Administrators Guide

Phone Robot

Version: 6.0.x

SUPPORT@TELISCA.COM
TEL. +33 (0)1 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 Phone Robot description

1.1 Overview

Some configuration changes require manual key strokes actions on the IP Phones using the soft keys and key pad. In order to automate these tasks, it is necessary to simulate pressing the keys and buttons on the IP Phones.

Phone Robot allows to automate these processes on a large number of IP Phones:
- Delete the CTL / ITL file of the IP Phone (to update certificate),
- Select a new IP Phone background,
- Upload IP Phone tailored backgrounds on the TFTP server,
- Change network settings,
- Execute non-regression tests after a firmware update,
- Capture IP Phone screen copies.

You can define any script that send keys, execute it on all, or a list, of IP Phones and get an execution report. It is also possible to capture the IP Phone's configuration status and image.

Different scripts can be executed by phone models. Phone Robot helps by splitting the list of phones by model.

1.2 Architecture

Phone Robot takes advantage of IPS Framework & Administration and CTI Server. The key strokes are sent using the CTI (JTAPI) interface. Unlike the push via HTTP, this solution eliminates the need to manage authentication and does not require that the IP Phones are 'Web Enabled'.

Phone Robot is able to retrieve the list of all IP Phones via AXL SOAP queries. It is also possible to load a list of IP Phones from a text file.

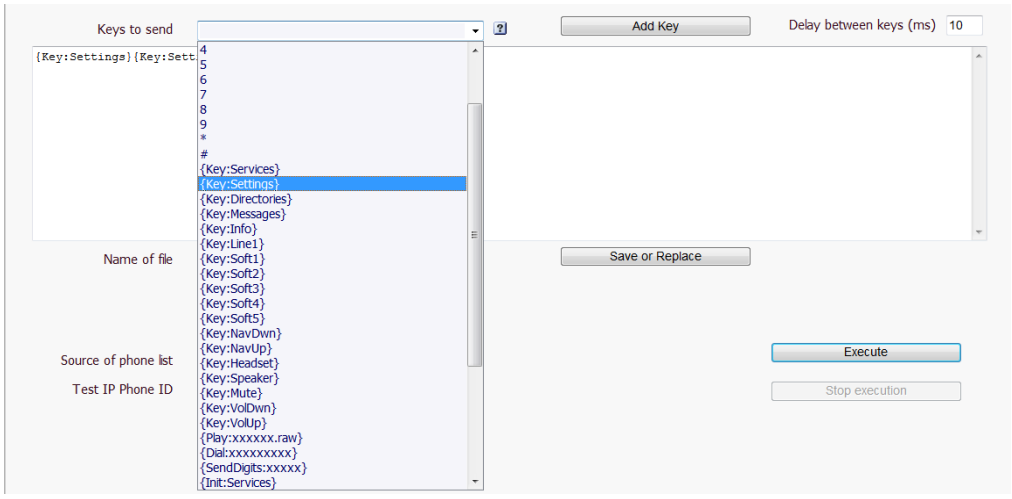
To facilitate the operations for a large number of IP Phones Phone Robot is multi-threaded, to be able to send keys simultaneously to several IP phones at the same time.

1.3 Administration and features

The administration Web interface provides a script editor, in order to define the list of IP Phone keys to send, separated by an administrator defined delay.

The script can be tested on one IP Phone. Then it can be applied to a list of IP Phone or all the IP Phones.

During the execution, the amount of IP Phones treated, the total amount of IP Phones selected and the remaining time of execution is displayed.



An execution report is generated, with succeeded and failed information.

It is also possible to capture a status parameter from the IP Phone (XML) Web Page and compare it to a target value. In this case, the IP Phones must be Web Enabled.

At least it is also possible to capture the image of the IP Phone's screens and save them for a visual control. In this case, the IP Phones must be Web Enabled.

