Administrators Guide

telisca Phone Remote

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 Product description

1.1 Administration Tools Bundle

This product is part of the range of administration tools offered by telisca. Installed on a single server, these applications are useful for administering, monitoring and operating the Cisco telephony infrastructure.
- Morning Check: Anticipates failures on the CUCM cluster by performing tests and notifying the operation / administration team in the event of an error.
- Phone Robot: Launches a series of keys in mass on the telephones of the cluster. Very handy for removing CTL or changing wallpapers on a large number of phones in an instant.
- Delog Relog: Disconnects the "mobility extension" from all users and reconnects them to the same stations later. May be useful during migration but also to improve cluster security.

These applications can be ordered all together as a bundle.

1.2 Description

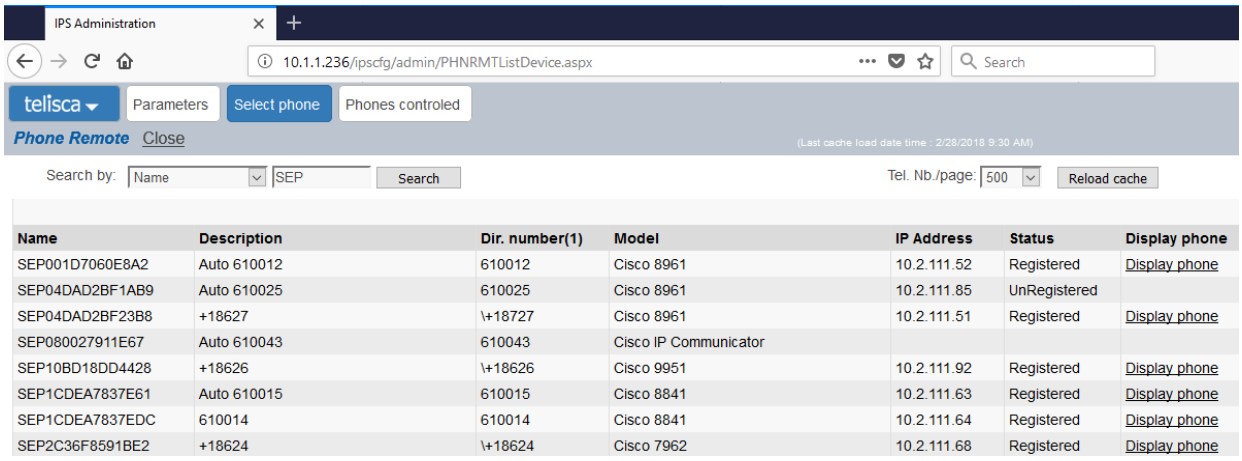
telisca Phone Remote is an application that allows the administrator to take control of a Cisco IP phone remotely. The administrator can see the phone screen and launch keys on the phone.

It will enable operations teams to offer remote support to telephony users. It allows the administrator to check configuration changes. It is useful to collect phone copies in order to create a user guide.

The various remote actions possible thanks to Phone Remote:
- Use all the keys accessible on the keyboard (directory key, messaging, transfer, conference ...),
- Use the soft keys,
- Use the line / Speed Dials keys,
- Send the procedure to restart or reset the phone,
- Dial a number from the phone,
- Login/logout from a user in "extension mobility" on a phone.

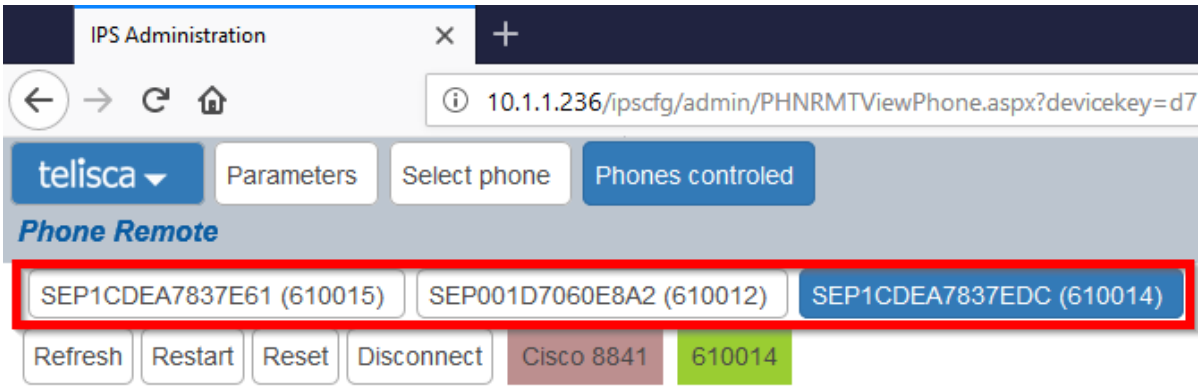
Each time you send a remote key, the screen automatically updates. The administrator can therefore easily check the result of his action.

A dedicated menu makes it easy to search for phones: by identifier (MAC), line number, description, phone model or IP address. Remote control of the phone is possible with one click.



