

CALL2UNLOCK

Administration Manual

V 4.0

Content

SYSTEM OVERVIEW	3
Introduction	3
INSTALLATION AND CONFIGURATION	6
1. Updating the Web Credentials.....	13
2. Updating the Database Credentials	14
3. LDAP Configuration WIZARD:.....	14
Testing Unlocking and Resetting Accounts	21
4. LDAP Configuration	26
Testing Unlocking and Resetting Accounts	32
5. LDAP ADMINISTRATORS.....	34
6. SIP CONFIGURATION WIZARD:	35
7. CONFIGURING YOUR CORPORATE PBX.....	40
8. SIP CONFIGURATION	40
9. CUSTOM PROFILES	43
CREATING CUSTOM PROFILES	46
10. WHITE LIST	47
11. ACCOUNT SYNCHRONIZATION.....	48
12. END USERS EDITION	49
13. RADIUS – MFA CONFIGURATION.	51
14. END USER PORTAL – GOOGLE AUTHENTICATOR ENROLLMENT INTERFACE.....	53
15. END USER WEB SELF SERVICE	55
16. REPORTS.....	56
17. LICENSE	57
18. TESTING THE SERVICE	58

SYSTEM OVERVIEW

Introduction

Call2Unlock is the first LDAP self-service solution which works towards a simple phone call.

A big percentage of calls that a service desk or IT support department receives, are related to unlock or reset user accounts. One self-service LDAP system, make this task possible, without the intervention of a human.

Typically, the products which solve this issue, have some disadvantages like the requirement to install software on the PCs, or even exposing and compromising the security using web tools or mobile applications available from the internet.

Users of Call2Unlock just need to dial an internal extension on the company's PBX, or a public DID, and following few instructions, the user account will be securely unlocked, or reseated. The "challenge" information (Employee ID, PIN numbers, tokens) could be stored in the Active Directory, the Call2unlock Database, or any kind of two factor authentication system towards a RADIUS server. Call2unlock provides its own RADIUS – Google Authenticator infrastructure as well for this purpose.

In order to implement Call2Unlock for your organization, you just need:

- Microsoft Active Directory 2008 or higher (2008,2012,2016,2019,2022) as directory server
- Any PBX system compatible with SIP protocol. (Otherwise Call2Unlock Cloud Secure Phone Gateway could be provided).

How does it work from the end user perspective?

Situation1: *"My name is Bob Smith, and I work for in financial department, and my account usually gets locked out, because I fail several times typing my password, and I need to be unlocked a.s.a.p. I typically work in my office, within the company's network"*

Bob should follow the following steps.

1. Dial the internal Call2Unlock extension provided by the administrator, one friendly IVR will ask for a personal identification number. (like an employee number or badge number)
2. The system will ask Bob; what action does he need to perform (Unlock or Reset his account)
3. Once Bob, press option 1 (unlock account), the system will find Bob's account and will play the message "The account that you are trying to unlock is 'Bob Smith. If this is the account you are trying to unlock, please press 1, otherwise press 0 or hung up the call". Then it will ask Bob for a PIN number to confirm the action.
4. Once the system gets the option key (1), and the PIN number, the system will say "Your account has been successfully unlocked", and immediately, the user will be able to login into the network. **This pin number could be something fixed stored in AD or the Call2Unlock DB, or a PIN + Token Number (Time based) provided to the user by the Google Authenticator app.**

Situation2: "Now Bob, has forgotten his password, it has expired, or he suspects that someone else can know it so he needs a new password".

Bob should follow the following steps.

1. Dial the internal Call2Unlock extension provided by the administrator, one friendly IVR will ask for a personal identification number. (like an employee number)
2. The system will ask Bob, what action does he need to perform (Unlock or Reset his password)
3. Bob, press now option 2 (reset password), the system will find Bob's account and will say to Bob "The account that you are trying to reset is Bob Smith. If this is the account you are trying to unlock, please press 1, otherwise press 0 or hung up the call".
4. Once the system gets the option key (1), the system will ask Bob for a PIN or validation number. Once provided, the system will tell Bob "Your temporal password has been send to your secondary email address".
5. Bob receive his temporal password on his secondary email. Now he can log into the network using the temporal password. Immediately the windows authentication system will ask Bob to create a new password.

**** The pin number could be something fixed stored in AD or the Call2Unlock DB, or a PIN + Token Number (Time based) provided to the user by the Google Authenticator app.**

Call2Unlock can send the temporal passwords to the end users, in 04 different ways:

-By Audio (Text To speech).

- By sending it to a Secondary Email (like the example above).
 - By sending an SMS to the employee's cell phone.
 - By sending a Combination using two delivery ways. For instance, the first 3 characters by Audio, and the second 5 characters in an SMS.
- ** The personal Information like secondary email, personal cell phone number and/or Google Authenticator account, is information that the end user provides once it's enrolled to the system.**

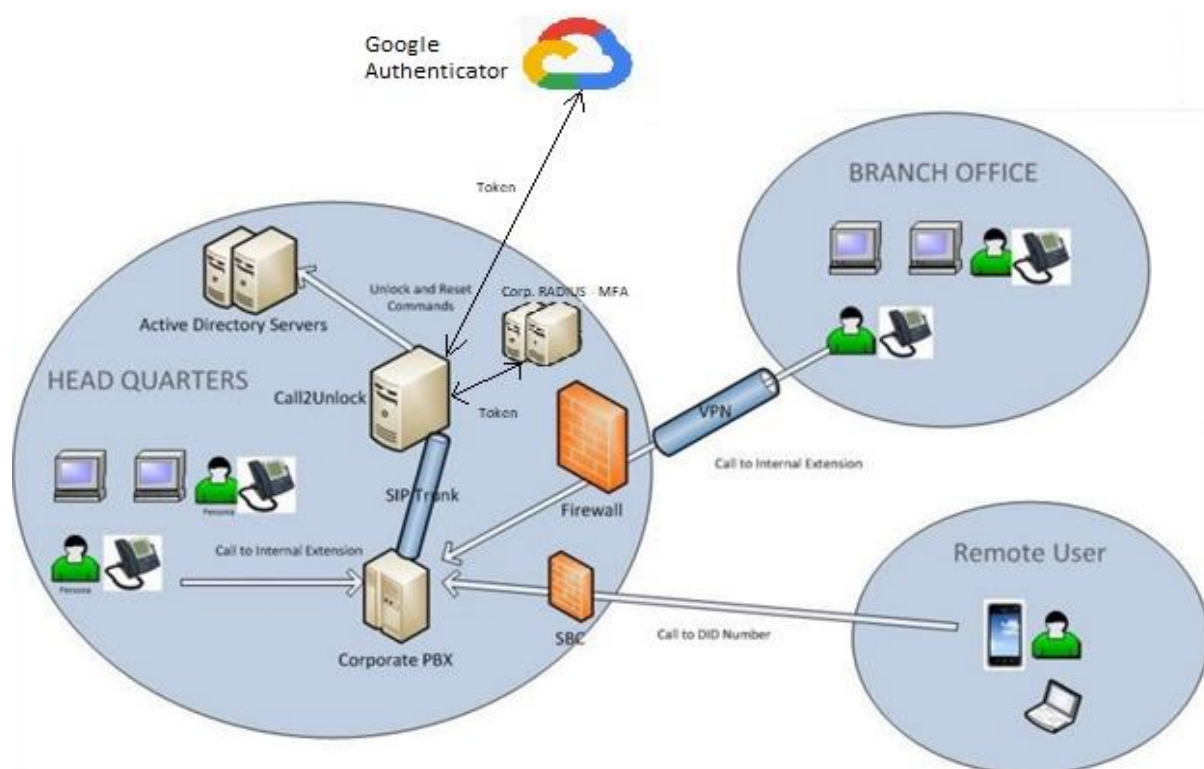
Situation3: “Bob is locked out, and he is working from home, trying to connect to the company’s VPN, and it’s authentication mechanism validates that the account is not locked out, disabled or its password is expired, or even worse, uses AD as authentication mechanism”.