1.4 Requirements

Supported Cisco CUCM:

- CUCM version 10.5, 11.5, 12, 12.5, 14

- 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

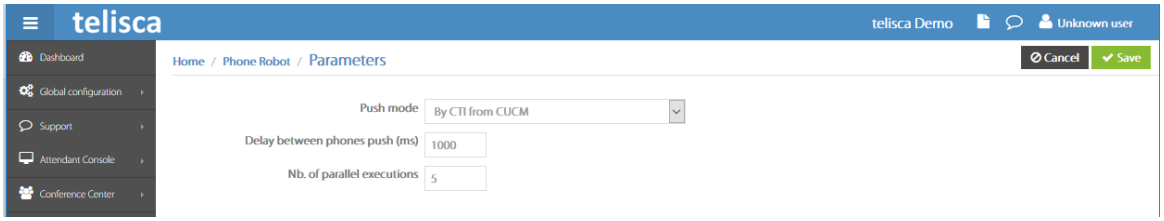
- Minimum configuration: 1 vCPU, 4GB RAM, 70GB disk
- Virtual Machine VMware vSphere, Hyper-V or Cisco UCS, Cisco UCS-E
- Cloud ready

It is also possible to capture a status parameter from the IP Phone (XML) Web Page and compare it to a target value. In this case, the IP Phones must be Web Enabled.

2 Administration

2.1 Phone Robot Parameters

This screen is accessible from Phone Robot menu, 'Parameters' tab.



This screen defines the mode to push scripts on IP Phones:

- **By CTI from CUCM**: telisca CTI Server send a SendData command to CUCM CTI Manager to push keys or URL to the phone by SCCP or SIP protocol. telisca CTI Server can control and CTI monitor dynamically any phone assuming it is checked as CTI enabled.

- **By HTTP**: telisca application does a direct http push to the IP Phones. Push parameters are defined in Global Config menu, Push config tab. It requires that the IP Phone have the parameter Web enabled set to true. For the best performance and security, we also provide an authentication proxy (see below).

Note: See appendix Push by HTTP settings.

You can set also performance parameters:

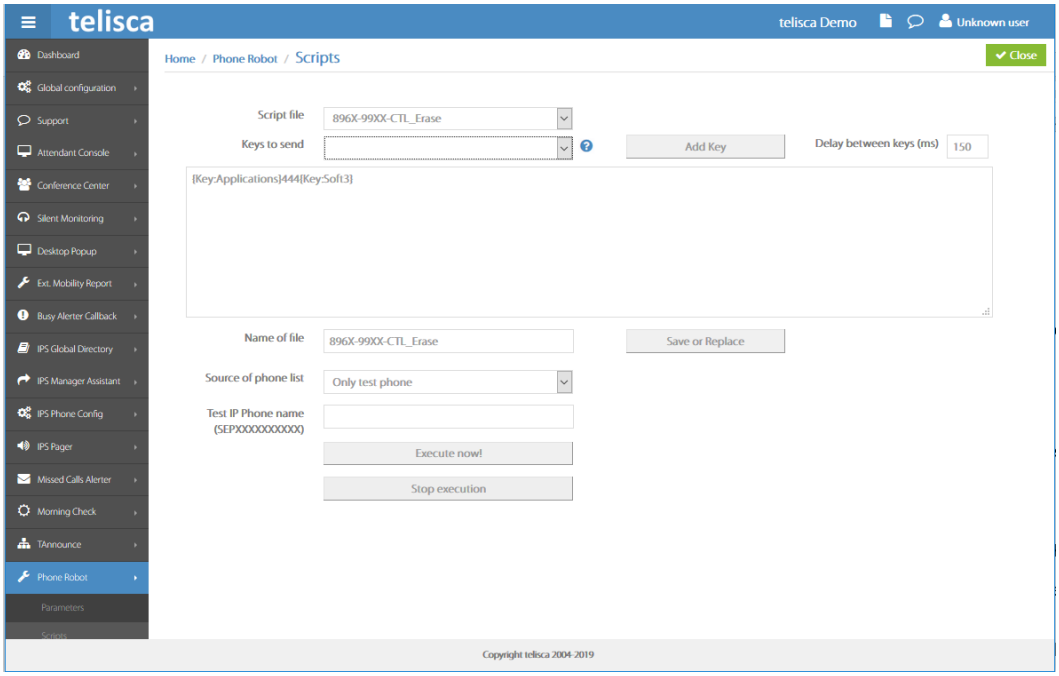
- Delay between scripts executions
- Number of simultaneous executions

With this parameter you can tailor the execution speed for large configurations. If by example the script is executed in 5 seconds + 1 seconds of pause between scripts and you execute 10 times simultaneously, the script should be executed on 10 x 60 / (5 + 1) = 100 phones in 1 minute.

2.2 Scripts

This screen is accessible from Phone Robot menu, 'Scripts' tab.

It defines the sequence of keys to send and save it in a script. Different scripts may be necessary depending on the IP Phone model. It is possible to define a standard delay between each button and add additional time with the {Delay: valueMs} indicating the timeout in milliseconds.