Name	Description	Dir. number(1)	Model	IP Address	Status	Display phone
SEP001D7060E8A2	Auto 610012	610012	Cisco 8961	10.2.111.52	Registered	Display phone
SEP04DAD2BF1AB9	Auto 610025	610025	Cisco 8961	10.2.111.85	UnRegistered	
SEP04DAD2BF23B8	+18627	\+18727	Cisco 8961	10.2.111.51	Registered	Display phone
SEP080027911E67	Auto 610043	610043	Cisco IP Communicator			
SEP10BD18DD4428	+18626	\+18626	Cisco 9951	10.2.111.92	Registered	Display phone
SEP1CDEA7837E61	Auto 610015	610015	Cisco 8841	10.2.111.63	Registered	Display phone
SEP1CDEA7837EDC	610014	610014	Cisco 8841	10.2.111.64	Registered	Display phone
SEP2C36F8591BE2	+18624	\+18624	Cisco 7962	10.2.111.68	Registered	Display phone

In addition, several phones can be controlled at the same time. Controlled phones are all accessible from a single menu. The control for each phone can be manually stopped at any time or automatically after a predefined period of inactivity.



The telisca solution administrator can allow an operator role to be defined in the application to allow only the access to the phone control functionality to identified individuals. The operating role does not allow changes to the telisca server configurations or the global settings of Phone Remote.

1.3 Architecture

The architecture is based on a telisca IPS Framework & Administration modules. Keys are sent via http requests.

The application automatically enables the "Web Access" on the phone when the administrator takes control of the phone remotely. It is disabled when the administrator logs out or after a period of inactivity.

Two methods of access authorization are possible. Either the authentication requests are handled by the telisca server Secured Authentication Proxy, which give access to the phones for a limited time thanks to a temporary user / password.

Otherwise, the authentication can be managed by the CUCM. Then the application authenticates via an "Application User". The association with the Application User is processed automatically by Phone Remote. When the phone control is stopped the application disassociates the phone from the user.

1.4 Requirements

- 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

1.4.1 CUCM

Supported CUCM Versions
CUCM versions 10.5 to 14 are supported.

CUCM configuration
Choose from the following:
- Create a user application
- Or modify the authentication URLs of the CUCM to user telisca Secured Proxy.

Supported phones
Cisco 6921, 6941, 6945, 6961, 7811, 7821, 7841, 7861, 7937, 7937G, 7940 / 7940G, 7941 / 7941G / 7941G-E, 7942 / 7942G, 7960 / 7960G, 7961 / 7961G / 7961G-GE, 7962 / 7962G, 7945 / 7945G, 7965 / 7965G, IP Communicator, 7970, 7971 / 7971G-GE, 7975 / 7975G, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, 8941, 8945, 9961, 9951, 9971

2 Administration

2.1 Server installation

The installation of the Phone Remote server application is done via the telisca global setup.
A license file is required for the installation of the server application.

All pre-requisites for telisca applications are automatically checked and installed by the telisca setup.

Note: For more information, please refer to the Installation and Operation Guide
http://telisca.com/docs/IPSCFG_ADMIN_EN.pdf

2.2 Server Administration

Configuration of telisca server applications is done from a web browser.

The url is as follows:

- http://<IP_telisca_server>/<instance_telisca_server>/ipscfg/admin/default.aspx
- https://<IP_telisca_server>/<instance_telisca_server>/ipscfg/admin/default.aspx

Access to the telisca administration is protected by login / password Windows.

The user account used for administration must be:

- The local administrator account of the server.
- A user account ("telisca_admin" for example) belonging to the "teliscaAdmin" group, previously created on the server.
- Security groups can be created on the AD domain, if the telisca server (s) is one of them.

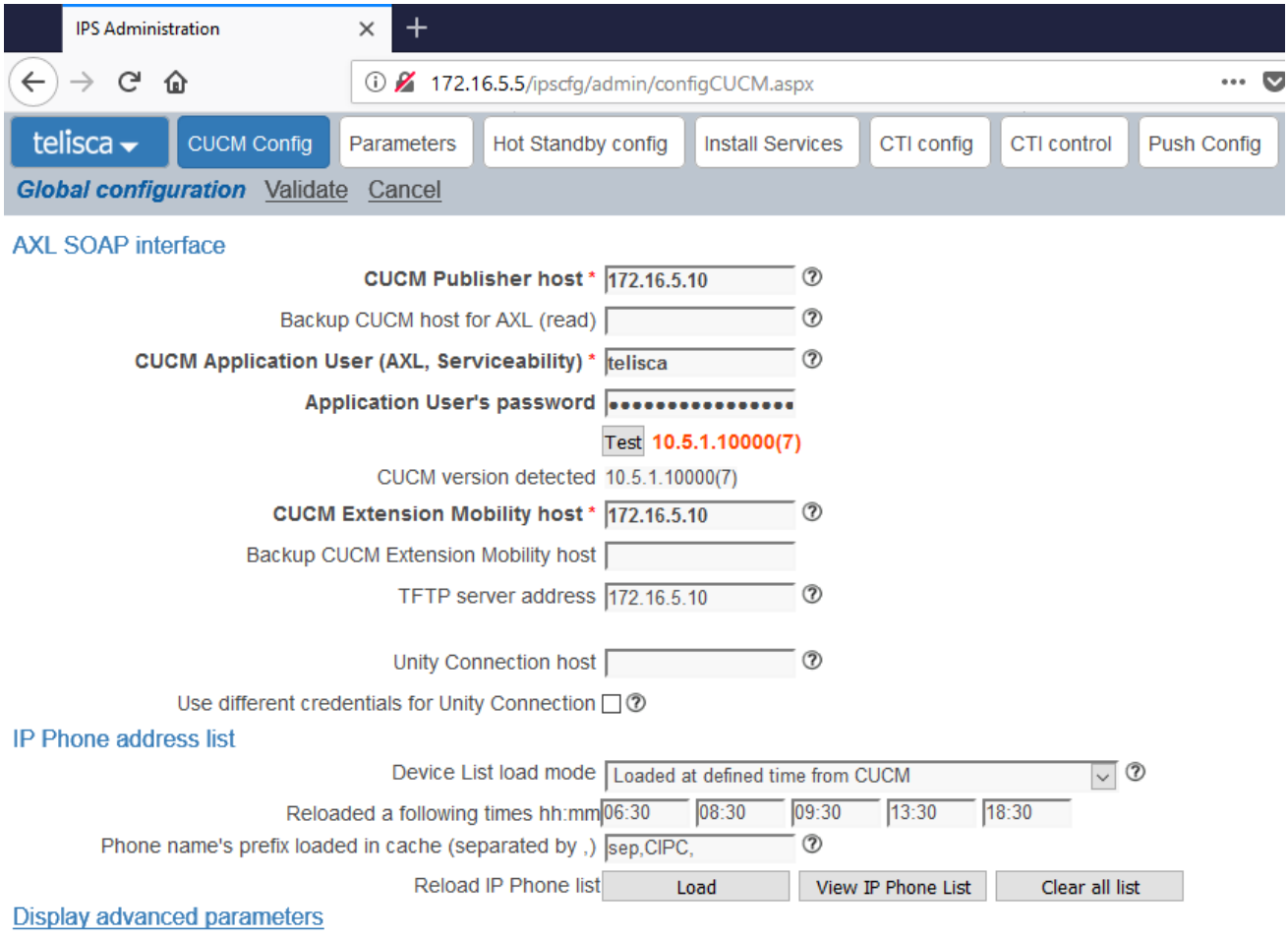
2.3 Global configuration - telisca server