-Bob will be able to unlock or reset his account using the same options than the examples above. The only difference is, now he is going to dial a public DID number configured on the company's PBX, His personal telephone number has been included in a “white list” for allowed personal phones to use Call2Unlock from the PSTN

How does it work from the IT administrator perspective?

In order to understand how Call2Unlock works, let's take a look at its architecture

Architecture



Call2Unlock has basically 5 components

Call2Unlock V 4.0 Administration Manual

- 1. IVR Engine.** This component interacts with the Corporate PBX of the company, sending audio messages to the user and getting the DTMF inputs from the user
- 2. LDAP command Engine.** This interacts sending the appropriate commands to the Active Directory servers to perform the unlocking or reset of the accounts in a secure and encrypted communication.
- 3. Web Administration tool:** Web site for Administrators, to configure the system, to get reports, and self-service pages, for end users, where they can provide extra information like PIN numbers, secondary emails or personal mobile phones.
- 4. RADIUS - Google Auth. Platform:** Call2unlock provides its own RADIUS - Google Authenticator Implementation, to be used as an authentication mechanism by the end users. This feature is configured 100% from the Web Administration Tool. Thus, Call2unlock can be used not only as a Self Service Tool for AD accounts, but also as two factor Authentication platform. Also Call2Unlock can be integrated with any Multi Factor Authentication System compatible with RADIUS.
- 5. Web User Self Service Tool.:** Since the users can auto-enroll their accounts to Google Authenticator using our Web User enrollment panels, they can also unlock or reset their accounts using their Google Authenticator app or the Token provided by your MFA in a secure way using our web self-service interface

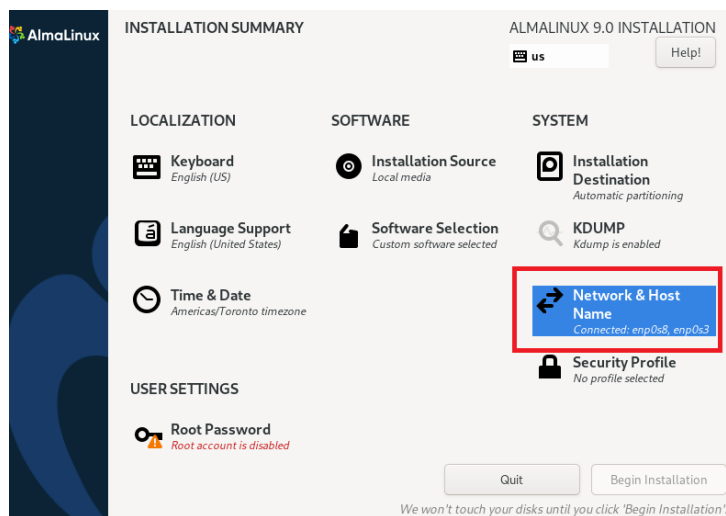
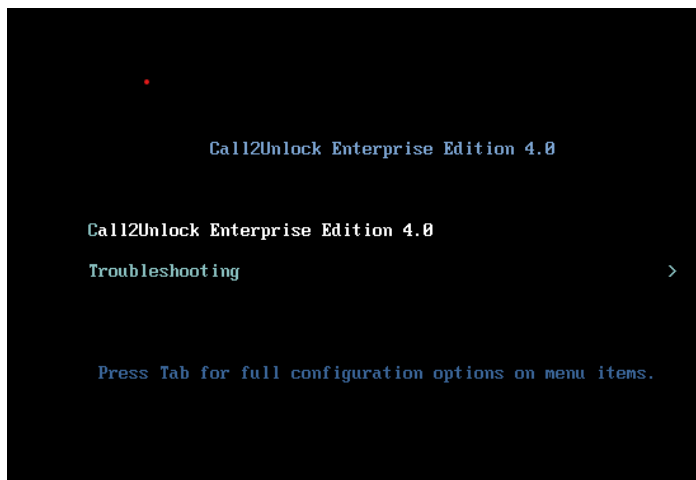
INSTALLATION AND CONFIGURATION

Getting the System

Fill the online form on <https://call2unlock.com>

You will get an email from Call2unlock with the link of the ISO image. Call2Unlock runs on the Operative System Linux, so the ISO installer called Call2UnlockEnt04.iso is basically an AlmaLinux 9.0 Linux Minimal ISO, customized with all the required packages, scripts and application tools.

The process to install the ISO, is basically the same of the installation of a Linux. This ISO can be installed on any server physical or virtual.



IMPORTANT:

In order to get a successful installation, it is mandatory to provide the IP addresses, host name, Default Gateway, etc., to the network interfaces, during the installation.

It is required to assign a static IPv4 manual address to your NIC, like in the example

It's also important also assigning a reachable DNS (internal preferably) , specially to make the internal services working and also to resolve your AD infrastructure. Also, it is recommended to disable IPv6

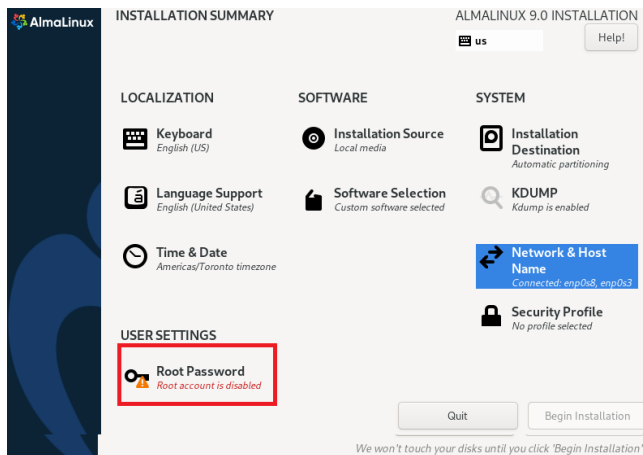
The image shows two side-by-side screenshots of the 'Editing enp0s3' network configuration window. In the left screenshot, the 'IPv4 Settings' tab is selected, showing a 'Manual' method with an IP address of 10.0.0.211 and a netmask of 24. In the right screenshot, the 'IPv6 Settings' tab is selected, showing the 'Method' set to 'Disabled'.

