

Administrators Guide

PIN and Password Manager



Version: 5.x

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	3
1.1	OVERVIEW	3
1.2	FEATURES LIST.....	3
1.3	PIN & PASSWORD MANAGEMENT UI	4
1.4	PIN & PASSWORD CONTROL	4
1.5	PIN & PASSWORD SELFCARE	4
2	PRE-REQUISITES, INSTALLATION	5
2.1	NETWORK REQUIREMENTS.....	5
3	ADMINISTRATION	6
3.1	PARAMETERS	6
3.1.1	<i>Update CUCM or AD, get email from.....</i>	6
3.1.2	<i>Operation configuration</i>	6
3.1.3	<i>Forbidden PIN, password check.....</i>	6
3.1.4	<i>PIN expiration check.....</i>	7
3.1.5	<i>PIN/password generation settings</i>	7
3.1.6	<i>Emails to send definition</i>	8
3.2	USER FORM	8
3.3	BATCH UPDATE.....	9
3.3	OPERATION.....	9
3.4	REPORT.....	11
4	USER SELF CARE	12
4.3	CHANGE AD PASSWORD WEB INTERFACE	12
4.4	CHANGE CUCM/UNITY PIN/PASSWORD FROM CUCM	12
4.5	IP PHONE RESET PASSWORD.....	13
3.4	USER INPUT VALIDATION SETTINGS.....	13
3.5	IVR SETTINGS.....	13

1 Product description

1.1 Overview

The management of lost PINs and passwords keeps Help Desk's agents busy. PIN & Password Manager allows Help Desk agents to generate new PINs and passwords without having access to Cisco CUCM, Active Directory nor Unity Connection administration.

To improve Extension Mobility security it is necessary to force users to change their PIN and eventually their password. After deployment, it is advised to assign a different PIN for each user and send it by e-mail. If the user has not changed for some time, the PIN may be changed and sent back by e-mail.

PIN & Password Manager also verifies that the user has not entered a trivial PIN code or password (list of prohibited PIN codes and passwords).

This tool also facilitates the generation of a new PIN code when the user has lost his PIN and called support. A manual mode is also available.

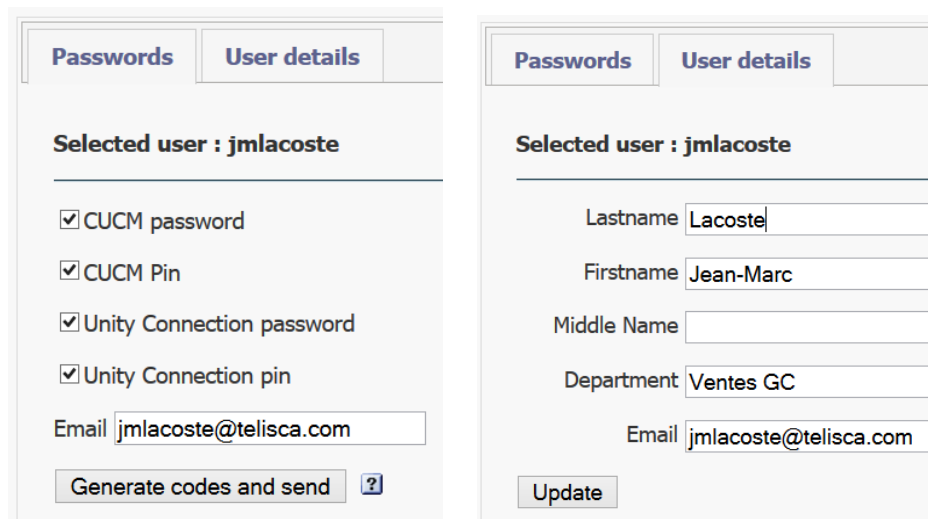
The application includes other features useful to the helpdesk:

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 random new Active Directory password,

Selfcare audio server:

