as soon as TSSO is launched again.

The profile is store in the registry in the path **HKEY_CURRENT_USER\Software\telisca\TSSO** in the string property **profile** (see below):



5.4 User configuration file: UserConfig.xml

All the settings that are available to the user from the TSSO client as well as previously used numbers... are saved into the user config file.

The user's config file is saved by TSSO in the user's personal directory:

```
%LOCALAPPDATA%\telisca\TSSO\UserConfig.xml
or if the above isn't present:
%APPDATA%\telisca\TSSO\UserConfig.xml
```

User settings and history are saved locally here

Here an example of the XML user's configuration file, UserConfig.xml:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<CONFIG>
<LOGOUT_TIME_ENABLED>1</LOGOUT_TIME_ENABLED>
<LOGOUT_TIME>21:45</LOGOUT_TIME>
<AUTO_LOGIN_ENABLED>1</AUTO_LOGIN_ENABLED>
<AUTO_LOGIN_DELAY>10</AUTO_LOGIN_DELAY>
<CUCM_USER>mdnguyen</CUCM_USER>
<LOGOUT_ON_CLOSE>0</LOGOUT_ON_CLOSE>
<LAST_DN>
<DN>6789</DN>
<DN>1234</DN>
<DN>789</DN>
<DN>7041</DN>
<DN>7022</DN>
</LAST_DN>
<LAST_DEVICE_NAME>SEP001B54CA0D1D</LAST_DEVICE_NAME>
<CONFIG_HTTP_URL>http://198.168.0.132/TSSO/Download/TSSCO_cfg.txt</CONFIG_HTTP_URL>
</CONFIG>
```

It contains

- The settings defined by the user
- The CUCM userID, if it is entered by the user
- The last 7 directory numbers entered
- The last IP Phone detected
- The URL to upgrade the setup file

5.5 Log files for support and debug

Please **always** provide server and client log files if you encounter any issues with TSSO. Use your current integrator support channel or raise a ticket on <http://support.telisca.com>

5.5.1 Server side logs

If TSSO relies on the server side features or you encounter issues using the administration, it is necessary to retrieve the logs on the server.

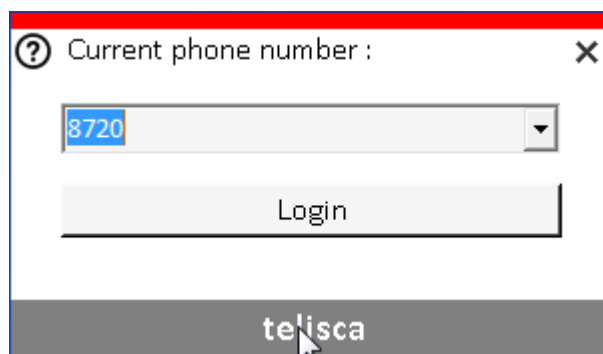
Administration > MENU > Support > Zip logs > TSSO + Generate



Retrieving the logs from the server

5.5.2 Client side logs

You can visualize the log file in notepad from the TSSO client. Click on the lower label indicating the name of the company defined in the license or "EVALUATION" while holding shift + Ctrl.

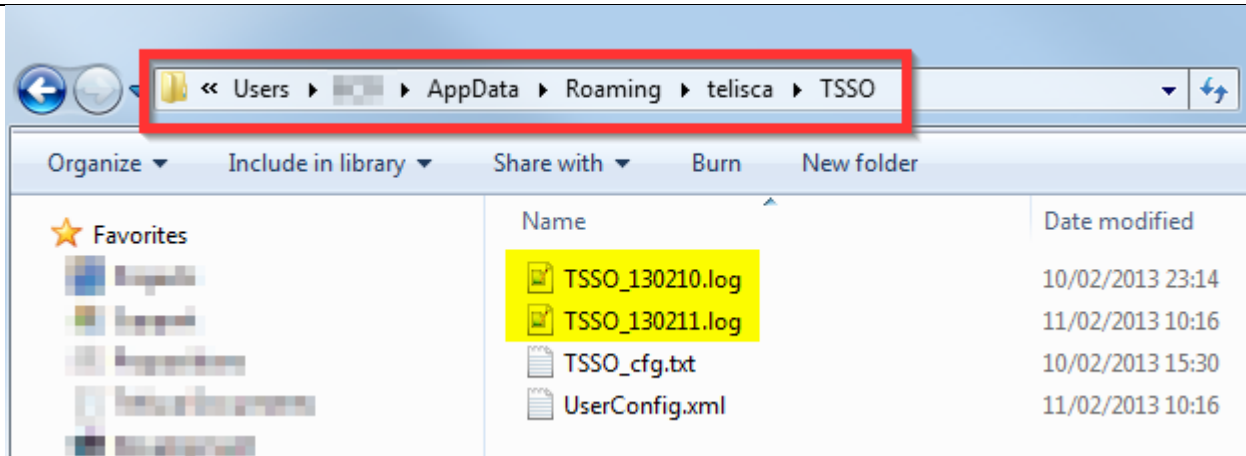


*Opening the log from TSSO
with Shift + Ctrl + Click
on the red rectangle area*

The log files on the user's PC are created in:

