Product Datasheet

IPS Lock

Directory
Phone Directory
Jabber UDS Server
Web Directory
IPS Popup / Reverse Lookup
Personal Directory
H350 Video Conf directory
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
IPS Lock
Wakeup Call
Missed Call Alerter
Conference Center
Busy Alerter Callback
Desktop Popup
Finesse Gadgets
Spark Bot
Attendant Console / IVR / Group
Tannounce
Line Group Manager
Silent Monitoring
Extension Mobility tools
TSSO
Delog / Relog
Pin & Password Manager
Recording
Call Recording
Recording Notification

1 IPS Lock presentation

1.1 Overview

Prevent all unauthorized calls from your Cisco IP Phone with IPS Lock. This application helps reducing premium rate calls abuse and impersonation. IPS Lock can be configured to block different categories of numbers: premium rates, international or all external numbers except emergency numbers.

The phone is locked by opening a service on the phone or by pressing a button (SURL). It can also be automatically locked on idle time and at a preset hour of the day.

To unlock their phones, users need to enter their CUCM PIN Code either on the IP Phone or through an audio menu (by DTMF) when making a blocked call (if IPS Lock is configured to reroute blocked calls to the integrated audio server).

IPS Lock can be used as an alternative for Extension Mobility or used as a complement.

The simplicity and speed of the process **encourages users to lock their phones** often or automatically.

IPS Lock can also let users change their own PIN and schedule their Call History clear up for added convenience and privacy.

IPS Lock is also included in the full IPS Phone Config Application Suite. IPS Lock can block access to an IP Phone service or the Directories service.

1.2 IPS Lock vs Extension Mobility

	IPS Lock	Extension Mobility
Inbound calls	Unaffected	Lost of forwarded to Voice Mail
Locking/Logout	Instant One key press At define time of day	Reset Access via menu
Unlocking/Logon	Instant PIN on device or audio menu At define time of day	Reset PIN or password via menu + User ID
Change PIN	Yes	Yes
Clear Call History	Option	Option

Main differences between Extension Mobility and IPS Lock

1.3 How it works

The lock can be applied in three different ways by the telisca server:

1. Calling Search Space
   IPS Lock can change the Line's or Device's Calling Search Space (CSS). The **same CSS** can be applied to all locked phones (Example: unlocked CSS: London_CSS > locked CSS: IPSLock_CSS).
   Or IPS Lock changes to a CSS which is the same as the current unlocked one **with a postfix**. (Example with "_IPSLocked" postfix: unlocked CSS=London_HQ_CSS > locked CSS=London_HQ_CSS_*IPSLocked*)

2. Translation Pattern + External Call Control Profile
   (compatible with CUCM 8.6 and above)
   The TP must block all external calls (and internal too if needed). The ECCP queries IPS Lock to check if the phone is Locked. If the phone is Locked, IPS Lock will check if the called number is in the allowed/blocked numbers lists defined by the administrator. If the call is definitely not allowed, the call is forwarded to the IPS Lock audio server which plays a warning message.

3. CTI
   All the phones using IPS Lock are CTI monitored. For every outbound call on these phones, IPS Lock decides from the administration's settings which calls are allowed or not. Blocked calls are forwarded to the audio server which plays a warning message.

With IPS Lock in modes 2 & 3, the administrator defines in telisca Administration a list of authorized phone numbers or masks and/or a list of not authorized phone numbers or masks. In these modes, IPS Lock can unlock phones temporarily (for a set duration) or permanently (until a PIN is entered in the phone menu or via the audio server). Also it provides an instant lock/unlock mechanism (no reset of the phone) and a very light load on CUCM.