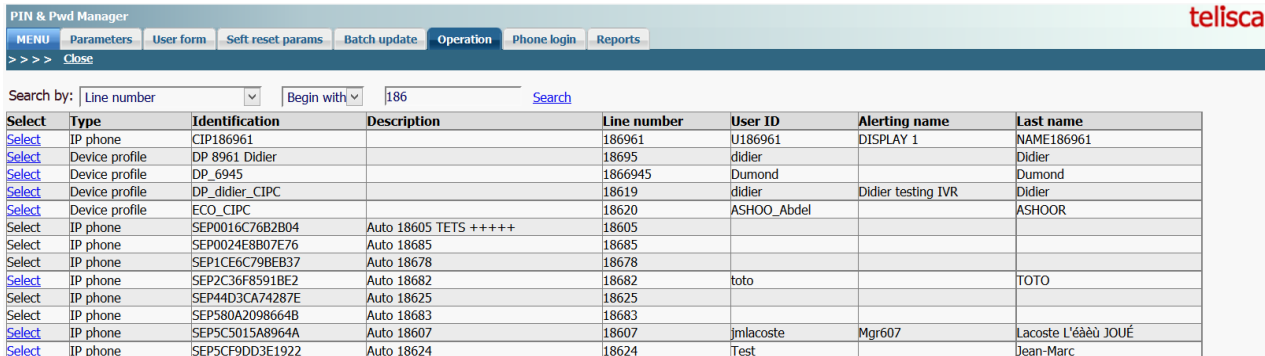
- Generate a random new Active Directory password,

Automatic process:

- Force changing PIN code,
- Force changing password,
- Reject forbidden PIN codes,
- Batch process to generate new PIN code and password and send it by email.

1.3 PIN & Password Management UI

PIN & Password Manager provides an interface for the support, used by the help Desk agents. The agent can search a user by its user name, phone/device profile or phone number. For the selected user, it generates a new PIN code and/or password which can be provided by phone or sent automatically by e-mail. It retrieves the email address of a user by querying the CUCM, an LDAP or AD server.



Select	Type	Identification	Description	Line number	User ID	Alerting name	Last name
Select	IP phone	CIP186961		186961	U186961	DISPLAY 1	NAME:186961
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. It is possible to define a list of users that are excluded from the automatic process.

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

1.5 PIN & Password Selfcare

PIN & Password Manager also offer a self-care to allow the user to reset himself his PIN & Pwd and receive it by email. In this case a secret question needs to be asked to secure the process. The answer to the secret question may be checked against a value in a SQL database.

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 10.5, 11.5, 12, 12.5, 14

- 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

2.1 Network requirements

The following ports must be open between the different systems.

Source	Destination	Protocols/ports	Timeout RTT
Server application Telisca	CUCM	AXL, Serviceability SOAP : https TCP/8443	500ms
Server application Telisca	Unity Connection	REST : https TCP/443	500ms
PC (IPS Administration)	Server application Telisca	http TCP/80 ou https TCP/443 (configurable)	1000ms
Server application Telisca	Server application Telisca (fault tolerance)	http TCP/80 (configurable), TCP/2011 (configurable)	1000ms

3 Administration

3.1 Parameters

This screen is accessible from the "PIN & Pwd Manager" menu "Parameters" folder.

3.1.1 Update CUCM or AD, get email from

PIN & Password Manager can be set to reset Password & PIN from CUCM, Unity Connect or Active Directory or both.

In order to send by email the new password/PIN, the email address associated to the userID can be found in:

- CUCM End users table
- Active Directory mail attribute
- LDAP mail attribute
- IPS Global Directory email column

Update CUCM/AD, get email from

Update password from	<input type="text" value="CUCM"/>	?
Get user's email address from	<input type="text" value="IPS Global Directory"/>	?
Source directory to get email address by userID	<input type="text" value="TESTUPD"/>	?

3.1.2 Operation configuration

The following parameters define the User Interface of the 'Operation Tab' used by the Help Desk to reset PIN & Password and send the information to the users.

Operation's Tab settings

Update from operation and user screen	<input type="text" value="PIN and/or password for CUCM and/or Unity"/>
PIN/password mode	<input type="text" value="Different PIN and password for CUCM and Unity"/>
After updating PIN/password	<input type="text" value="Send it by email"/>
User's email	<input type="text" value="Auto + Edit"/>
Display primary extension number	<input type="checkbox"/>

The user will be able to change from the Operation Tab:

- PIN and/or password from CUCM and CUC
- PIN and password for CUCM or CUC
- Password Only for CUCM
- PIN for CUCM and CUC only
- PIN for CUC

It is possible to set the same PIN for CUCM and Unity

It is possible to set the same value for PIN, Password for CUCM and Unity








The new generated PIN/Password can be sent automatically by email to the requesting contact or displayed in the Web Interface and communicated by phone.