```
%LOCALAPPDATA%/telisca/TSSO/TSSO_[DATE].log
or if the above isn't present:
%APPDATA%/telisca/TSSO/TSSO_[DATE].log
```

Log files location




Log files are retained for the number of days [specified here](#), and contains the level of details [specified here](#).

6 TSSO user interface

The TSSO user interface may differ depending on the settings defined by the administrator.

6.1 Opening TSSO

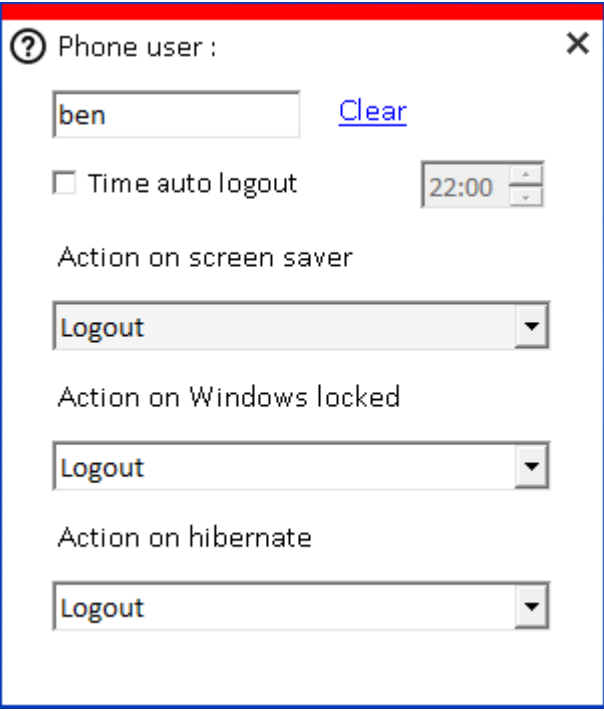
TSSO is [usually launched automatically](#) when opening the Windows session and appears in the bottom right of the screen (just above the Windows taskbar). It disappears at the end of a [defined lead time](#) or after clicking on the top right cross.

To open TSSO again, click on the  icon in the Windows taskbar notification area. By right clicking, you get the following menu: Open (displays TSSO), Settings (user's setting screen), Quit.

A contextual online help is made available by clicking on the (?) icon on left top. These messages can be customised in the [Help text tab](#)

6.2 Entering the CUCM userID

When TSSO is used for the first time or as long as the CUCM userID is not defined, TSSO automatically displays the user's setting form. It thus makes it possible to enter the CUCM userID and other parameters as well. These other parameters can be disabled by the administrator. The settings are saved automatically when closing the form.



Phone user :

ben [Clear](#)

Time auto logout 22:00

Action on screen saver

Logout

Action on Windows locked

Logout

Action on hibernate

Logout

6.3 Phone selection

6.3.1 Automatic IP Phone detection

When launched, TSSO displays the message "Searching IP Phone." The "Login" button is then disabled. When the IP Phone is detected, it displays the identifier of the IP Phone and the Login button is enabled.

When TSSO has already been used, it also displays the last IP Phone used. The "Login last phone" button is enabled. This allows you to avoid waiting for the same IP Phone to be detected again.

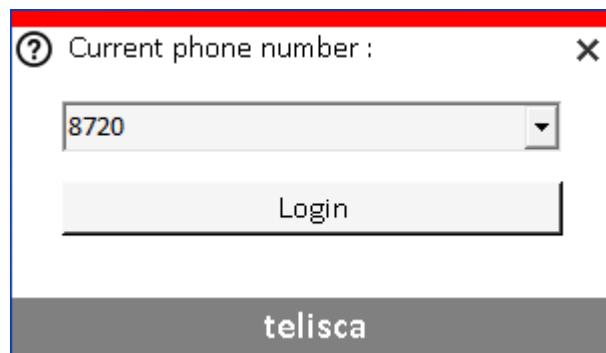


If the automatic login has been enabled, a hyperlink appears under the "Login last phone" button, followed by the number of seconds remaining before the automatic login will be executed. By clicking on this hyperlink, the user cancels the automatic login process.



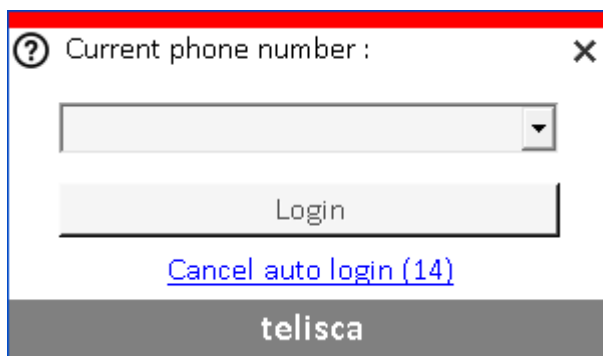