Repeat the same steps if you will configure an extra NIC interface. Depending of your network architecture, sometimes could be a good Idea to dedicate a NIC to comunicate to your AD infrastructure and the other NIC to Management or VoIP traffic.

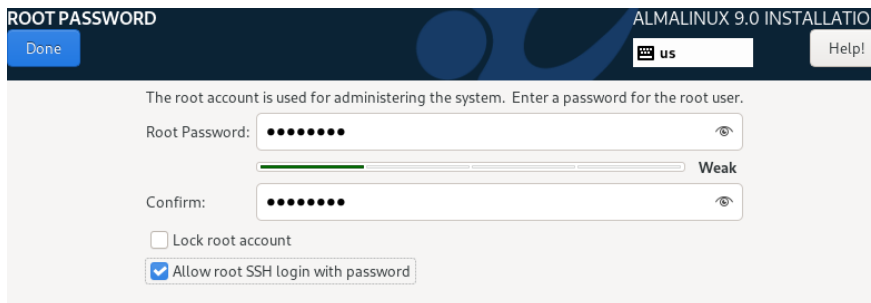
The image shows a screenshot of the 'NETWORK & HOST NAME' configuration window in the ALMALINUX 9.0 INSTALLATION. It displays two Ethernet interfaces: 'Ethernet (enp0s3)' and 'Ethernet (enp0s8)'. The 'Host Name' field is set to 'democ2u.cordialo.net'.

Then you must assign a name to your new Call2unlock server.

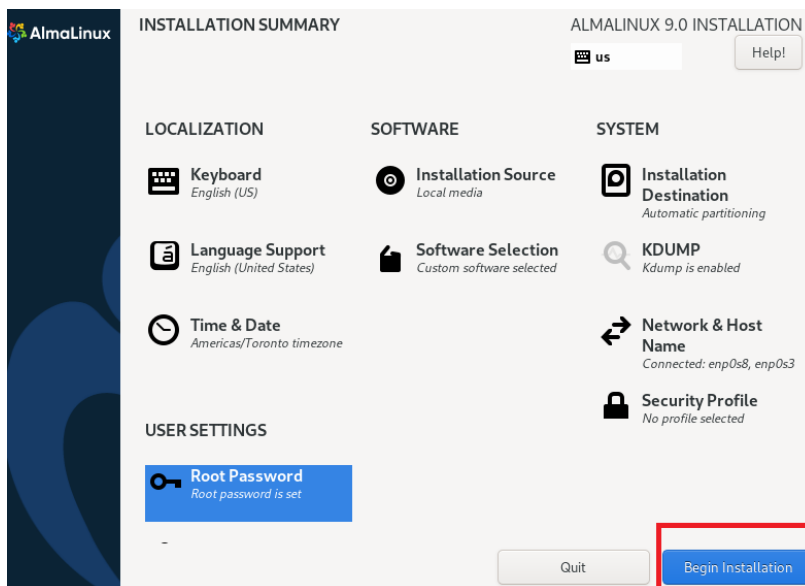
Finally, you shuold assing a Root password for the system.



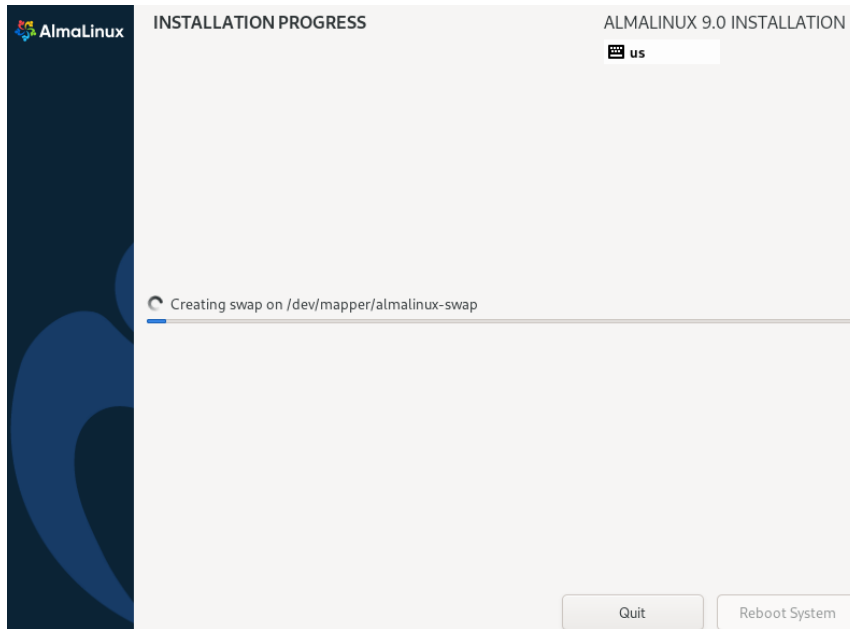
Is very important, that you check the box “Allow root SSH login with password” to be able to ssh to the box. Later on you can assign SSH keys or Certs for SSH authentication. Also uncheck “Lock root account”, as in the image below:



Once you have completed the previous steps, you’re ready to start the installation. Click on “Begin Installation”



Like a regular Linux installation, you just need to wait until the installation is completed.



Validation of the Installation.

