Product Datasheet

PIN & Password Manager

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 PIN & Password Manager description

1.1 Overview

The management of PIN codes and passwords generates a significant amount of work for internal support services and habitually requires Administrator-level access to the Cisco telephone system. PIN & Password Manager allows support center agents to generate new PIN codes and passwords without needing Administrator access to Cisco CUCM.

In order to improve security, it is necessary that PIN codes be changed regularly to robust codes unknown to third parties. PIN & Password Manager allows forcing on a regular basis the update of PIN codes and passwords which are too old or too simple. Additionally, the generated PIN codes and passwords are sent to users automatically via email.

This tool also facilitates the generation of a new PIN code when the user has lost his PIN and has called support. The Help Desk or the user himself can reset the PIN/password and receive it by email.
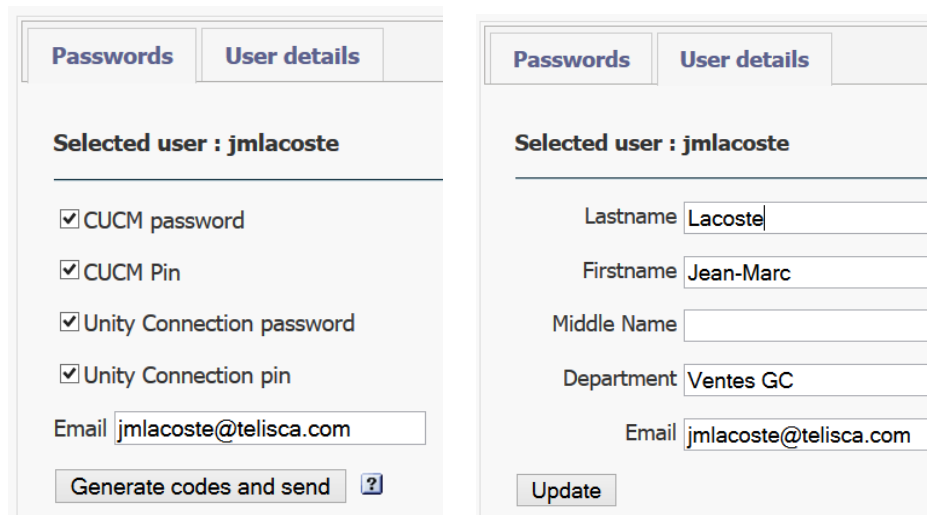
The application includes other features useful to the helpdesk:
- Change user's info in CUCM,
- Delog and relog a user.

1.2 Features list

Web interface for help desk agents:
- Generate a random new CUCM PIN code,
- Generate a random new CUCM password,
- Generate a random new Active Directory or LDAP password,
- Generate a random new Unity Connection PIN code,
- Generate a random new Unity Connection password,
- Send PIN code and password by email to Cisco users.
- Change the user's information and update the line information according to template.

Passwords	User details

Selected user : jmlacoste

☑ CUCM password
☑ CUCM Pin
☑ Unity Connection password
☑ Unity Connection pin

Email jmlacoste@telisca.com

[Generate codes and send] [?]

Passwords	User details

Selected user : jmlacoste

Lastname Lacoste
Firstname Jean-Marc
Middle Name
Department Ventes GC
Email jmlacoste@telisca.com

[Update]

Self-care Web interface :
- Generate a new PIN code (CUCM & VoiceMail) and receive it by email,
- Generate a new Password (CUCM & VoiceMail) and receive it by email,
- Generate a new Active Directory password and receive it by email,

PIN & Pwd Manager

CUCM userID: jmlacoste

eMail address: jmlacoste@telisca.com

Reset PIN code ☑

Reset password ☑

[Reset and send by email]

Self-care IP Phone interface:
- Generate a new Active Directory password.

Self-care audio server :
- Generate a random new Active Directory password,

Automatic process :
- Force changing PIN code,
- Force changing password,
- Reject forbidden PIN codes,
- Batch process to generate new PIN code and password and sen dit by email.

1.3 PIN & Password Management UI

PIN and Password Manager also offers a screen for the support team, accessible from an exploitation security group. This screen permits searching for a user by ID, name, or telephone number. For the selected user, it permits effecting the same PIN code update procedure as in batch mode, displaying on the screen the result of the operation.

Optionally, support personnel may visualize the PIN codes and passwords which are generated randomly or by default in order to communicate them by telephone rather than by email.

PIN & Pwd Manager   telisca

MENU | Parameters | User form | Seft reset params | Batch update | **Operation** | Phone login | Reports

> > > > Close

Search by: Line number ▾ | Begin with ▾ | 186 | Search

Select	Type	Identification	Description	Line number	User ID	Alerting name	Last name
Select	IP phone	CIP186961		186961	U186961	DISPLAY 1	NAME186961
Select	Device profile	DP 8961 Didier		18695	didier		Didier
Select	Device profile	DP_6945		1866945	Dumond		Dumond
Select	Device profile	DP_didier_CIPC		18619	didier	Didier testing IVR	Didier
Select	Device profile	ECO_CIPC		18620	ASHOO_Abdel		ASHOOR
Select	IP phone	SEP0016C76B2B04	Auto 18605 TETS +++++	18605			
Select	IP phone	SEP0024E8B07E76	Auto 18685	18685			
Select	IP phone	SEP1CE6C79BEB37	Auto 18678	18678			
Select	IP phone	SEP2C36F8591BE2	Auto 18682	18682	toto		TOTO
Select	IP phone	SEP44D3CA74287E	Auto 18625	18625			
Select	IP phone	SEP580A2098664B	Auto 18683	18683			
Select	IP phone	SEP5C5015A8964A	Auto 18607	18607	jmlacoste	Mgr607	Lacoste L'éàèù JOUÉ
Select	IP phone	SEP5CF9DD3E1922	Auto 18624	18624	Test		Jean-Marc

1.4 PIN & Password Control

PIN & Password Manager allows you to define a periodic renewal of the PIN code and password. You can select all the CUCM' userId or a list provided in a text file.

A periodic process, detects when a user has changed a PIN code. The new PIN code is checked against a list of prohibited (trivial) PINs. For these users, PIN & Password Manager performs an authentication request. If the authentication succeeds, it retrieves the e-mail, regenerates a new random PIN and sends it by e-mail to the user with a specific message including the new PIN code.

PIN & Password Manager includes a screen to select, view and export execution reports including date / time, user IDs, e-mail address, operation result.

2 Pre-requisites, installation

For more information, please read the common requirements for all telisca apps in IPS Framework Administration Guide

Supported Cisco CUCM:

- CUCM version 8.5, 8.6, 9.1, 10.5, 11, 11.5, 12, BE 6000, BE 7000

NOTE: In the case of querying the CUCM to recover the email address of users will require that the "Mail ID" field is filled in correctly configuring CUCM users.

- Windows servers supported:

    Windows Server 2008 R2 SP1 or 2008 SP2 Foundation, EN/FR (Upgrade only),
    Windows Server 2008 R2 SP1 or 2008 SP2 Standard, EN/FR (Upgrade only),
    Windows Server 2012 or 2012 R2 Essentials, EN/FR,
    Windows Server 2012 or 2012 R2 Standard, EN/FR,
    Windows Server 2016 Essentials, EN/FR
    Windows Server 2016 Standard, EN/FR

- DotNet 4.5.1 (minimum) up to 4.6.2 (advised)
- Minimum configuration: 1 vCPU, 4GB RAM, 70GB disk
- Virtual Machine VMware vSphere, HyperV or Cisco UCS, Cisco UCS-E