6.3.2 IP Phone detection by directory number

The user enters a directory number or selects a directory number in the drop down list.



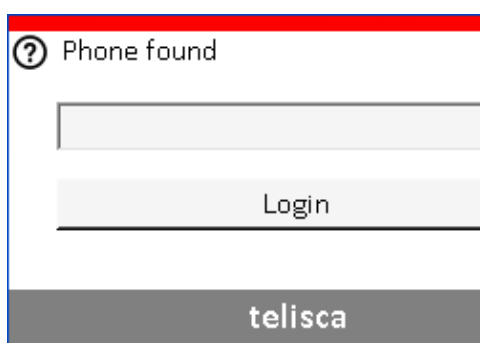
If the user has already logged in from TSSO on the same IP phone, he or she can leave the number already entered and press the login button.

If the automatic login is enabled, a hyperlink appears under the "Login" button, followed by the number of seconds remaining before the automatic login will be executed. The user can cancel the automatic login if he or she has changed IP Phones.

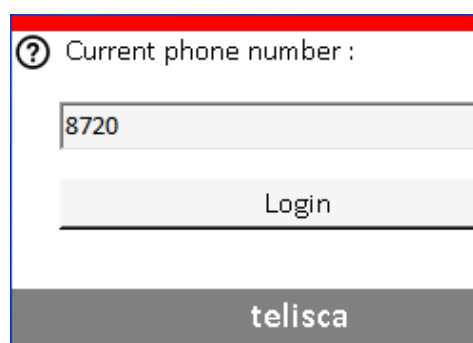


6.3.3 Fixed mode: PC/Phone association

If TSSO uses a profile with PC/Phone association, TSSO will query the telisca server to find out what phone to use. Depending on if other phone selection modes and other settings are enabled, the user will be able to change the phone returned from the association list or not.



Fixed + phone detection



Fixed + DN entry (+phone detection)

6.4 Login process

When the login process is completed (this operation can last 8 to 10 seconds), TSSO displays the login status with the first and last name of the user. The "Login" button changes to "Logout", if enabled.



Different error messages may be displayed if the login process failed.

6.5 The IP Phone is already logged

If the IP Phone is already logged with the current user, TSSO displays the login status immediately.

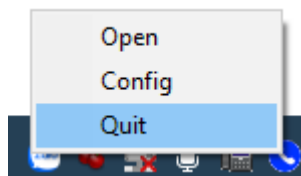
However, if the "automatic Logout at a defined time" option has been configured, TSSO logs out and immediately logs in again to apply the appropriate login duration.

If the IP Phone is already logged in with a different user, TSSO displays the userID already logged in and requires a validation to log it out if [the setting is enabled](#).

Note: If the current user is already logged on another IP Phone, an error can occur depending on your CUCM Extension Mobility settings. You may change the CUCM parameter of [Intra-cluster Multiple Login Behavior](#) to "Multiple Login Allowed" or "Auto Logout" to authorize it or force TSSO to [log the user out](#) first.

6.6 Exiting from TSSO

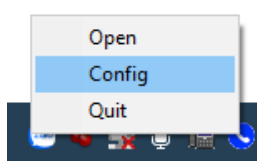
You can manually exit from TSSO by right clicking on the icon of the Windows taskbar and selecting the "Quit" menu.