- Start an ssh sesión to your Call2Unlock instance. You should get the banner of call2unlock similar to the image below.
- Verify that asterisk PBX is up and running executing “asterisk -rvvvv”. You should get an output like this:

```
AlmaLinux 9.0 (Emerald Puma)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

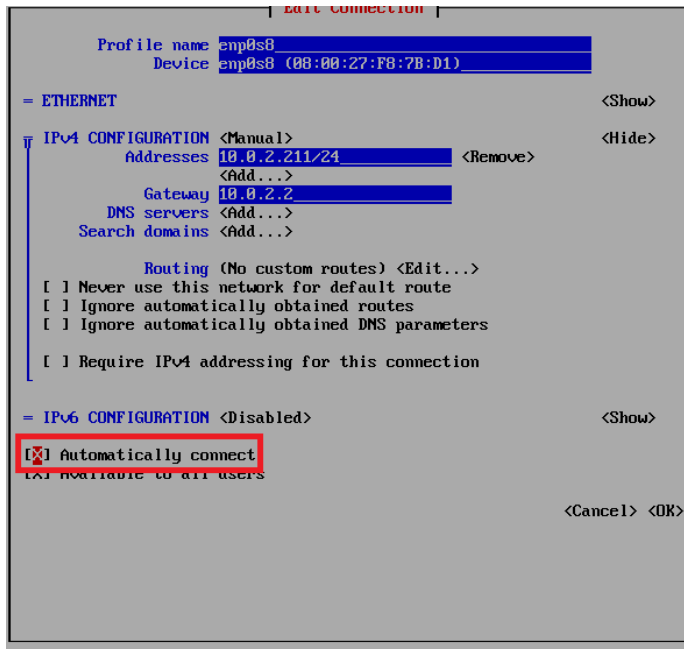
Activate the web console with: systemctl enable --now cockpit.socket

c2u24manual login: root
Password:
#####  #####  #  #
#          #  #  #
#          ###  #  #
#          #  #  #
#####  #####  #####

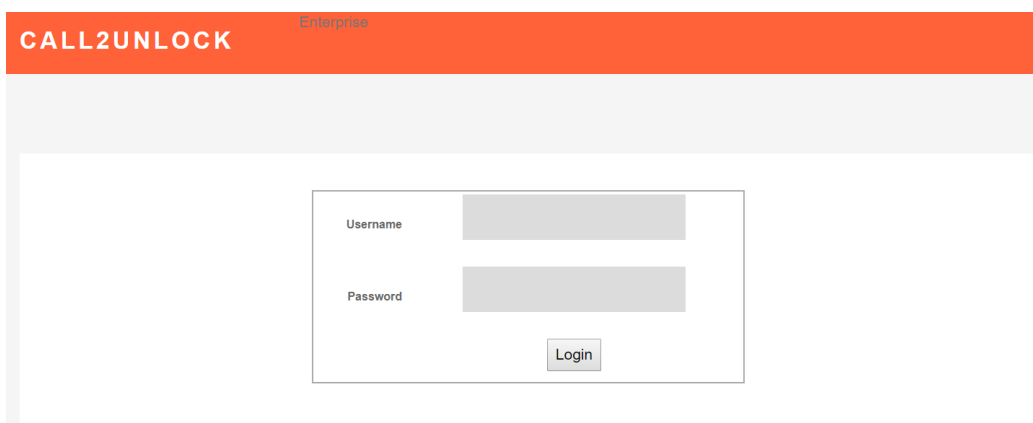
Call2Unlock Enterprise Edition v. 4.0
To configure the system go to https://IP-Address

[root@c2u24manual ~]#
```

IMPORTANT: If you have more than one NIC, please be sure all of them are enabled at Startup. Even if during the installation you set this up, that applies only for the first NIC. For NIC #2 or #3, please confirm you have this enabled or configure it executing **nmtui** from the Linux command line. Be sure “Automatically connect” is checked.



- Verify the web configuration panel, and login into that panel. Open a web browser and go to [https://\[ip-address\]](https://[ip-address]). Use the default credentials to log in (root/call2unlock). You must change that password later.



Done!

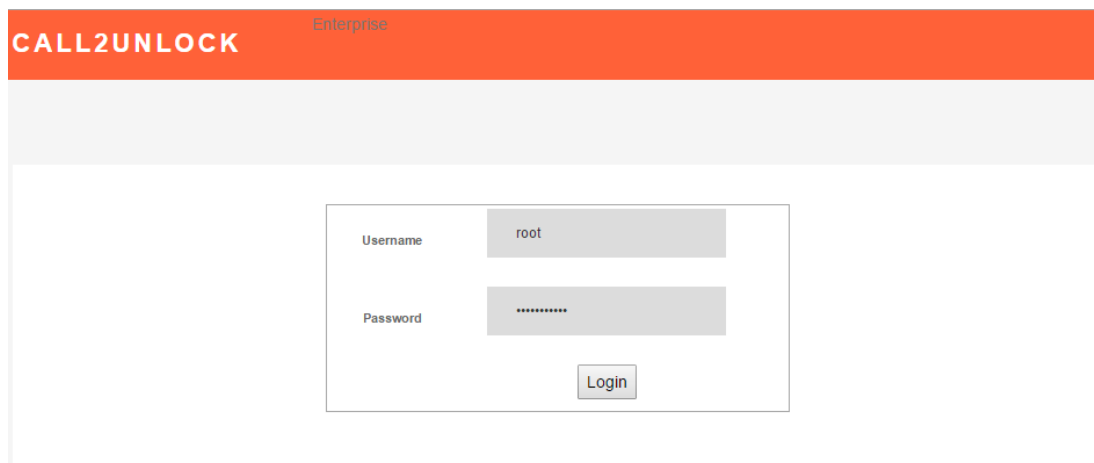
Once you have verified that asterisk is running and the web panel is accessible and you are able to log into the panel, we are ready to configure the platform and integrate it to your Phone System and your AD infrastructure.

Default Values

Once you have Call2Unlock up and running, it is recommended that you immediately change the default credentials provided

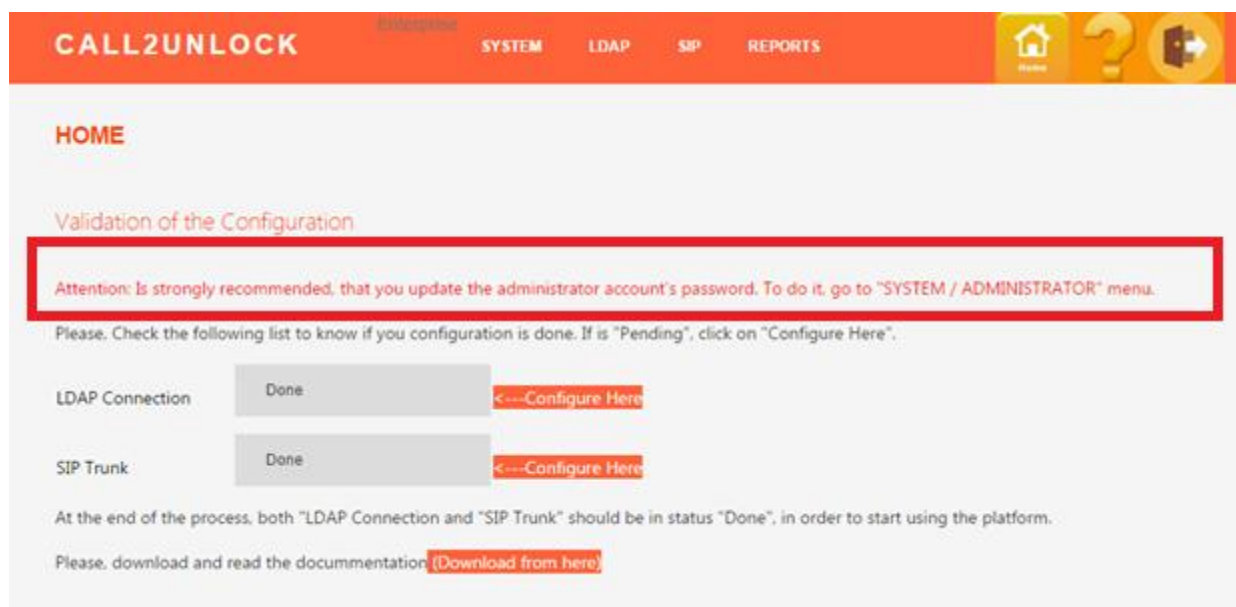
Configuring the System

Log in into the web interface of call2unlock `https://ipaddress`

The screenshot shows the login page of the Call2Unlock Enterprise web interface. At the top, there is an orange header bar with the text "CALL2UNLOCK" in white and "Enterprise" in a smaller font to its right. Below the header is a light gray horizontal bar. The main content area is white and contains a login form. The form has two input fields: "Username" with the value "root" and "Password" with a masked value represented by eight asterisks. Below these fields is a "Login" button.