It is possible to send all keyboard keys type commands {Key: key}.

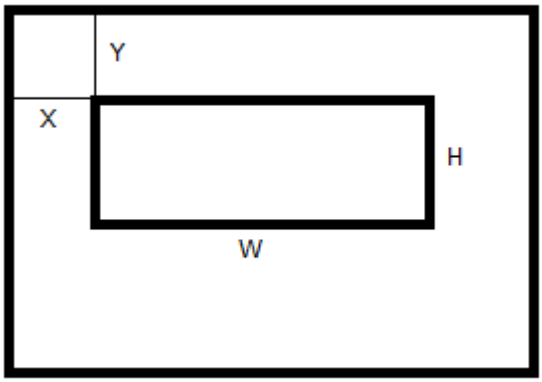
It is possible to reset the environment (for example at the end of the script), for example with the command {Init: Services}.

You can send a sound file (stored on the TFTP server) {Play: fichierRaw}.

It is possible to dial with the {Dial: number} (not supported on very old firmware).

Finally, it is possible to capture a screen shot with the {ScheenShot: user: pwd: x: y: w: h} which is then stored in a PNG file on behalf of the IP Phone. Please note this command requires authentication. It will only operate in push mode providing http login, password or IP Phones by configuring the proxy authentication (see global configuration). Moreover, the web must be IP Phone Enabled.

{ScreenShot format: user: pwd: x: y: w: h} capture a portion of the IP Phone screen:



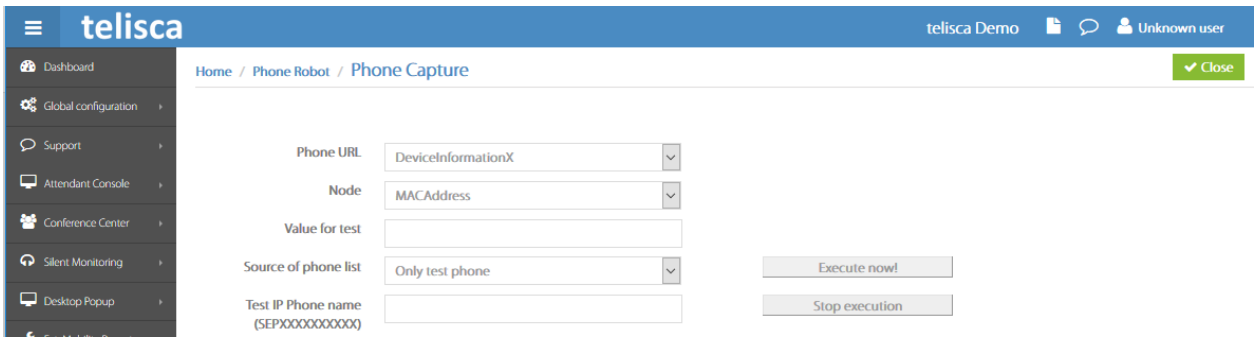
Note: User / Pwd associated with the IP Phone or with the proxy User / Pwd authentication is replaced by X.

You can execute the script on:
- A test phone
- A list of phones by model
- A list of phones you have loaded
- A report of execution
- A list of directory numbers (which are converted to IP phone by the application)

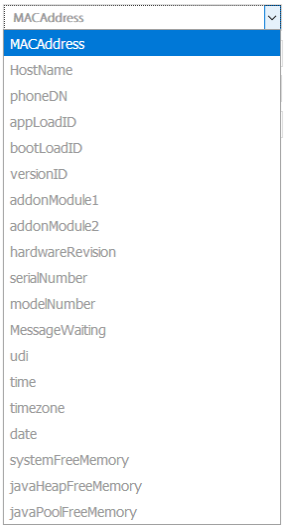
2.2.1 Phone Capture

This screen is accessible from Phone Robot menu, 'Phone Capture' tab.

It allows you to capture the configuration of IP Phones to XML, extract the contents of an XML tag and compare it to a predefined value. In the report we have generated OK if the value of XML tag matches the value being tested.