When the Windows session is closed, TSSO is automatically closed and by default logs out the IP Phone. [The option to change this behaviour is here](#).

6.7 TSSO user settings

The user settings screen is available from the TSSO menu by right clicking on TSSO icon in the Windows taskbar notification area.

 A screenshot of the TSSO user settings dialog box. The title bar reads 'CUCM UserID :'. Below the title bar, there is a text input field containing 'mdn' and a 'Clear' button. There are three checked checkboxes: 'Delay auto login(s)' with a value of '10', 'Time auto logout' with a value of '22:00', and 'Action on screen saver' with a dropdown menu set to 'Logout'. Below these are two more dropdown menus, both set to 'Logout', labeled 'Action on Windows locked' and 'Action on hibernate'.


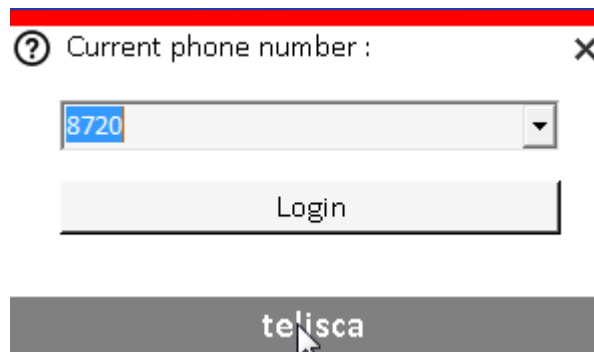
User may be prompted for confirmation to quit and can log out from extension mobility automatically depending on [the Action when user close setting](#).

6.8 User profile configuration

This screen lets users or admins:

1. select a profile to use (can also be done with a [tssso client launch parameter](#))
2. create a new phone/PC association

To access this screen, the user or administrator must Right Click + Alt on the company name or evaluation label at the bottom of the TSSO client interface.

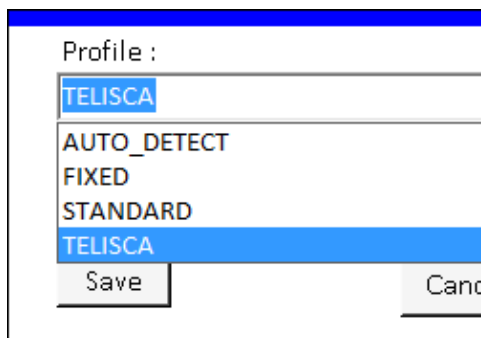


*Opening the user profiles from TSSO
with Shift + Alt + Click
on the red rectangle area*

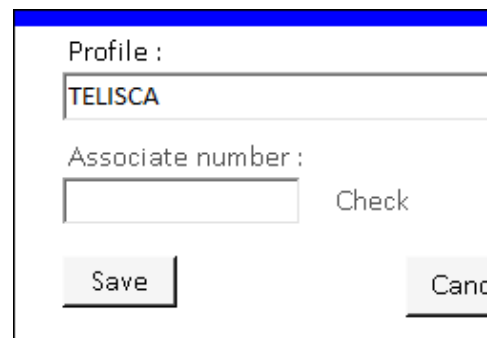
Selecting a profile and creating a new association can be [restricted with a password](#).
Important: The changes will be effective when TSSO restarts.

6.8.1 Selecting a profile to use

Once tssso client has started, you need to `Ctrl+Alt+right click on the company name which will present you with the profile selection:



Selecting a new profile



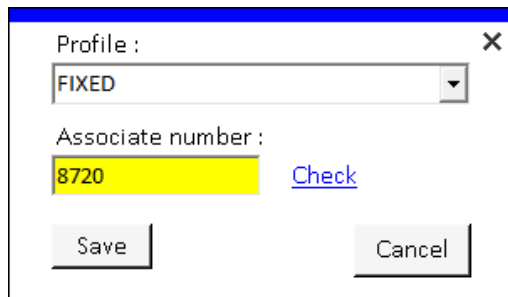
then save

Restart TSSO, and the new profile will be used.
See [the Profile section](#) for other methods to change a user's profile.

6.8.2 Creating a new PC/Phone association

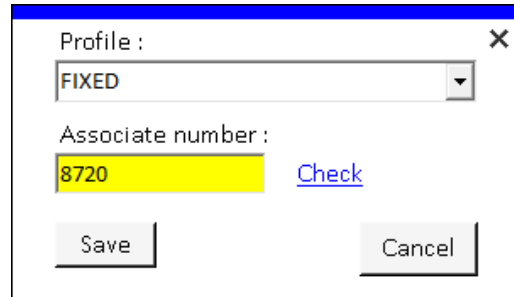
This allows creating an association PC and IP Phone and to save it on the telisca server.

1. Select the profile to use
2. Enter the DN of the phone to associate with this computer
3. Press "check".
 - a. A red color indicates that the phone is not yet verified.