It is possible to allow or not the email address found for the contact.

3.1.3 Forbidden PIN, password check

This section define automatic treatments at specific time of day to check if current PIN or Password are not in the forbidden list. It is possible to limit the number of users updated each day.

Forbidden PIN/password check

Check existing PIN codes at defined time of day 
 Check existing passwords at defined time of day 
 Maximum number of PIN/Password updates (0 unlimited)
 Daily check execution time (hh:mm)
 Check new PIN codes when created or updated 
 Check new password when created or updated 
 Forbidden PIN codes, passwords check period (mn) 
 List of forbidden PIN codes (.) 
 List of forbidden passwords (.) 


It is possible also to check if new PIN or Password created/changed by the user or the administrator are not part of forbidden PIN and Password lists. This done periodically every n minutes (10 by default).

A new CUCM PIN and/or Password is generated and sent by email. A report is generated REPORT_AUTO_yymmdd-hhmmss.txt and can be displayed from the Report tab.

3.1.4 PIN expiration check

After a define number of days, the PIN is considered as expired. Checking the expiration PIN is done every day at **23:00**.

PIN expiration check

Check PIN codes expiration date 
 Maximum PIN code validity duration (d)

A new PIN is generated and sent by email.

3.1.5 PIN/password generation settings

Path text file containing userID list to exclude from treatment: Full path and name of file containing a list of user IDs to exclude CUCM during automatic processing of PIN codes and passwords past. User IDs should be separated by a comma or a newline. This list is used during automatic processing, or treatment via the "immediate execution" screen. It is not taken into account when changing a PIN code / password in the screen "exploitation."

Generally the PIN & Password is generated randomly and sent by email, but is also possible to set the same PIN / Password to everybody and force the user to change it the first time.

You must then define the length of generated PIN and passwords. This value must be compatible with the one set in CUCM Credential policy settings.

Generated PIN & Password are compatible with non-trivial PIN/Password parameter set in CUCM Credential policy settings.

Update PIN/Password even if user not authorized to do it: event if the user does not have right to change PIN or Password, PIN & Password Manager will update it.

Number of AXL SOAP updates / minute, for updating PIN/Password (default 20, maximum 60 in production, 200 in non-working hours). This value must be the same than the one defined in CUCM Administration, Service Parameters, Cluster wide parameters.

3.1.6 Emails to send definition

These parameters define types of emails that will be sent to users to inform them of their new PIN / passwords.

Variables can be used to customize these emails:

- %USERID%: userId of CUCM user.
- %PINCODE% or %PINCODE_CUCM%: new CUCM PIN.
- %PASSWORD% or %PASSWORD_CUCM%: new CUCM password.
- %PINCODE_UC%: new Unity Connection PIN code
- %PASSWORD_UC%: new Unity Connection Password
- %CUCMUSERPAGE%: is the URL with CUCM Publisher host that the user can call to update the PIN and password.

During a new installation, or if all the fields are cleared, default fields will be used to avoid sending empty emails.

Language: Language select to configure emails to be sent to users based on that language. Currently only the following languages are available: English / French.

Title of message sending new PIN: Title the email address to send the new PIN CUCM to the user.

Message body sending new PIN: Contents of the email used to send the new PIN CUCM to the user.

Title of message sending new password: Title the email address to send the new password to the user.

Message Body sending new password: Content of the mail used for sending the new password to the user.

Title of message sending PIN, if PIN code invalid: Title the email address to send the new PIN CUCM to the user, if the user has changed their PIN CUCM but it may not match the security criteria.

Message Body sending PIN, if invalid PIN: Contents of the email used to send the new PIN to the user, if the user has changed their PIN CUCM but it may not match the security criteria.

Title of message sending new PIN Unity: Title the email address to send the new PIN Unity Connection to the user.

Message Body sending new PIN Unity: Contents of the email used to send the new PIN Unity Connection to the user.

3.2 User form

This screen is used to define the fields which will be possible to edit from the Operation Tab.