Use the default credentials to log into the system `u= root, p=call2unlock`.
Select your language (In this version only available in English/Spanish)

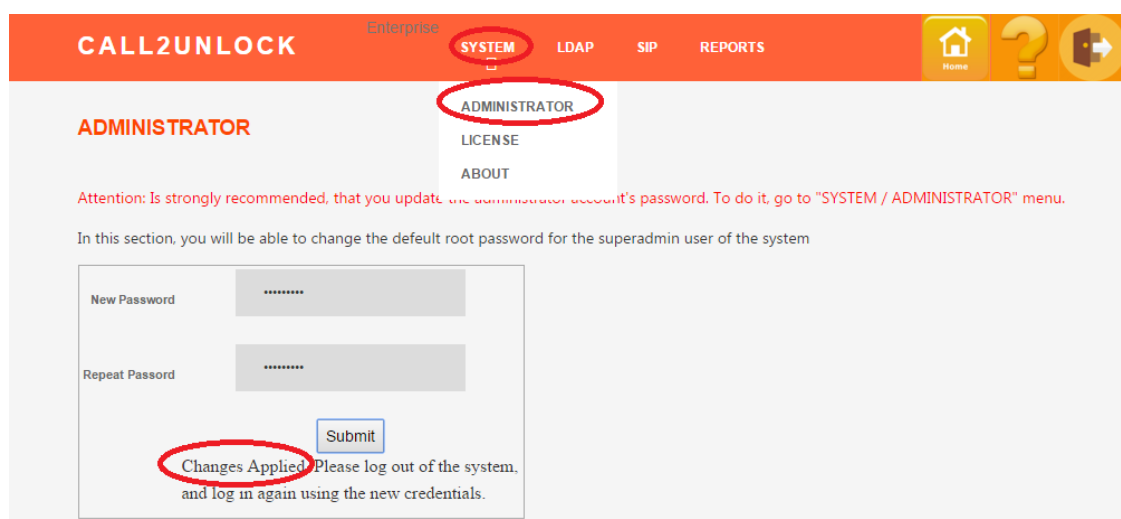
Once authenticated, the system will take you to the HOME site. A message recommending to change the default Web Interface user's password will appear in red.



Note: These credentials are used to log in to the application, so the password should be changed as soon as possible. Don't confuse application credentials with database credentials. We will change the database credentials in the "Database Administration" option, detailed later.

1. Updating the Web Credentials

Go to the "SYSTEM/ ADMINISTRATOR" menu option. The Administration page will load. Once you write a new password and submit it, a message "Changes Applied", will appear. The user should re-login to the system.



2. Updating the Database Credentials

In the same way than the Web Credentials, we should update our database credentials, with a secure password. Go to the “SYSTEM/DB ADMINISTRATION”, provide the default current DB password and update the password. You will need to logout/login of the system after applying the changes

DB ADMINISTRATION

Attention: Is strongly recommended, that you update the administrator account's password. To do it, go to "SYSTEM / ADMINISTRATOR" menu.

In this section, you will be able to change the DB Password to connect to the Call2unlock Database

Current Password	<input type="password"/>
New Password	<input type="password"/>
Repeat New Password	<input type="password"/>
<input type="button" value="Submit"/>	

3. LDAP Configuration WIZARD:

This is the most important section. Here you will be able to configure and test the necessary parameters and credentials to connect to your Active Directory server, and also test actions like Unlock and reset. This assistant consists in a series of 05 steps that will guide you to trough the process and will detect any issues and the remediation recommendations.

Previously, is necessary to create a service account dedicated to call2unlock with enough privileges to unlock and resear accounts.

Step01: Connectivity Test. The System Verifies the involved ports are accessible from call2unlock to your AD Infrastructure

Step02: LDAP Authentication and Bind The System Verifies your service account, can authenticate to your Active directory from Call2Unlock


Step03: Unlock and Reseat Test: The System will validate your service account has enough privileges to unlock and resear accounts using test user accounts.

Step04: Retrieve Objects. Call2Unlock will retrieve to its internal database, the user accounts (Only account names). Those users are filtered by the Group Names and OUs provided on this assistant.

Step05: Provide the rest of configuration parameters, like: User validation place (Active Directory, Call2unlockDB, 2FA), Password Delivery (Audio, SMS, Email), Password Complexity, etc.

Once all the 05 steps are completed, call2unlock will generate the IVR script, which will be presented to the user every time he/she dials the Call2Unlock internal extension or public DID phone number. Go to the “LDAP / CONFIGURATION ASSISTANT” menu option. You should get the Step1 page

Step01:



STEP 1. Let's verify you have connectivity to your Active Directory Infrastructure. The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
IP Address	10.0.2.231	Ip Address of the Main Domain Controller
Hostname	myadserver	Hostname of the Main Domain Controller
Type of LDAP Connection	1.Global Catalog	0. Active Directory Server. Use this option if you are going to use a unique Domain. Only the LDAP port will be used to connect the Active Directory Server. 1. Global Catalog. Use this option if you have a Forest with multiple Domains. The Global catalog Port, on the root domain AD server will be used to search objects and the LDAP port to unlock and reset accounts. Please be sure to include the list of your servers on the field AD Servers List .
LDAP Port	636	LDAP port to Connect to LDAP (389 by default, 636 Recommended)
Global Catalog Port	3269	Global Catalog port (3268 by default, 3269 Recommended)
AD Servers List	10.0.2.231 cordialo.net;10.0.2.131 evt.cordialo.net;10.0.2.31 lv.cordialo.net	Please Write your AD Servers List if you are using a Global Catalog and a Multi-Domain Enviroment Write the IP, Server name and a semi-colon for each domain controller. This content will be added to the /etc/hosts file Example: 10.0.2.230 domain.net; 10.0.3.230 child1.domain.net; 10.0.4.230 child2.domain.net Please, delete blank spaces specially at the beginning of each row

Ldap Connection Test: Success
 Global Catalog Connection Test: Success
 Other AD Servers: 10.0.2.231 :Success
 10.0.2.131 :Success
 10.0.2.31 :Success

 Update Status: Changes Applied on Database

The following parameters should be provided. (All the Properties labeled in Red)

IP Address: IP Address of the main Active Directory Server. If you want to work with a complete domain forest, this IP is the root domain AD server with a Global Catalog running

Hostname: Name of the Active Directory Server. (This value is just informative, will not be considered as a parameter for the LDAP connection).