 - b. A yellow color indicates that TSSO is trying to verify it and is waiting for confirmation on the IP Phone.
4. Once it is all white, it is possible to save it (enter the password if required)



The dialog box shows the 'Profile' dropdown set to 'FIXED' and the 'Associate number' field containing '8720'. The 'Associate number' field has a yellow background, indicating that the phone is not yet verified. A blue 'Check' button is visible next to the number field. The 'Save' button is disabled, and the 'Cancel' button is active.

Phone not associated



The dialog box shows the 'Profile' dropdown set to 'FIXED' and the 'Associate number' field containing '8720'. The 'Associate number' field has a yellow background, indicating that TSSO is trying to verify it and is waiting for confirmation on the IP Phone. A blue 'Check' button is visible next to the number field. The 'Save' button is disabled, and the 'Cancel' button is active.

Association pending

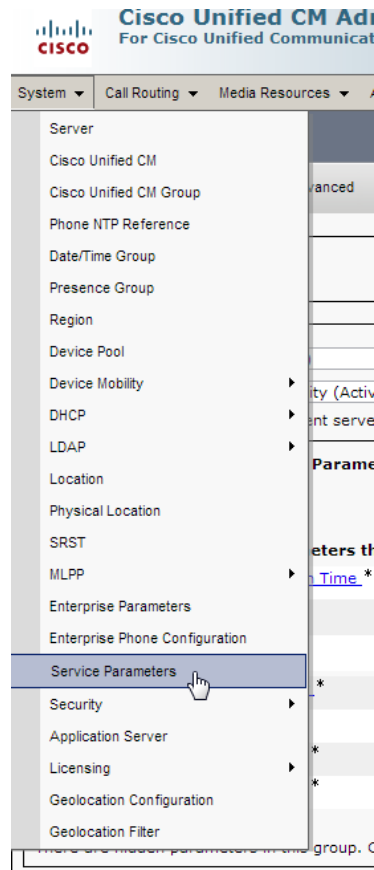
Restart TSSO, and TSSO will now automatically use the fixed association.

7 Appendix

7.1 Multiple login behavior

This CallManager behaviour relates to [this TSSO setting](#).

To check and set how the extension mobility behaves when trying to log a user already logged on another phone, you can access the CUCM Administration > System > Service Parameters.



Select Server and Service

Server*

Service*

All parameters apply only to the current server except parameters that are in th

Then check **Intra-cluster Multiple Login Behavior** setting:

[Inter-Cluster Maximum Login Time](#)*

Intra-cluster Multiple Login Behavior*

[Alphanumeric User ID](#)*

[Remember the Last User Logged In](#)*

[Clear Call Logs on Intra-Cluster](#) False

7.2 Setting user profile from registry

It is possible to change a registry key to set the user's TSSO Profile.

The typical content of a registry file (example: change_profile.reg) to write the correct parameters in the registry to change the current user's selected profile is:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\TELISCA\TSSO]
"profile"="[PROFILE_NAME]"
"configURL"="http://[TELISCA_SERVER]/TSSO/Download/TSSO_cfg.txt"
```

It is necessary to restart the TSSO application to apply this change.

See [the Profile section](#) for other methods to change a user's profile.