List of values that can be tested:



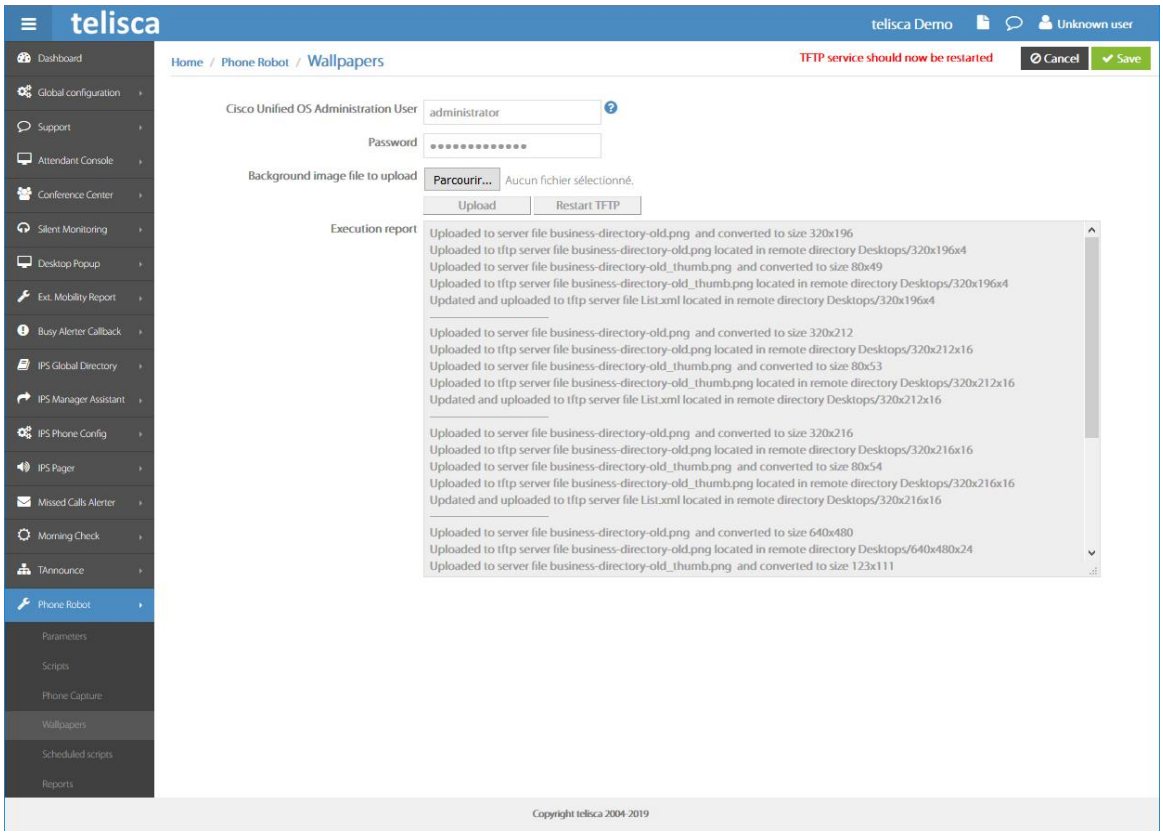
2.3 IP Phone screen background upload

This screen is accessible from Phone Robot menu, 'Wall paper' tab.

Phone Robot ease the task to load a new background screen on the TFTP server to make it available to IP Phones.

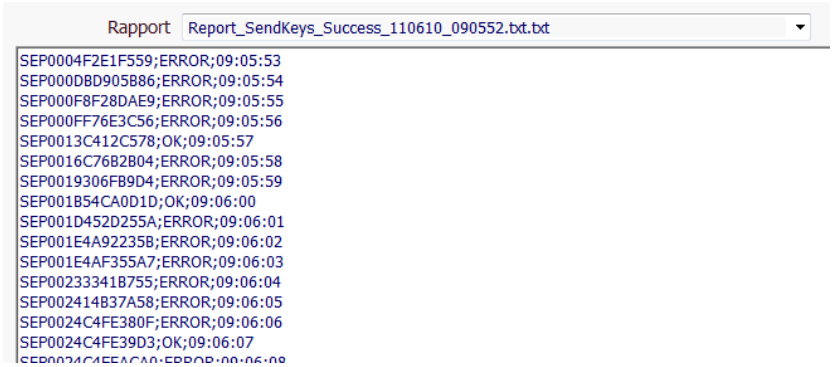
It adapts the size and colors to the different models, upload the image as well as the thumb images and update the XML list files. It is also possible to reset the TFTP from Phone Robot.

You need to enter a login & password suitable to log-in the Cisco Unified OS Administration.



2.4 Reports

It displays reports of the execution, indicating the time of execution, the IP Phone, the result of execution. Each execution report is stored in a text file with a suffix of the date and time, selectable from the administration.