From the administration interface, it will be necessary to configure at least the following global parameters.
For more information on global configuration, see the IPSCFG_ADMIN_EN and IPSFT_ADMIN_EN administration guide (for installing two fault-tolerant servers).

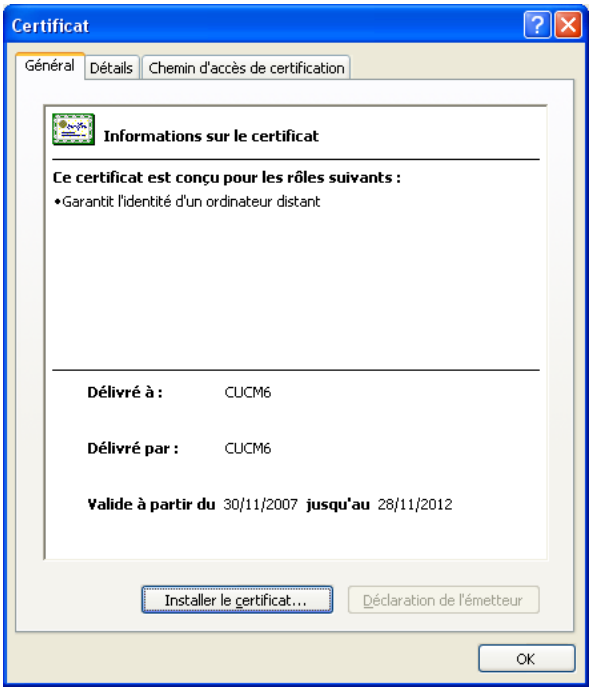
2.3.1 CUCM Config

- The IPv4 address or DNS name (recommended) of the CUCM Publisher server.
- The login and password of the User application belonging to the following groups
- Standard Super User (or a group that includes the AXL SOAP Write roles, SERVICEABILITY, EM Proxy user)
- Standard EM Authentication Proxy Rights
- The IPv4 address or DNS name (recommended) of the CUCM Extension Mobility Server.

Once these parameters have been entered, care should be taken to "test" the connection and check that the version of the CUCM obtained is correctly displayed, and then validate the configuration screen.



Note: To avoid problems of response time due to SSL authentication, it is advisable to install the SSL certificate of the CUCM publisher on the telisca server. To do this, simply call the CUCM administration from Internet Explorer, using the DNS name of the CUCM server, then by right-clicking in the address box in red or on the padlock, to display the certificate and install it.

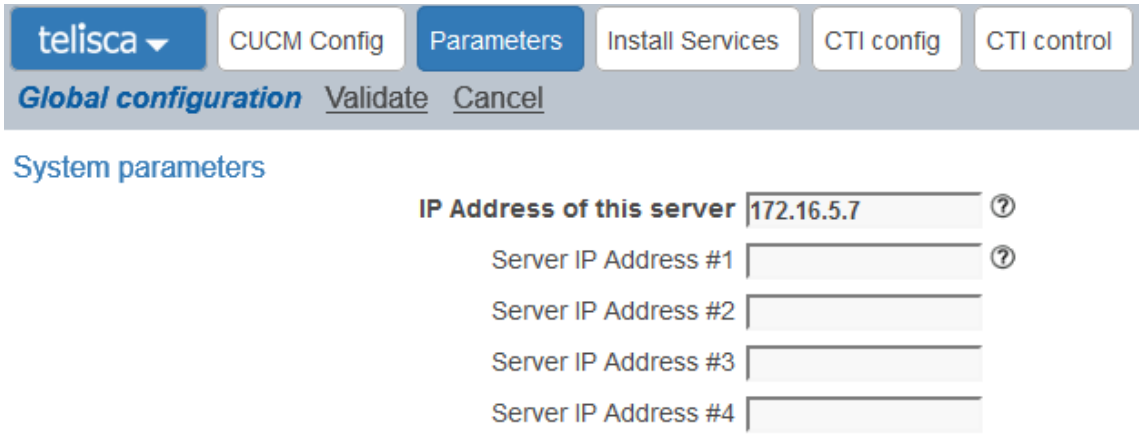


Note: For more information, please refer to the Installation and Operation Guide http://telisca.com/docs/IPSCFG_ADMIN_EN.pdf

2.3.2 Parameters

In the Parameters screen of the Global Configuration menu. Only one minimum parameter is required.

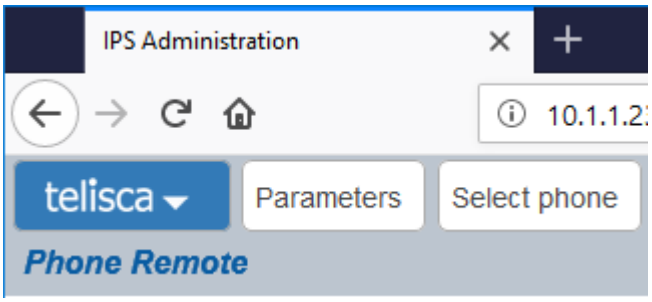
- IP address of this physical machine.



Note: For more information, please refer to the Installation and Operation Guide http://telisca.com/docs/IPSCFG_ADMIN_EN.pdf

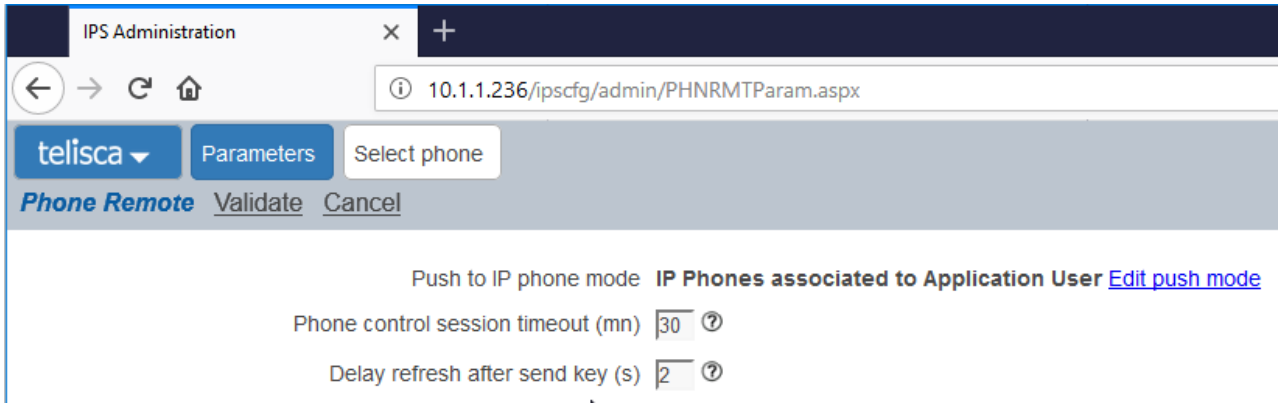
3 telisca Server Configuration for Phone Remote

Select Phone Remote menu.



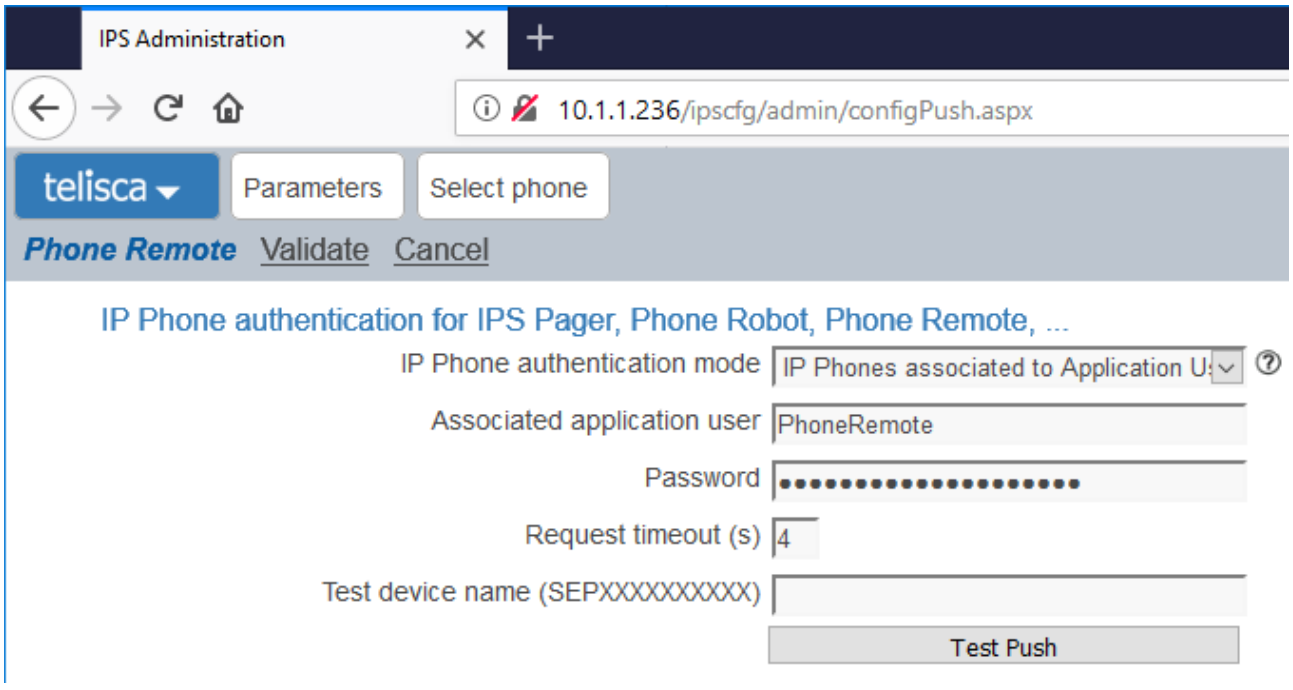
3.1 Parameters

Phone Remote Parameters screen allows you to define the various general parameters of the application.



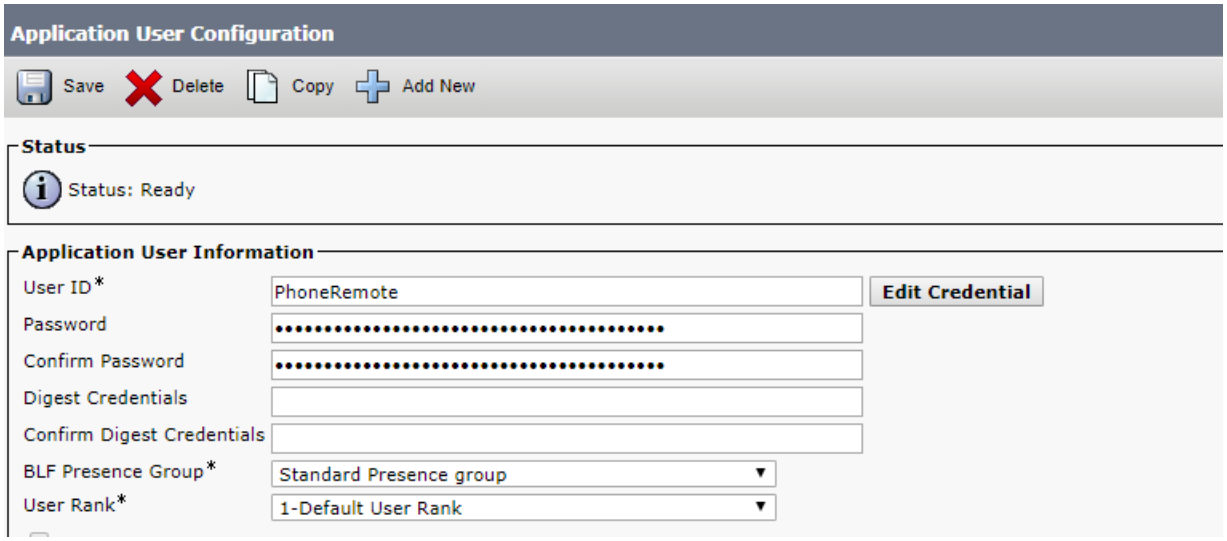
3.1.1 Push mode to IP Phone

Choose the authentication method of the application.
2 choices are available:



3.1.1.1 IP Phones associated with a CUCM Application User

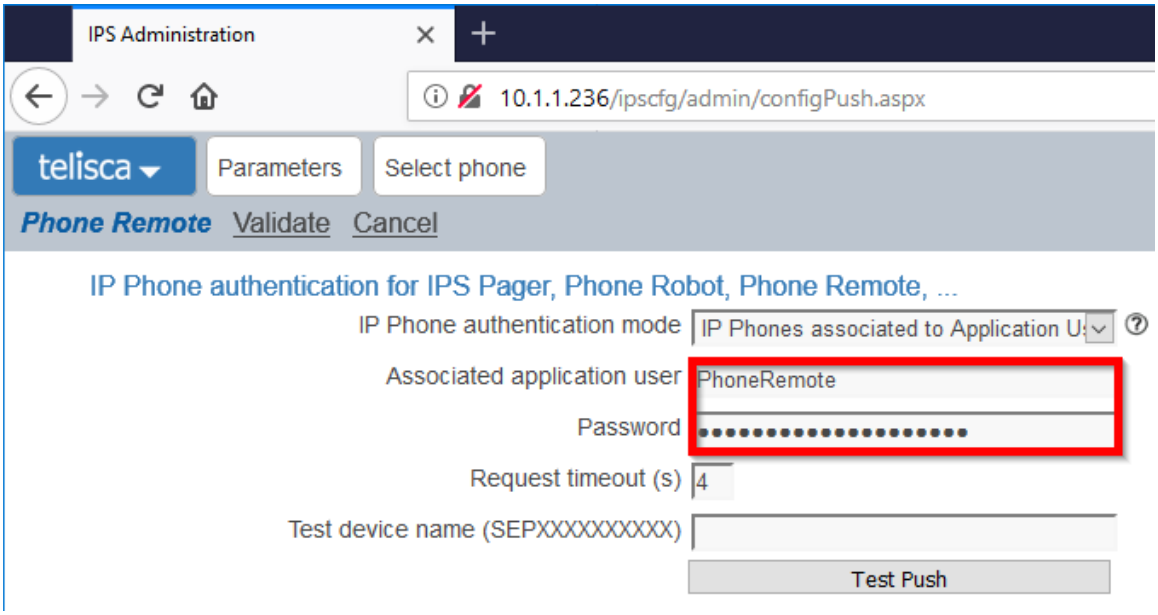
The first authentication method requires to create a user application on the CUCM:
User Management> Application User> Add



Create an Application User (for example PhoneRemote) with a password (will be used in the configuration of the telisca application).

This method is dynamic. For authentication to be possible, it is mandatory for the phone to be associated with the user (user application). When a request for supervision by the operator, the telisca server associates the phone with the user automatically. At the end of the supervision, the phone is disassociated from the user.

After creating the user application, just enter it in the telisca interface with its name and password:

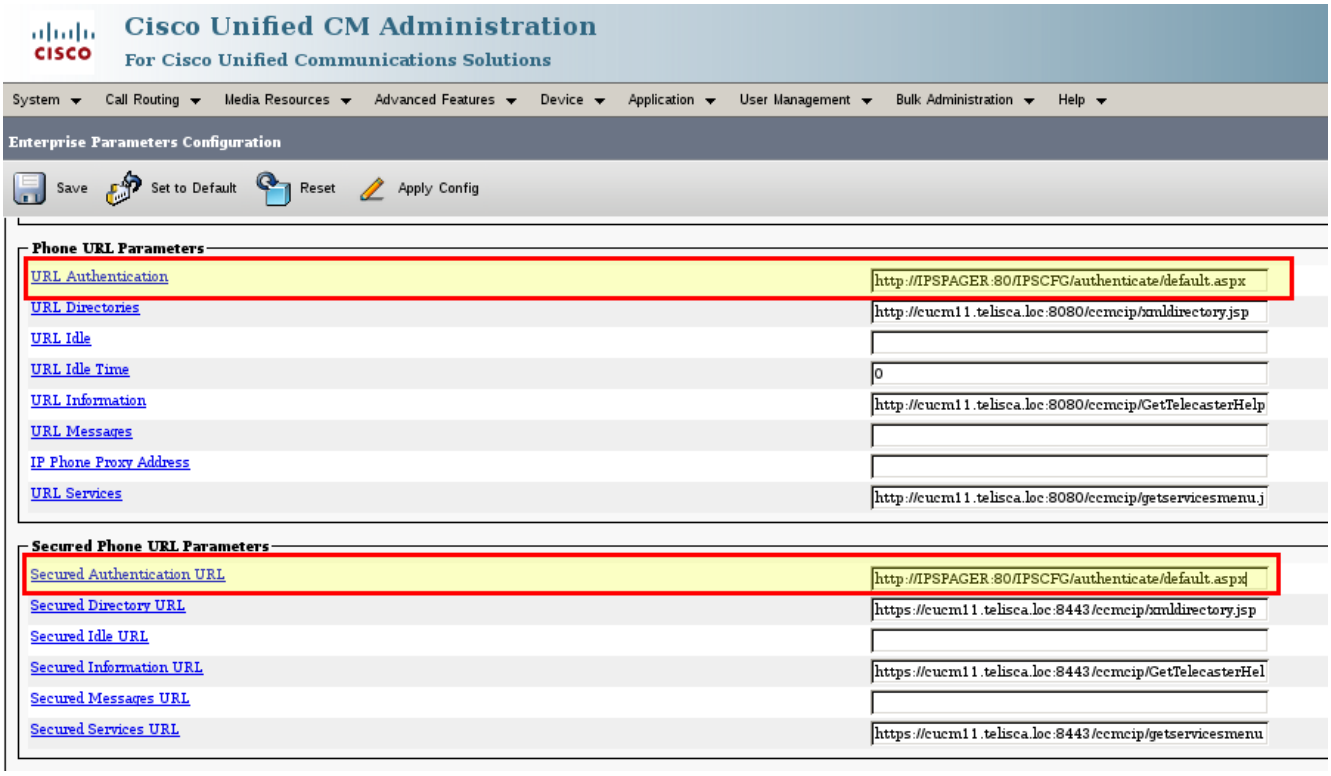


3.1.1.2 Using a secure Auhentication Proxy

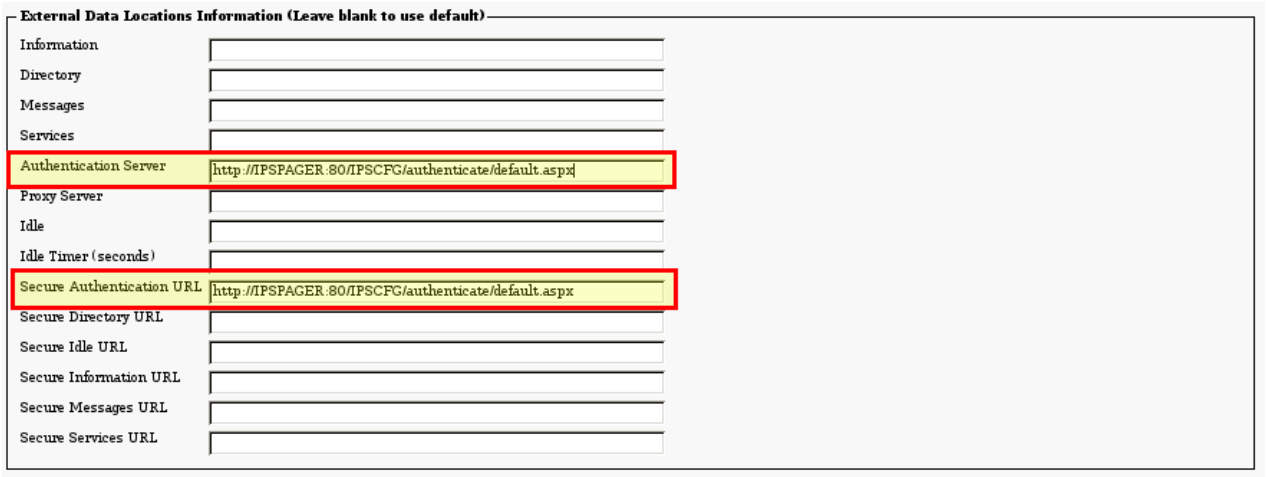
The second authentication method is to redirect the authentication requests to the telisca server. This solution is more efficient and more secure (use of a password generated according to the time). Its implementation requires a "restart" IP Phones to support the change of authentication URL. The new authentication URL takes the form: http: // <telisca_server_server>: 80 / IPSCFG / authenticate / default.aspx.

The authentication URL can be configured in two ways on the CUCM:

- Global configuration (accessible via System / Enterprise parameters):



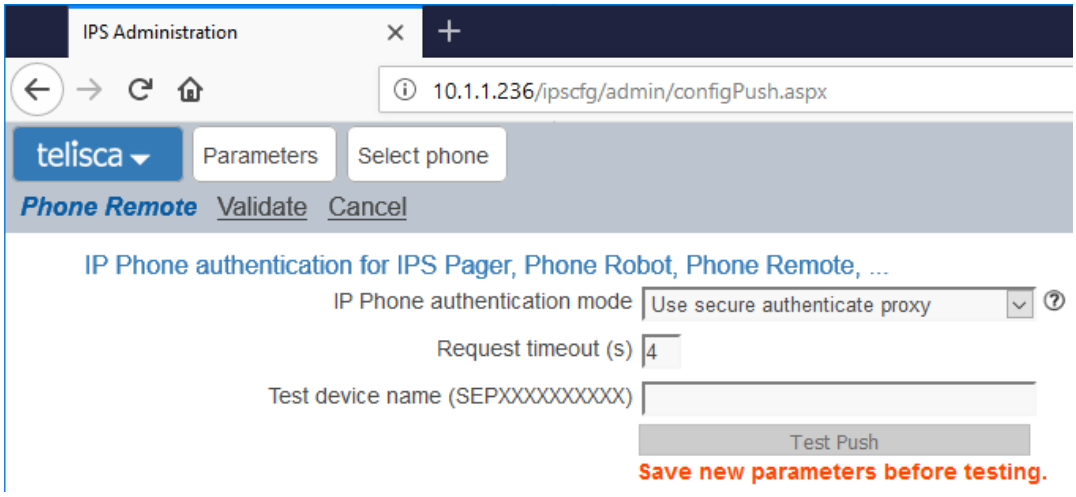
- Local configuration of the IP Phone:



NOTE: If the "Secure Authentication URL" is configured in HTTPS, the SSL certificate used by the Telisca server must be installed on the CUCM as a "Phone-Trust" certificate.

If the configuration is made globally, it will be valid on all existing phones but also future additions.

On the telisca server, change the authentication mode to "Secure Proxy Usage" and press OK.



3.1.2 Session control phone time

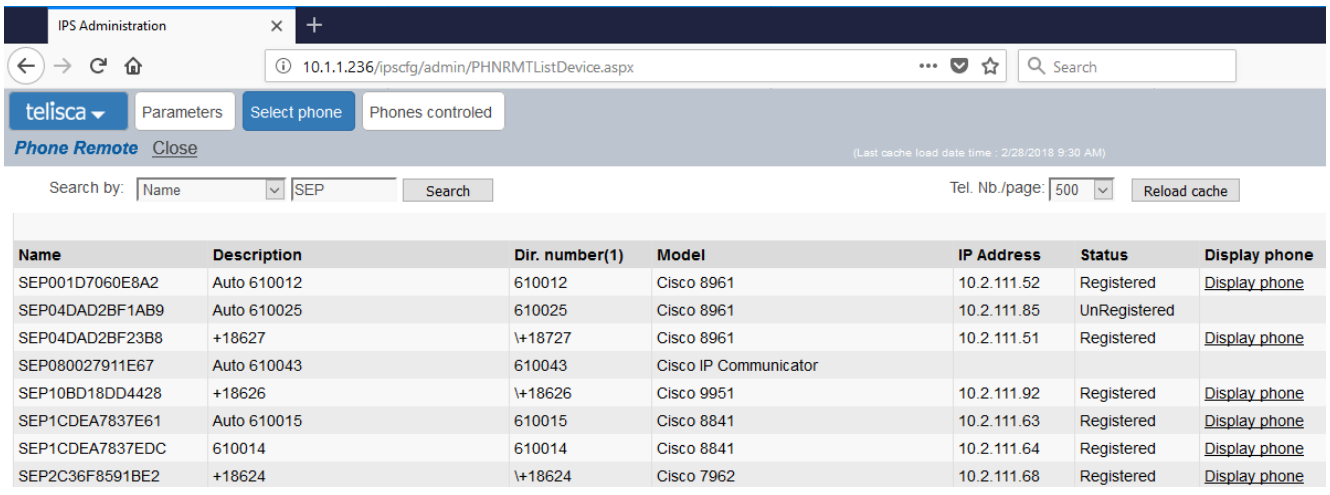
The application will automatically close the session after a given time. The phone will disappear from the "Phones Controlled" page. The control procedure will have to be restarted by the administrator for this phone.