Type of LDAP Connection: This selection allows us to work with a complete Active Directory Forest, including child domains, or directly with a single domain AD server.

0. Active Directory Server. Use this option if you are going to use a unique Domain. Only the LDAP port will be used to connect the Active Directory Server.

1. Global Catalog. Use this option if you have a Forest with multiple Domains. The Global Catalog Port, on the root domain AD server will be used to search objects and the LDAP ports to unlock and reset accounts on all the Domain Controllers

LDAP Port: LDAP port for your Active Directory. By default, 389. Call2unlock uses LDAPS (Secure Ldap) so 636 will be recommended.

Global Catalog Port: Port used for the Global Catalog (In case 1. Global Catalog is selected as Type of LDAP Connection). Typically port 3269 for secure connections

AD Servers List: This is the list of AD Servers List. If you are using the Global Catalog and a Multi-Domain Environment, write the IP, Server name and a semi-colon for each domain controller. This content will be added to the /etc/hosts file Example of Content of this field:

10.0.2.230 domain.net;

10.0.3.230 child1.domain.net;

10.0.4.230 child2.domain.net

The system will add at the end of the /etc/hosts file something like:

10.0.2.230 domain.net


10.0.3.230 child1.domain.net

10.0.4.230 child2.domain.net

Once you completed filling the information, click the “Test” button. The system will test the ports and destination to be sure call2unlock can communicate to your AD infrastructure from the network prospective. Only if there are no “failed” test, the system will allow you to save and move forward to the Step2

<input type="button" value="Test"/>	Ldap Connection Test:	Success
	Global Catalog Connection Test:	Success
	Other AD Servers:	10.0.2.231 :Success 10.0.2.131 :Success 10.0.2.31 :Success
<input type="button" value="Save"/>	Update Status:	Changes Applied on Database
<input type="button" value="NEXT STEP"/>		

Step02:



STEP 2: Let's verify you can bind (Authenticate) to your AD Infrastructure with the Service Account you have created for call2unlock, and the CA Client Certificate exported from your Domain Controller. All the disabled controls corresponds to settings already provided on the previous step (Step1). The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
IP Address	10.0.2.231	Ip Address of the Main Domain Controller. (Assigned on the previous Step)
Hostname.	myadserver	Hostname of the Main Domain Controller (Assigned on the previous Step)
Type of LDAP Connection. (Assigned on the previous Step)	1.Global Catalog	(Selected on the Previous Step). The Test will use the LDAP Port or the Global Catalog Port, according to this selection
LDAP Port	636	LDAP port to Connect to LDAP (Assigned on the previous Step)
Global Catalog Port	3269	Global Catalog port (Assigned on the previous Step)
Adm accountname	scv_c2admin	Account with admin privileges
Adm password	*****	Password of the Account with admin priv.
Adm DC string	cn=Users,dc=ext,dc=cordialo,dc=net	DC String for the Account with admin priv. Example. cn=Adminuser,dc=domain,dc=com
Upload Certificate	Upload your AD Certificate Choose File No file chosen Submit	Certificate generated, using the Active Directory Certificate Services. Once you upload your certificate, wait until you get the successfully Uploaded message. To learn how to generate a CA Certificate in you Active Directory Server, check this guide

Save and Test Success . Changes Applied on Database Success

NEXT STEP

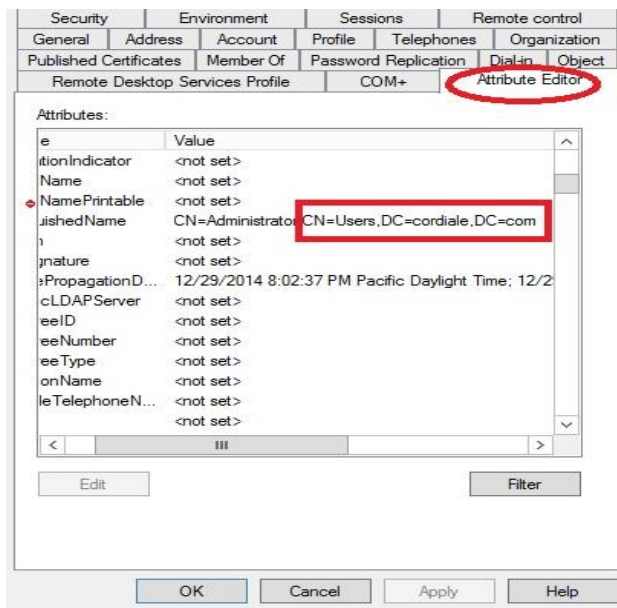
The following parameters should be provided. (All the Property labels in Red). The disabled controls correspond to the settings already provided on the previous step

Adm Accountname: This account should have enough privileges to unlock or reset accounts in your active directory. Typically a service account.

Adm Password: AD Password for the adm account.

Adm DC string: This is the distinguished name of the OU where the Admin LDAP Account belongs. In order to get this information, go to your AD server, in "Active Directory Users and Computers", go to "Attribute Editor", and copy the distinguished name, but just from the OU, not taking the account name.

In the picture below ,from the string “cn=Administrator,cn=Users,dc=cordiale,dc=com” just “cn=Users,dc=cordiale,dc=com” has been taken



Upload Certificate: You should upload the pem client certificate previously generated on your AD. This certificate is needed to perform actions like reset passwords from call2unlock or simply to bind your active directory.

Upload Certificate	Upload your AD Certificate	Certificate generated, using the Active Directory Certificate Services. Once you upload your certificate, wait until you get the successfully Uploaded message. To learn how to generate a CA Certificate in you Active Directory Server, check this guide
	Choose File No file chosen	
	Submit	

To generate this certificate following the manual , “Generating the AD Certificate”, that is available on the web site of Call2Unlock <https://www.call2unlock.com>

Once you completed filling the information, click the “Save and Test” button. The system will test the binding to your active directory, to validate that your Service Account is able to Authenticate to your Active Directory from Call2Unlock, also to proof that the info provided is accurate and the certificate is valid. Getting the “Success” message on the test, will allow you to move to the Step 3

Save and Test	Success . Changes Applied on Database	Success
NEXT STEP		

Step03:



STEP 3. Let's verify you can unlock and reset accounts from your AD, and if your service account has the privileges. If you're connecting a Domain Tree using Global Catalog, please be sure the User Attribute is part of the PAS and is enabled to be Replicated. All the disabled controls corresponds to settings already provided on the previous steps (1-2), they are presented just as a reference. The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
IP Address	10.0.2.231	Ip Address of the Main Domain Controller. (Assigned on the previous Step)
Hostname.	myadsrver	Hostname of the Main Domain Controller (Assigned on the previous Step)
Type of LDAP Connection. (Assigned on the previous Step)	1. Global Catalog	(Selected on the Previous Step). The Test will use the LDAP Port or the Global Catalog Port, according to this selection
LDAP Port	636	LDAP port to Connect to LDAP (Assigned on the previous Step)
Global Catalog Port	3269	Global Catalog port (Assigned on the previous Step)
Adm accountname	scv_c2admin	Account with admin privileges
Users DC String	dc=cordialo,dc=net	Branch on the LDAP directory, from where the system will try to find the users. Example: ou=Person,ou=Corporate,dc=domain,dc=com
User Attribute	employeeNumber	User property, that will be used by the user by dial tones from the phone. This should be numerical. Example: employeeNumber
Attribute Length	5	Standard lenght of the User attribute. This should be the same lenght for all the users. Ex:(In the attribute is 01903399, the Leght =8)

System Updated Successfully

Let's try to unlock and reset one account in your LDAP, the account must be placed on the "Users DC String" OU or deeper.