It defines the format (mask) used to generate:

- Line description
- Alerting name
- Display name
- Line label

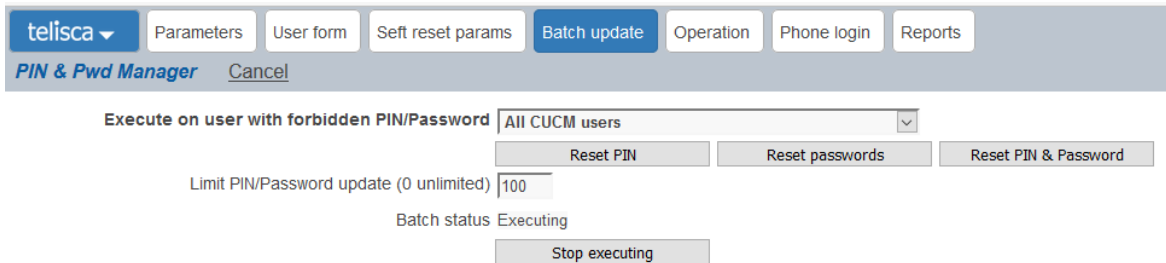
If the '***' is entered then the value is not updated.

You can include the following columns: [LAST_NAME], [MIDDLE_NAME], [FIRST_NAME], [DEPARTMENT], [EMAIL].

[FIRST_NAME,1] means the first character of the first name.

3.3 Batch update

This screen is accessible from the "PIN & Pwd Manager" menu, "Batch update" Tab. It allows you to force checking Forbidden PIN and/or Password and generate a new PIN/ password for a list of users or all CUCM users. The list of forbidden PIN and password is defined in PIN & Pwd Manager menu, Parameters' Tab.



Method of selecting users for changing PIN and / or passwords codes. The choices are:

- All CUCM users: The PIN and / or password code will be changed for all CUCM users with an email address and do not belong to the list of excluded users. If All CUCM users is selected it is possible to limit the number of users that will be updated.
- User List CUCM loaded from a text file: The PIN and / or password code will be changed for all CUCM users listed in the file, with an email address and do not belong to the list of excluded users. The file should contain a list of comma-separated or newline users.

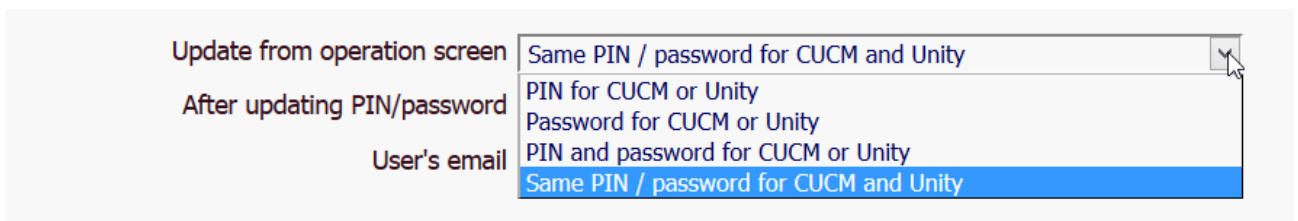
It is possible to stop the current batch execution but also the automatic execution at a defined time of day by clicking on the Stop executing button.

The result of the batch update is available in the Report's Tab, in file REPORT_BATCH_yymmdd-hhmmss.txt.

3.3 Operation

This screen is accessible from the "PIN & Pwd Manager" menu "Operation" folder. It allows you to change the PIN and / or password code for a selected user.

Depending of the setting in 'Parameters' the user will be able to change the PIN code and/or Password in CUCM or Unity. If CUCM userId and Unity Connection Alias are the same, it is possible to set at the same time CUCM and Unity Connection PIN code/Password with the same value.



If one of the first three modes are selected, the operation screen will look like hereafter. It allows to search by user name, line number or IP Phone / device profile associated with the userId. By clicking on the hyperlink it is possible to generate a new random PIN code or Password and send it by email.

Service :

Search by:

Update PIN Code	Update password	Type	Identification	Description	Line number	User ID	Alerting name	Last name
Update PIN Code	Update password	IP phone	CIP186961		186961	U186961	DISPLAY 1	NAME186961
Update PIN Code	Update password	Device profile	DP 8961 Didier		18695	didier		Didier
Update PIN Code	Update password	Device profile	DP_6945		1866945	Dumond		Dumond
Update PIN Code	Update password	Device profile	DP_didier_CIPC		18619	didier	Didier testing IVR	Didier
Update PIN Code	Update password	Device profile	ECO_CIPC		18620	ASHOO_Abdel		ASHOOR
Update PIN Code	Update password	IP phone	SEP0016C76B2B04	Auto 18605 TETS +++++	18605			

If no email address is found (in CUCM or AD/LDAP) for this user, the PIN or password is not updated and an error message is displayed.



If the option 'Display it' has been selected in 'Parameters' then the PIN or Password is displayed to the agent instead of being sent to the user.



If the setting allows to update CUCM and PIN code at the same time, the operation screen will look like hereafter. It allows to search by user name, line number or IP Phone / device profile associated with the userId.

PIN & Pwd Manager te

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

>>> Close

Search by:

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

After selecting the user's device, the helpdesk agent can select which PIN/Password will be updated and send the email with the new generated password. There is an option to allow entering the email address, otherwise the email address is retrieved from CUCM end user or from AD/LDAP.

Passwords
User details

Selected user : jmlacoste

CUCM password

CUCM Pin

Unity Connection password

Unity Connection pin

Email

The helpdesk agent can also change some user's info as defined in parameters. The values entered are used to update the line description, alerting name, display name and label as defined in User Form tab.

Users fields updated

Line description mask

Alerting name mask

Display name mask

Line label mask

Passwords | **User details**

Selected user : jmlacoste

Lastname

Firstname

Middle Name

Department

Email

The following fields can be used in the mask: [LAST_NAME], [FIRST_NAME], [MIDDLE_NAME], [DEPARTMENT], [EMAIL]. *** means that the value will not be updated.

3.4 Report

The report can be displayed from Report's Tab.

telisca
Parameters
User form
Seft reset params
Batch update
Operation
Phone login
Reports

PIN & Pwd Manager

Report

```

170528-193017, adent.jmlacoste@telisca.com PIN UPDATED
170528-193024, adent.jmlacoste@telisca.com, EMAIL SENT
170528-193026, assistant1, CANNOT UPDATE CREDENTIAL, EMAIL NOT FOUND
170528-193027, assistant2, CANNOT UPDATE CREDENTIAL, EMAIL NOT FOUND
170528-193028, ccxadmin, CANNOT UPDATE CREDENTIAL, EMAIL NOT FOUND
170528-193115, NB CHECKED=63, NB FORBIDDEN=4, NB UPDATED=1

```

Three type of reports are available:

- REPORT_BATCH: executed from Batch tab
- REPORT_AUTO: executed for all users at define time of day
- REPORT_UPDATE: executed periodically for newly created/updated PIN/Password

It contains the following detail information:

- PIN updated
- Password updated
- Email sent
- Email not found (which makes the update impossible)
- Cannot be changed (user is in excluded userId list or user cannot change password set in CUCM)
- Fails to update a new PIN
- Fails to update a new Password
- Fails to send the email after updating PIN/Password

A the end of the report, it tells the count of users checked, users with forbidden PIN/Passwords, users updated

4 User Self Care

4.3 Change AD password Web interface

A Web user interface can be used to change the password of Active Directory password. This page can be called from the Jabber tab (by editing Jabber configuration).

The URL to call is <http://host/IPSCFG/admin/UserADLogin.aspx>

The user must re-enter its previous mode password before changing it.

4.4 Change CUCM/Unity PIN/Password from CUCM

A Web user interface can be used to change the PIN and/or password CUCM/Unity by providing the Active Directory authentication. Then an email will be sent to the user with the new PIN/Password.

The URL to call is <http://host/IPSCFG/admin/UserPwdReset.aspx>

PIN & Pwd Manager

CUCM userID: jml
eMail address: jmlacoste@telisca.com

Reset CUCM PIN code

Reset CUCM password

Reset Unity PIN code

Reset and send by email

If telisca's server is in Active Directory domain you can retrieve automatically the user's Windows login. You need then to change from IIS Administration the authentication settings for this page by setting Anonymous authentication to disabled and Windows authentication to enabled.

This page can be called from the Jabber tab (by editing Jabber-config.xml configuration file).

4.5 IP Phone reset password

You can reset the password from an XML IP Phone interface. The amendment applies to the associated user or logged on the IP Phone. The user is asked to enter additional personal information (eg mobile number) who is wanted in Active Directory.

The URL to call is <http://host/IPCFG/admin/ADReset.aspx>

The use and display messages parameters are defined in the configuration screen 'CDM ResetAD' administration.

3.4 USER INPUT VALIDATION SETTINGS

These settings require Professional Services from telisca

3.5 IVR Settings

These settings require Professional Services from telisca