1.4 User experience

IPS Lock provides functionality from Cisco IP Phones:

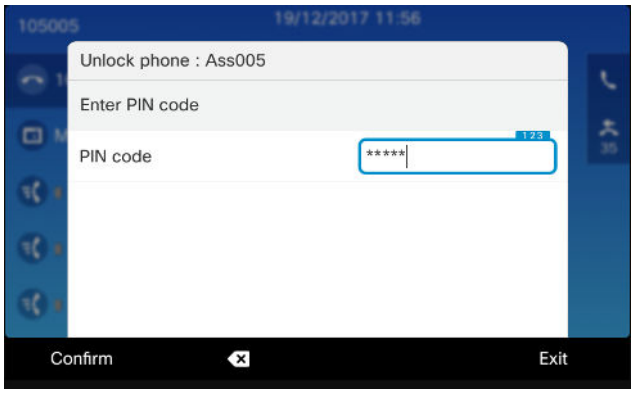
- Locking/Unlocking a phone
- Changing a PIN Code
- Calls History deletion scheduling

A locked IP Phone blocks all or some outbound calls (internal and emergency numbers can remain accessible) without affecting incoming calls. It works for all users, logged in Extension Mobility or not.

To lock a phone the user will access the service via the Service Button or by using an SURL shortcut. On first access, IPS Lock displays the detected username and can optionally prompt for a PIN. This is to make sure the users know their own PIN and won't lock themselves out forever.

Users' devices can be automatically locked after a period of inactivity. The phone will simply trigger IPS Lock when switching to idle mode. Phones can also be locked every day at specific times (outside business hours for example).

To unlock a phone, users can access the IPS Lock service on their phone and enter their PIN Code or make a call and type the PIN with DTMF on the audio server.

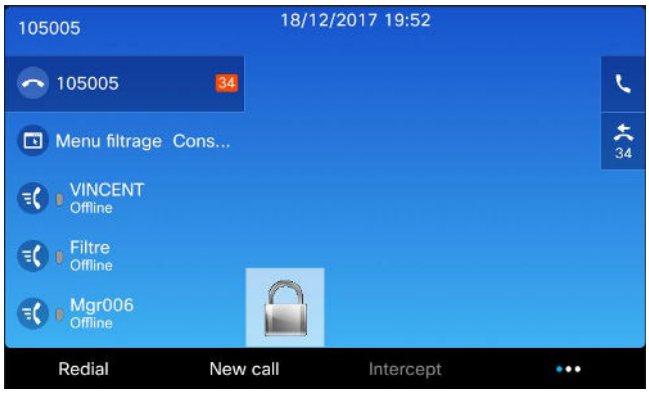


Users need to type their PIN to unlock a phone

When a phone is locked access to an IP Phone Service can be blocked. (IPS Global Directory if installed)

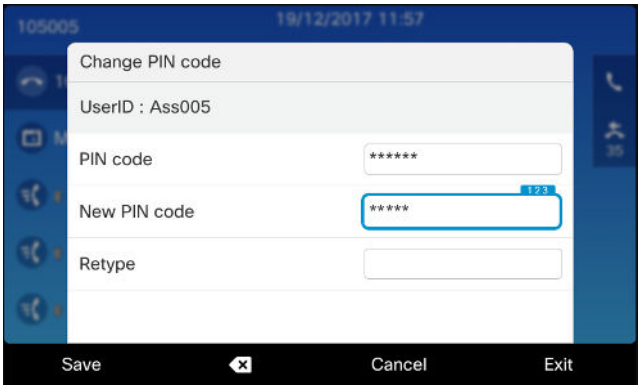
The locked status is visible on the phone with:

- A padlock icon displayed on the screen
- A modified line label (example "Locked_1044" or "1044_locked")



Lock status displayed as an icon and as a modified line label

IPS Lock also offers a way to update the PIN code from the IP Phone.