User Attribute Value

<input type="button" value="Test Unlock Account"/>	Account Name: cn: Jhon Smith	Result: Success
<input type="button" value="Test Reset Account"/>	Account Name: cn: Jhon Smith	Result: Success Temp Pass: "TTab21#\$"

The following parameters should be provided. (All the Property labels in Red). The disabled controls correspond to the settings already provided on the previous step

Users DC String: "DistinguishName" of the OU where the users are located. Users inside other OUs inside of the root OU, will be considered as well.

Example: If in the system we have as User DB String:

ou=Person,ou=Corporate,dc=cordiale,dc=com

It means that users in the following OU will be also included.

ou=UK,ou=Europe,ou=Person,ou=Corporate,dc=cordiale,dc=com

User Attribute: Your accounts in your AD, should have one standard numeric parameter, which will be used to identify the accounts. In the example employeeNumber will be used.

Important:

- The parameter selected should be numeric.
- Should have a standard length for all the users

If you don't have in your AD, one numeric parameter that identifies the users, first consider including this attribute, and assign it every time new accounts are created. Run one script to populate this information for all your current users than does not have yet this attribute filled out.

There are several examples on the web, about scripts to update user accounts parameters. One basic example, is using the command:

Set-ADUser {samaccountname} –employeeNumber {employenumber}.

So you can easily generate the list of commands in a spreadsheet and run the whole list on your Windows Power Shell

Example:

```
PS> Set-ADUser Bobama –employeeNumber 12345678
```

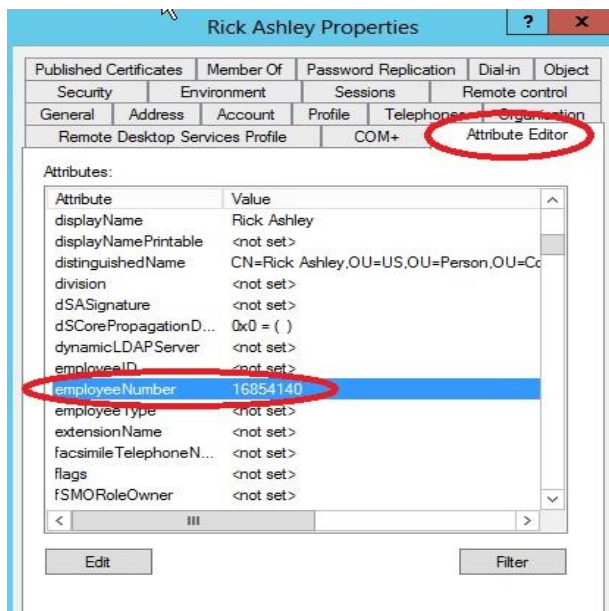
IMPORTANT:

When 1-Global Catalog, is selected as LDAP connection Type, some attributes like "EmployeeID" are not by default part of the Global Catalog Schema. (PAS or Partial Attribute Set)

Please, be sure the attributes selected are part of the Global Catalog.

You can consult this guide to include them on the Global Catalog.

<https://www.ntweekly.com/2017/10/12/add-attributes-global-catalog-server-windows-server-2016/>



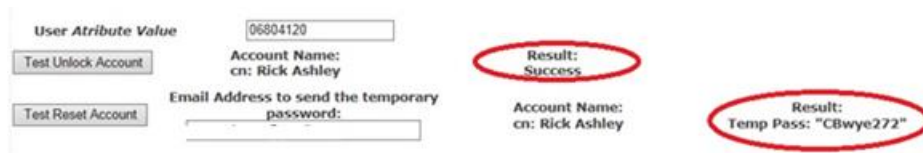
Attribute Length: Number of digits of the numeric attribute. Again, the values on the Users should have always the same length. In the example above, this number is 8.

Save Configuration: Click on “Save”, and you should see “Changes Applied on Database” or “Success”. If you get another message, review the parameters above. The message “Success”, indicates that so far, the connection to the LDAP is successful.



Testing Unlocking and Resetting Accounts.

Once the connection has been validated, you should test if the user provided in the last steps, is able to unlock and reset accounts. Proceed to test with a test account, providing its numeric value for its “User Attribute”. Click on “Test Unlock Account” and “Test Reset Account”



Testing Unlock:

If you get any error message instead of “Success”, review the permissions of your Administrator Account or Service Account. If you got “Success” this means that the user account correspondent to the “EmployeeNumber” (we are using EmployeeNumber just as an example). You can test locking an account on purpose, and then trying to unlock it in this step, then validate on your AD that the account is actually unlocked.

Testing Reset:

You should see the temporary password created, next to the message “Success”

Important: Call2Unlock generates a random password that compliances with the basic security policies for Windows passwords. 8 characters or more, 1 or more numeric chars, 1 or more capital chars

Once the Unlock and Reseat Test are completed, the system will allow us to move on to the step 4

Step04:

Step1

Step2

Step3

Step4

Step5

STEP 4. Let's retrieve the list of user accounts. Call2Unlock will query your AD user objects filtered by OU or Groups. In case of Universal or Nested Groups among a Domain Tree (Parent and Child Domains), we will get all the accounts across the domain that match the criteria of being inside the nested groups belonging to the one set on "Group DC String". All the disabled controls corresponds to settings already provided on the previous steps (1-2-3), they are presented just as a reference. The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
Users DC String	dc=cordialo,dc=net	Branch on the LDAP directory, from where the system will try to find the users. Example: ou=Person,ou=Corporate,dc=domain,dc=com This field was populated on the Step3. If you need to update it, please run the Wizzard Again and update it on Step3
Group DC String	memberOf:1.2.840.113556.1.4.1941:=CN=all 2 unlock users,DC=cordialo,DC=net	Group to filter users, Only the users from this group will be able to use the system. (Leave Blank if you are not using groups to filter Example: memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net For nested groups inside a Universal Group. Please add this string before your Group String memberOf:1.2.840.113556.1.4.1941:= So the complete Group DC including nested groups would be for the example: memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net

Save Configuration

...