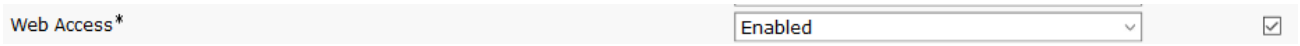

Rapport
Report_SendKeys_Success_110610_090552.txt.txt
SEP0004F2E1F559;ERROR;09:05:53
SEP000DBD905B86;ERROR;09:05:54
SEP000F8F28DAE9;ERROR;09:05:55
SEP000FF76E3C56;ERROR;09:05:56
SEP0013C412C578;OK;09:05:57
SEP0016C76B2B04;ERROR;09:05:58
SEP0019306FB9D4;ERROR;09:05:59
SEP001B54CA0D1D;OK;09:06:00
SEP001D452D255A;ERROR;09:06:01
SEP001E4A92235B;ERROR;09:06:02
SEP001E4AF355A7;ERROR;09:06:03
SEP00233341B755;ERROR;09:06:04
SEP002414B37A58;ERROR;09:06:05
SEP0024C4FE380F;ERROR;09:06:06
SEP0024C4FE39D3;OK;09:06:07

3 Appendix

3.1 Push IP Phone by HTTP settings

3.1.1 Set Web enabled option on the IP Phones

In CUCM administration, set the parameter 'Web Access' to 'Enabled' for every destination phones.



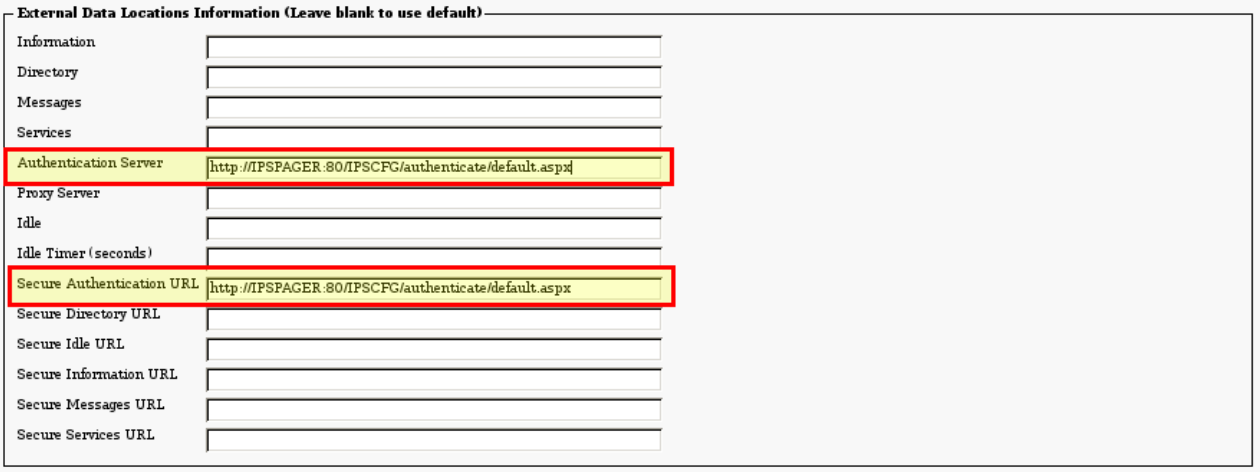
This can be changed globally by setting it in 'Common Phone Profile' and applying the updated Common Phone Profile by CCMBAT.

Note: Web Access is secured by our 'Authentication Proxy' (see after).

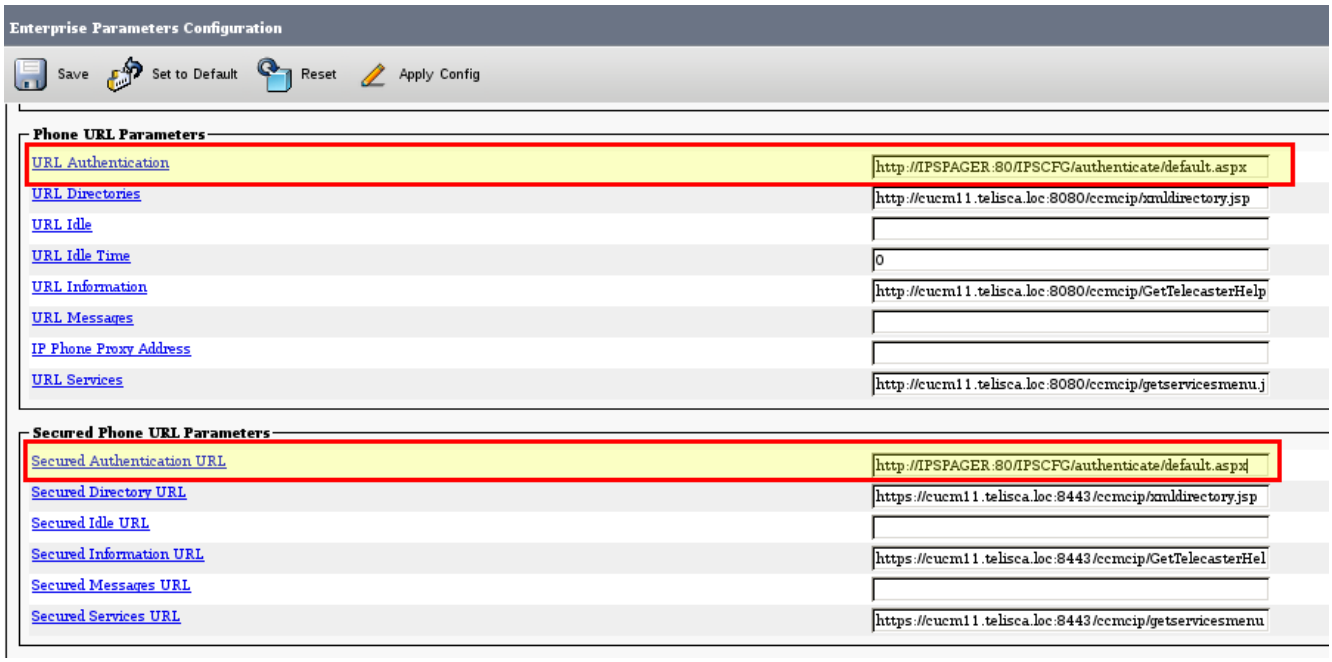
3.1.2 Change IP Phone's authentication URL

The authentication URL needs to be changed to redirect the authentication request to IPS Pager server instead of CUCM.

This can be done for test on the device setting or globally in Enterprise parameters.



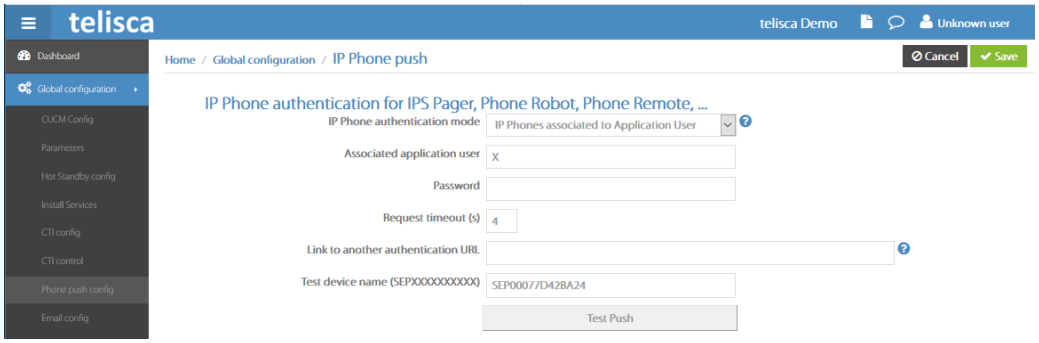
The new URL should be http://ipsPagerHost:80/IPSCFG/authenticate/default.aspx . If HTTPS support has not been configured in telisca and CUCM (see Install & Exploitation guide IPSCFG_ADMIN_EN.pdf), then you can force the HTTP URL on the Secured Phones URL Parameters as well.



The IP phones need to be restarted to take into account the change.

3.1.3 telisca Push setting configuration

From Global Configuration menu, Push Config folder, select the Push mode 'User secure authenticate proxy'.



The user login and password is disabled. IPS Pager will generate a one-time user and password.

You can configure the CUCM Host to the CUCM Publisher, so that the authentication is redirected to CUCM if the user is not the one pushed by a telisca application.

The authentication is normally very fast (a few milliseconds) however is the server is 100% busy by pushing with a too high number of threads, it can be usefull to accept a few seconds for the timeout.

You can test the authentication by entering a phone name (MAC address), after validating the configuration. It should display the services menu on the phone. If this does not work, please check the Web Access settings and authentication URL. If it still does not work, you can check the authentication logs from Support Menu, Application logs folder. If you do not see the authentication request in the logs, this may be a problem with one of the previous CUCM settings.