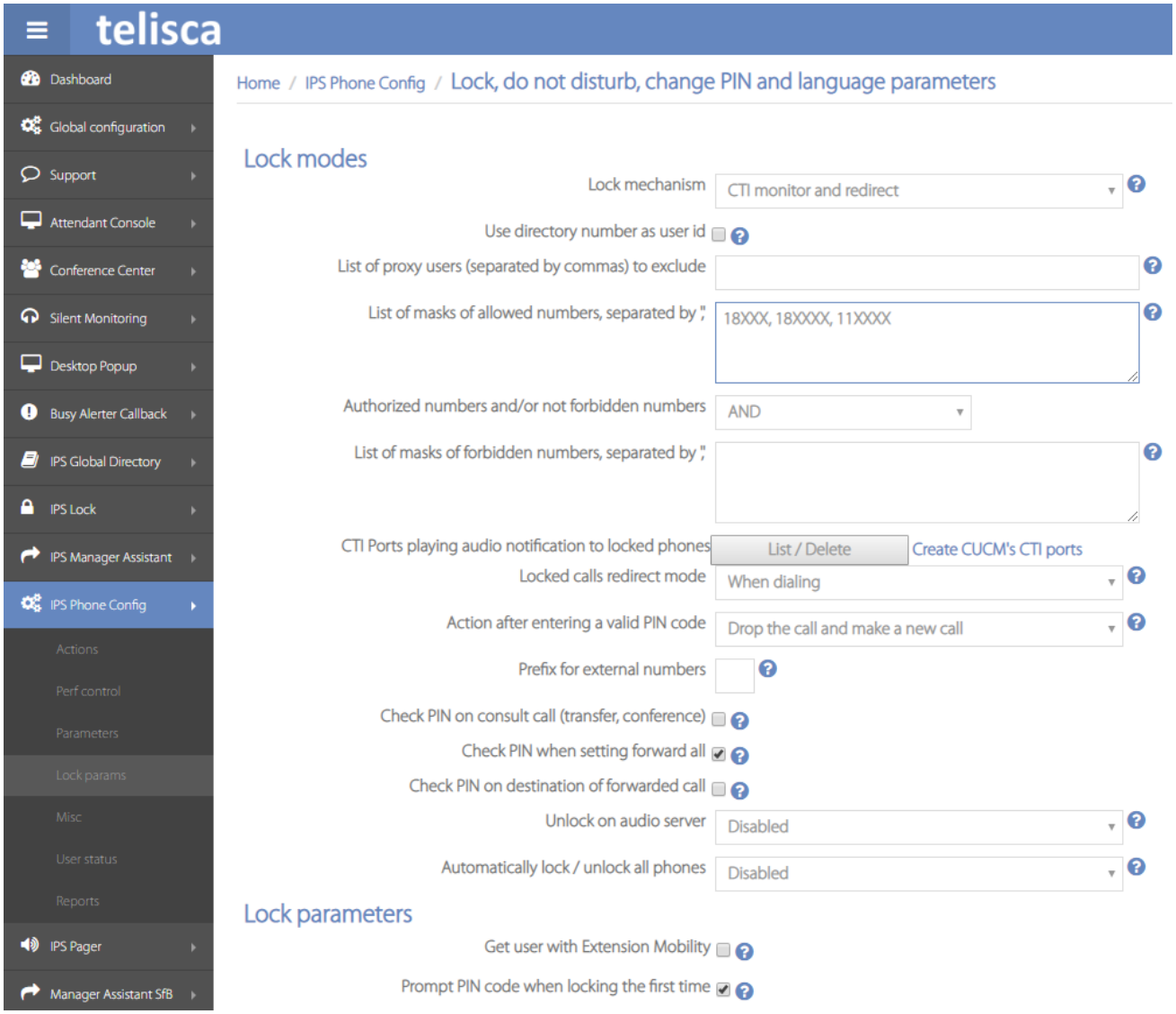
Users can change their PIN Code

It is possible to erase the Calls History when the phone is locked or to schedule times when it is automatically going to be deleted. (For instance during a lunch break and at the end of the day)

IPS Lock IP Phone interface is available in English, French, German, Spanish, Italian and Hungarian. Other languages can be added quickly and simply, contact telisca.

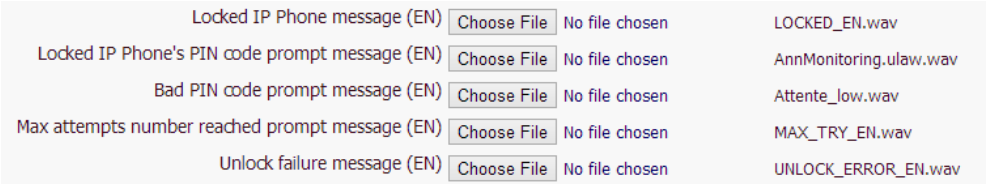
1.5 Administration

Like all other telisca applications, all the IPS Lock parameters can be modified live from a centralized Web interface.