In this section you have to provide the group (in a Multidomain Environment, could be a Universal Group), it will include all the nested groups members of the parent group.

Group DC String: Group to filter users, Only the users from this group will be able to use the system.
(Leave Blank if you are not using groups to filter)

Example: **memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net**

IMPORTANT:

When 1-Global Catalog, is selected as LDAP connection Type, the Group DC String will be used to filter the users across the domain. So this group must be a "Universal Group".

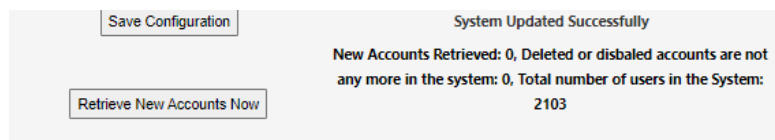
NESTED GROUPS IN EACH DOMAIN

Another possibility is to enroll the members of some Global Groups you may already have in each AD server. In this case you just need to make those Global Groups members of the Universal Group. This is called "members of NESTED groups". In order to make the group filter reach the members of the NESTED groups, you have to include the code parameter "1.2.840.113556.1.4.1941"

Example:

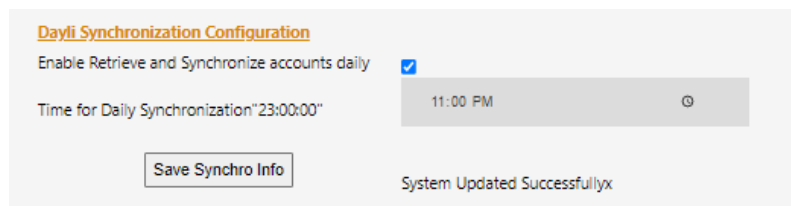
memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net

Once you saved your changes, click on "Retrieve New Accounts Now". If this is the first time running the assistant, all the accounts will be considered new, otherwise the system will just add the new ones, and remove from its internal database the disabled accounts.



The screenshot shows a light gray background with a white box containing a 'Save Configuration' button at the top left. Below it is a 'Retrieve New Accounts Now' button. To the right of these buttons, the text 'System Updated Successfully' is displayed. Below this, a status message reads: 'New Accounts Retrieved: 0, Deleted or disabled accounts are not any more in the system: 0, Total number of users in the System: 2103'.


This process can be configured to be ran daily at a specific hour. So the new accounts created on the Active Directory will be able to use Call2Unlock no later than the next day.




The screenshot shows a 'Daily Synchronization Configuration' dialog box. It has a title bar with the text 'Daily Synchronization Configuration'. Inside, there is a checkbox labeled 'Enable Retrieve and Synchronize accounts daily' which is checked. Below this, there is a text field labeled 'Time for Daily Synchronization' with the value '23:00:00'. To the right of this field is a time picker showing '11:00 PM'. At the bottom left is a 'Save Synchro Info' button. At the bottom right, the text 'System Updated Successfullyx' is displayed.

You can run this process manually any time If you just created new accounts on your AD and you want them to be able to use the system immediately. Go to LDAP/ACCOUNT SYNCHRONIZATION).

Finally, you may click on “Run Report”, to verify we get the list of accounts. You can search for a specific account as well using the filter box.

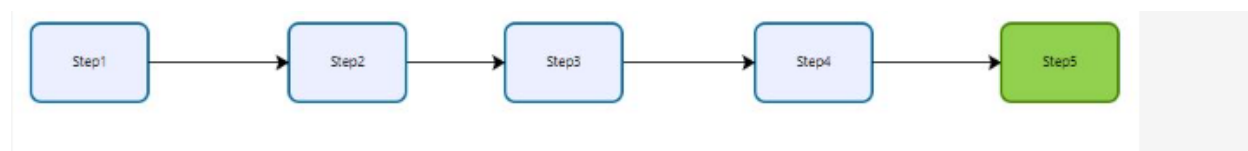
Find Accounts by name (blank to retrieve all)  [Get Report](#)

User Accounts				
ID	Username	Domain	Retrieveddate	InternalPhone
154 Edit	root20	cordialo.net	2022-11-05 13:56:50	
150 Edit	root16	cordialo.net	2022-11-05 13:56:50	
151 Edit	root17	cordialo.net	2022-11-05 13:56:50	
152 Edit	root18	cordialo.net	2022-11-05 13:56:50	
153 Edit	root19	cordialo.net	2022-11-05 13:56:50	
149 Edit	root15	cordialo.net	2022-11-05 13:56:50	
143 Edit	root9	cordialo.net	2022-11-05 13:56:50	
144 Edit	root10	cordialo.net	2022-11-05 13:56:50	
145 Edit	root11	cordialo.net	2022-11-05 13:56:50	
146 Edit	root12	cordialo.net	2022-11-05 13:56:50	

 Export to CSV 146 rows Page 1

Once completed, we can move forward to the 5th and last step of our configuration assistant.

Step05:



STEP 5. Almost Done. Finally, let's complete the security and delivery options and Apply the Changes! Some Controls may be disabled, since you already provided that info on the previous steps (1-4). The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
User Attribute	employeeNumber	User property, that will be used by the user by dial tones from the phone. This should be numerical. Example: employeeNumber
Attribute Length	5	Standard lenght of the User attribute. This should be the same lenght for all the users. Ex: (In the attribute is 01903399, the Leght =8)
Type of User Confirmation Attribute	<div>1. In AD </div>	<div>0. In Call2unlock DB. The system will use the PIN number generated by the user in the self service portal of call2unlock.</div> <div>1. In AD. Means that the confirmation pin is placed in the AD, and you will need to fill the User Attribute for Confirmation Information.</div> <div>2. MFA Radius Server. Means that the user will validate with PIN + Token Number provided by the Second Factor Authentication provider (like Google Authenticator) thru a Radius Server. The Radius Server could be a local Radius running on the Call2unlock server or any external Radius server existent in the company. Go to the Radius Configuration Section to make this working</div>
User Attribute for Confirmation	employeeID	Just in case Type of User Confirmation Attribute is "In AD". User property, that will be used to confirm the action by the user by dial tones from the phone. This should be numerical. Example: 4 last digits of SSN, or employeeID
Attribute Length for Confirmation	4	Just in case Type of User Confirmation Attribute is "In AD". Standard lenght of the User attribute for confirmation This should be the same lenght for all the users. Ex: (In the attribute is 1157, the Leght =4)
Users DC String	dc=oordialo,dc=net	<div>Branch on the LDAP directory, from where the system will try to find the users. Example: ou=Person,ou=Corporate,dc=domain,dc=com</div> <div>This field was populated on the Step3. If you need to update it, please run the Wizzard Again and update it on Step3</div>

In this step you will configure the rest of configuration parameters, like: User validation place (Active Directory, