Product Datasheet

PIN & Password Manager

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.

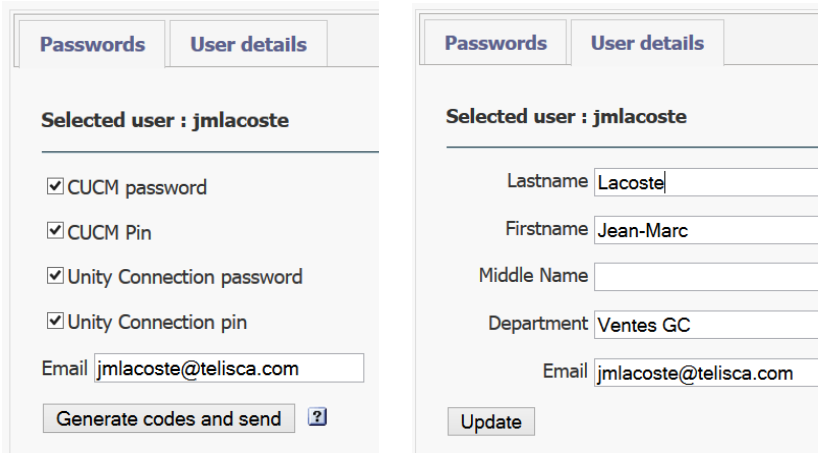
In order to improve security, it is necessary that PIN codes be changed regularly to robust codes unknown to third parties. PIN & Password Manager allows forcing on a regular basis the update of PIN codes and passwords which are too old or too simple. Additionally, the generated PIN codes and passwords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

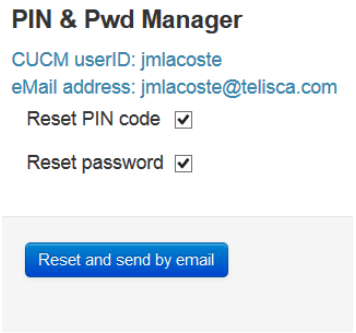
The application includes other features useful to the helpdesk:
- Change user's info in CUCM,
- Delog and relog a user.

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.



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,



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

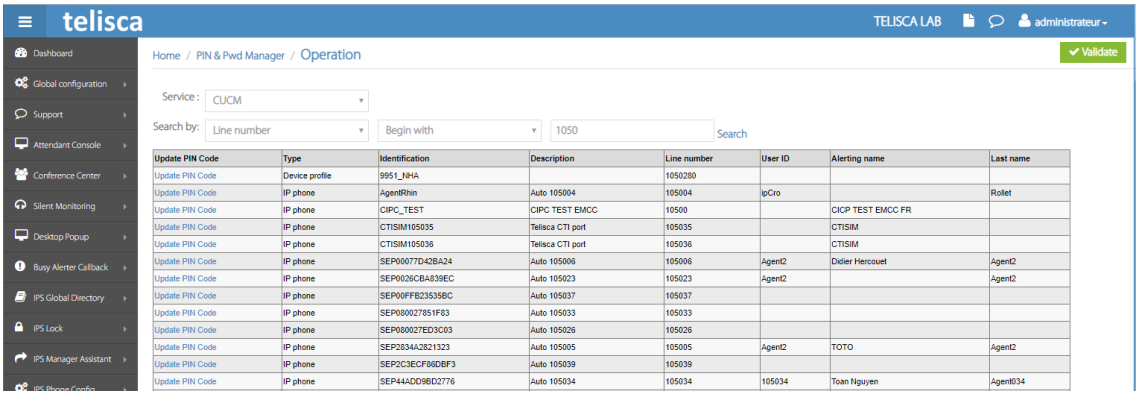
Self-care audio server :
- Generate a random new Active Directory password,

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.



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

Supported Cisco CUCM:

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

Available on private cloud company.telisca.cloud

On premise installation:

Windows servers supported:

- Windows Server 2012 or 2012 R2 Update 1 Essentials
- Windows Server 2012 or 2012 R2 Update 1 Standard
- Windows Server 2016 Essentials
- Windows Server 2016 Standard
- Windows Server 2019 Essentials
- Windows Server 2019 Standard

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