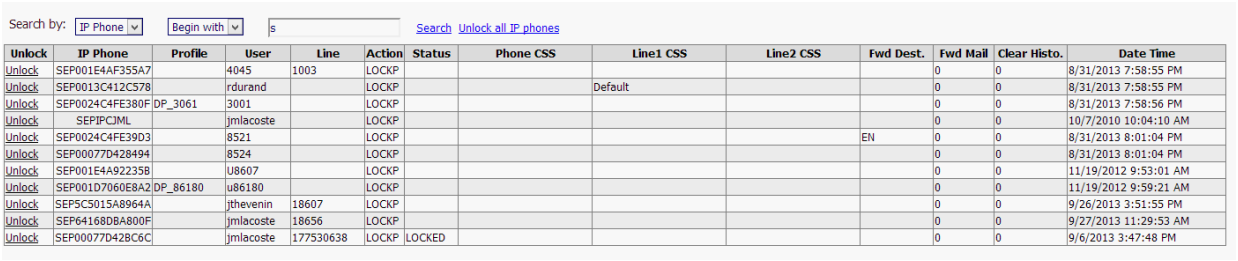
One of the IPS Lock administration pages

Adding a lock/unlock schedule



Customising the audio server messages

The administrator can manually lock or unlock all phones or subsets from the interface.


Search by: IP Phone | Begin with | s | Search | Unlock all IP phones

Unlock	IP Phone	Profile	User	Line	Action	Status	Phone CSS	Line1 CSS	Line2 CSS	Fwd Dest.	Fwd Mail	Clear Histo.	Date Time
Unlock	SEP001E4AF355A7		4045	1003	LOCKP						0	0	8/31/2013 7:58:55 PM
Unlock	SEP0013C412C578		rdurand		LOCKP			Default			0	0	8/31/2013 7:58:55 PM
Unlock	SEP0024C4FE380F	DP_3061	3001		LOCKP						0	0	8/31/2013 7:58:56 PM
Unlock	SEPIPCJML		jmlacoste		LOCKP						0	0	10/7/2010 10:04:10 AM
Unlock	SEP0024C4FE39D3		8521		LOCKP					EN	0	0	8/31/2013 8:01:04 PM
Unlock	SEP00077D428494		8524		LOCKP						0	0	8/31/2013 8:01:04 PM
Unlock	SEP001E4A92235B		U8607		LOCKP						0	0	11/19/2012 9:53:01 AM
Unlock	SEP001D7060E8A2	DP_86180	u86180		LOCKP						0	0	11/19/2012 9:59:21 AM
Unlock	SEP5C5015A8964A		jthevenin	18607	LOCKP						0	0	9/26/2013 3:51:55 PM
Unlock	SEP64168D8A800F		jmlacoste	18656	LOCKP						0	0	9/27/2013 11:29:53 AM
Unlock	SEP00077D42BC6C		jmlacoste	177530638	LOCKP	LOCKED					0	0	9/6/2013 3:47:48 PM

The phones status and batch lock/unlock screen

1.6 Requirements

Telisca products should be installed on a server accessible by all the IP Phones.

- CUCM: 10.5, 11.5, 12, 12.5, 14
- Cisco IP Phone 6921(1) (2), 6941(1), 6961(1) (2), 7811(1) (2), 7821(1), 7841(1), 7861(1), 7905(1), 7911(1), 7912(1), 7920(1), 7921(1), 7931(1), 7937(1), 7940, 7941, 7942, 7945, 7960, 7961, 7962. 7965, 7970, 7971, 7975, 8811, 8831(1) (2), 8841, 8851, 8941, 8945, 8961, 9951, 9971, IP Communicator,

(1) : Background icon not supported

(2) : Line label not supported

Available on private cloud company.telisca.cloud

On premise installation:

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