3.1.3 Refresh time display after sending key

Each time a key is sent, the phone screen may change. The reloading of the new screen can be done automatically after sending a key.
Note: At any time, the administrator can refresh the screen manually with a dedicated button.

3.2 Phone selection

This menu allows you to list all the telephones supervised by the telisca server.



Name	Description	Dir. number(1)	Model	IP Address	Status	Display phone
SEP001D7060E8A2	Auto 610012	610012	Cisco 8961	10.2.111.52	Registered	Display phone
SEP04DAD2BF1AB9	Auto 610025	610025	Cisco 8961	10.2.111.85	UnRegistered	
SEP04DAD2BF23B8	+18627	\+18727	Cisco 8961	10.2.111.51	Registered	Display phone
SEP080027911E67	Auto 610043	610043	Cisco IP Communicator			
SEP10BD18DD4428	+18626	\+18626	Cisco 9951	10.2.111.92	Registered	Display phone
SEP1CDEA7837E61	Auto 610015	610015	Cisco 8841	10.2.111.63	Registered	Display phone
SEP1CDEA7837EDC	610014	610014	Cisco 8841	10.2.111.64	Registered	Display phone
SEP2C36F8591BE2	+18624	\+18624	Cisco 7962	10.2.111.68	Registered	Display phone

It is possible to search for a particular phone. To start the remote control of the phone, click on "Show Phone".

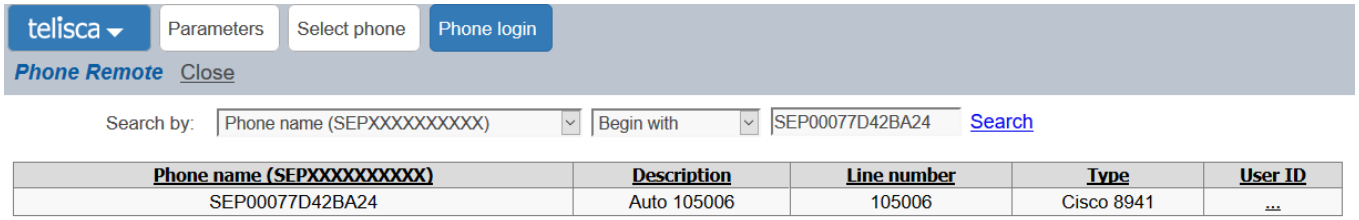
3.3 Phones controlled

After starting the control of a phone, several actions are possible:
- Refresh: Reload the screen display manually
- Restart: Starts the phone restart procedure as it exists on the CUCM.
- Reset: Starts the phone reset procedure as it exists on the CUCM.
- Disconnect: Stops the control of this phone.
- Calls: Directly dials the filled phone number in the text field.

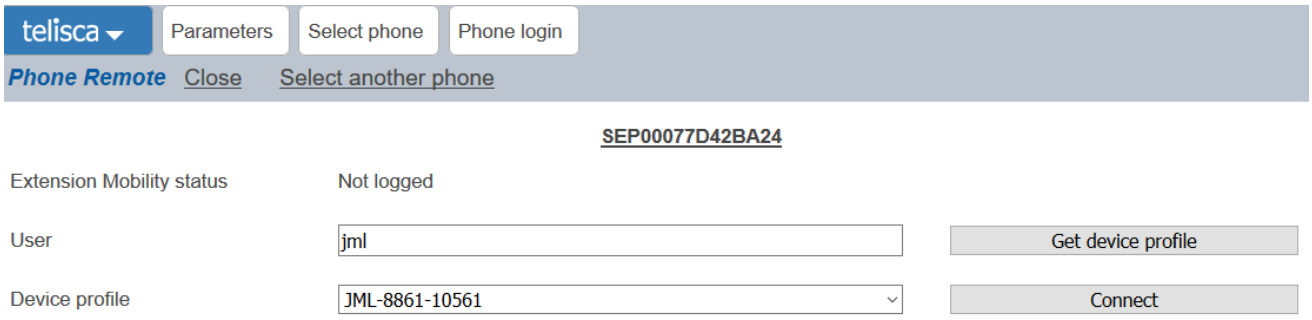
All keys on the phone (digital, messaging, phonebook ...) and around the screen are functional and can be launched remotely. The screen refreshes automatically after pressing a button (see chapter 4.1.3).

3.4 Login / logout Extension Mobility

From the Phone Login tab it is possible to select an IP Phone, by its identifier (MAC address), its line number or its description.



If the phone is not logued in Extension Mobility, the displayed UserID is replaced by .... By clicking on the hyperlink ... we display the screen below, which allows to connect a user.



By entering the UserID CUCM, then clicking on the button Get Device profile we get the list of associated device profiles, then we can login it to the phone.

If the phone is already connected, the connected UserId is displayed in the search result. By clicking on the UserId link, you can logout the user from the phone.

4 Troubleshooting

The most common error when trying to control a phone is the authentication error: Cisco error #4

This error is due to an authentication problem. Depending on your authentication method, please check:
1- If the password of the user application is still valid.
2- If the authentication URL on the "enterprise parameter" has not been modified.
3- If the authentication url on the device has not been modified.