Administrators Guide telisca Phone Remote

Directory

Phone Directory Jabber UDS Server Web Directory IPS Popup / Reverse Lookup Personal Directory H350 Video Confdirectory Corporate Speed Dials ClickNDial Alerting Voice Alert **IPS** Pager Admin tools Morning Check Phone Remote Phone Robot Provisioning Phone Deployment CMS Admin & Selfcare Extension Mobility Report Manager Assistant IP Phone / Jabber Interface

Productivity tools IPS Phone Config IPS Alarm Callback **IPSLock** Wakeup Call Missed Call Alerter Conference Center Busy Alerter Callback Desktop Popup **Finesse Gadgets** Spark Bot Attendant Console / IVR / Group Tannounce Line Group Manager SilentMonitoring **Extension Mobility tools** TSSO Delog/Relog Pin & Password Manager Recording Call Recording **Recording Notification**

SUPPORT@TELISCA.COM TEL. +33 (0)1 46 45 05 12



HELP

Open a ticket with your logs on <u>http://support.telisca.com</u> for a prompt and efficient response! Server: <u>MENU>Support>Zip Logs</u>

Summary

	1	PRODUCT DESCRIPTION	3
1.1 1.2	AdM DES	AINISTRATION TOOLS BUNDLE	3
1.3	ARC	CHITECTURE	4
1.4 <i>1.4.1</i>	Req / C	QUIREMENTS	5 .5
	2	ADMINISTRATION	6
2.1	SER	VER INSTALLATION	6
2.2	SER	VER ADMINISTRATION	6
2.3	Glo	DBAL CONFIGURATION - TELISCA SERVER	6
2.3.1		CUCM Config	.6
2.3.2	? F	Parameters	8
	3	TELISCA SERVER CONFIGURATION FOR PHONE REMOTE	9
3.1	Par	AMETERS	9
3.1.1	l A	Push mode to IP Phone	.9
3.1.2	? 5	Session control phone time	2
3.1.3	8 F	Refresh time display after sending key	2
3.2	Рнс	DNE SELECTION	2
3.3	Рнс	DNES CONTROLLED	3
3.4	Log	SIN / LOGOUT EXTENSION MOBILITY	3
	4	TROUBLESHOOTING1	5

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.

IPS Administration	IPS Administration X +						
← → C' ŵ	i 10.1.1.236/ipscfg/admin/PHN	RMTListDevice.aspx			🛡 🟠 🔍 Se	arch	
telisca 🗸 🛛 Paramet	ers Select phone Phones controled						
Phone Remote Close							
Search by: Name V SEP Search Tel. Nb./page: 500 V Reload cache			cache				
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.

IPS Administration	× +
← → ♂ û	10.1.1.236/ipscfg/admin/PHNRMTViewPhone.aspx?devicekey=d7
telisca - Parameters	Select phone Phones controled
Phone Remote	
SEP1CDEA7837E61 (610015)	SEP001D7060E8A2 (610012) SEP1CDEA7837EDC (610014)
Refresh Restart Reset Dis	connect Cisco 8841 610014

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 <u>http://telisca.com/docs/IPSCFG_ADMIN_EN.pdf</u>

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.

telisca

IPS Administration	× +					
$\overleftarrow{\bullet}$ \rightarrow $\overleftarrow{\bullet}$	i 🔏 172.1	6.5.5/ipscfg/admin/con	figCUCM.aspx			🖸
telisca - CUCM Config	Parameters	Hot Standby config	Install Services	CTI config	CTI control	Push Config
Global configuration Validate	e <u>Cancel</u>					
AXL SOAP interface						
	CUCM Publ	isher host * 172.16.5	.10 ⑦			
Backu	p CUCM host fo	or AXL (read)	0			
CUCM Application U	ser (AXL, Serv	viceability) * telisca	0			
Арр	lication User	s password				
		Test 10.	5.1.10000(7)			
	CUCM vers	sion detected 10.5.1.10	000(7)			
CUCM	Extension Mo	bility host * 172.16.5	.10 ⑦			
Backup Cl	UCM Extension	Mobility host				
	TFTP se	rver address 172.16.5	.10 ⑦			
	Unity Cor	nnection host	0			
Use different cred	lentials for Unit	y Connection 🗌 🕐				
IP Phone address list						
	Device Li	st load mode Loaded	at defined time from (CUCM	\sim	0
Reloa	ded a following	times hh:mm06:30	08:30 09:30	13:30	18:30	
Phone name's prefix loade	ed in cache (se	parated by ,) sep,CIPC	C, ⑦			
	Reload	IP Phone list	.oad View	IP Phone List	Clear all lis	st
Display advanced parameters						

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.

Certificat	? 🛛					
Général Détails Chemin d'a	Général Détails Chemin d'accès de certification					
Informations sur le certificat Ce certificat est conçu pour les rôles suivants : •Garantit l'identité d'un ordinateur distant						
Délivré à :	CUCM6					
Délivré par :	CUCM6					
¥alide à partir du	30/11/2007 jusqu'au 28/11/2012					
Installer	le <u>c</u> ertificat					
	ОК					

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



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.

telisca 🗸	CUCM Config	Parameters	Install Services	CTI config	CTI control
Global configu	ration Validat	te <u>Cancel</u>			
System parame	ters				
		IP Address of	this server 172.1	6.5.7	0
		Server IP	Address #1		0
		Server IF	Address #2		
		Server IF	Address #3		1
		Server IF	Address #4		1

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



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.

IPS Administration	× +
← → ♂ ✿	10.1.1.236/ipscfg/admin/PHNRMTParam.aspx
telisca - Parameters S	Select phone
Phone Remote Validate Can	<u>ncel</u>
Phone	Push to IP phone mode IP Phones associated to Application User Edit push mode
Dela	ay refresh after send key (s) 2 0

3.1.1 Push mode to IP Phone

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

IPS Administration	× +				
\leftarrow \rightarrow C \textcircled{a}	③				
telisca - Parameters Se	elect phone				
Phone Remote Validate Cano	<u>cel</u>				
IP Phone authentication fo IP Ph As	IP Phone authentication for IPS Pager, Phone Robot, Phone Remote, IP Phone authentication mode IP Phones associated to Application U: Associated application user PhoneRemote Password				
	Request timeout (s) 4				
Test device	name (SEPXXXXXXXXX) Test Push				



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

	Application User Configuration					
	🔚 Save 🗙 Delete 🕞 Copy 🕂 Add New					
I	Status					
	i Status: Ready					
	-Application User Informa	tion				
	User ID*	User ID* PhoneRemote Edit Credential				
	Password					
	Confirm Password					
	Digest Credentials					
Confirm Digest Credentials						
	BLF Presence Group* Standard Presence group					
	User Rank* 1-Default User Rank					
1	_					

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:

IPS Administration	× +
$\overleftarrow{\leftarrow}$ > C $\widehat{\mathbf{G}}$	🛈 🔏 10.1.1.236/ipscfg/admin/configPush.aspx
telisca - Parameters S	elect phone
Phone Remote Validate Can	cel
IP Phone authentication for	r IPS Pager, Phone Robot, Phone Remote,
IP P	hone authentication mode \square Phones associated to Application U \checkmark \textcircled{O}
A	ssociated application user PhoneRemote
	Password
	Request timeout (s) 4
Test device	name (SEPXXXXXXXXXX)
	Test Push

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):

CISCO Unified CM Administration For Cisco Unified Communications Solutions	
System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management	▼ Bulk Administration ▼ Help ▼
Enterprise Parameters Configuration	
🔚 Save 🧀 Set to Default 🏻 🎦 Reset 🏒 Apply Config	
Phone URL Parameters	
URL Authentication	http://IPSPAGER:80/IPSCFG/authenticate/default.aspx
URL Directories	http://cucm11.telisca.loc:8080/ccmcip/xmldirectory.jsp
URL Idle	
URL Idle Time	0
URL Information	http://cucm11.telisca.loc:8080/ccmcip/GetTelecasterHelp
URL Messages	
IP Phone Proxy Address	
URL Services	http://cucm11.telisca.loc:8080/ccmcip/getservicesmenu.j
Secured Phone TIRI Parameters	
Secured Authentication URL	http://JPSPACER.80/JPSCEC/authenticate/default.acmy
Secured Directory URL	https://cuem11_telisea.loc.8443/cemein/ymldirectory.isn
Secured Idle URL	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
Secured Information URL	https://cucm11.telisca.loc:8443/ccmcip/GetTelecasterHel
Secured Messages URL	
Secured Services URL	https://cucm11.telisca.loc:8443/ccmcip/getservicesmenu

• Local configuration of the IP Phone:

– External Data Locations In	itormation (Leave blank to use default)	
Information		
Directory		
Messages		
Services		
Authentication Server	http://IPSPAGER:80/IPSCFG/authenticate/default.aspx	
Proxy Server		-
Idle		
Idle Timer (seconds)		
Secure Authentication URL	http://IPSPAGER:80/IPSCFG/authenticate/default.aspx	
Secure Directory URL		
Secure Idle URL		
Secure Information URL		
Secure Messages URL		
Secure Services URL		

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.

telisca

IPS Administration	× +
← → ♂ ✿	10.1.1.236/ipscfg/admin/configPush.aspx
telisca - Parameters Se	elect phone
Phone Remote Validate Can	cel
IP Phone authentication fo	or IPS Pager, Phone Robot, Phone Remote, hone authentication mode Use secure authenticate proxy 🗸 ⊄
	Request timeout (s) 4
Test device	e name (SEPXXXXXXXXX)
	Test Push
	Save new parameters before testing.

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.

IPS Administration	× +						
← → ♂ @	10.1.1.236/ipscfg/admin/PHNRMTListDevice.aspx				Search		
telisca - Parameters Select phone Phones controled							
Phone Remote Close (Last cache load date time : 2/28/2018 9:30 AM)							
Search by: Name	Search by: Name V SEP Search Tel. Nb./page: 500 V Reload cache						
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".

telisca

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.



telisca - Parameters Select phone Phone login Phone Remote Close								
Search by: Phone name (SEPXXXXXXXXX) Search SEP00077D42BA24 Search								
Phone name (SEPXXXXXXXXXXXX)				Description	Line number	Type	User ID	
SEP00077D42BA24			Auto 105006	105006	Cisco 8941			

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.

telisca 🚽 🛛 Pa	arameters Se	elect phone	Phone login			
Phone Remote Close Select another phone						
				SEP00077D42BA24		
Extension Mobility st	tatus	Not logged				
User		jml			Get device profile	
Device profile		JML-8861-10	0561	~	Connect	

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.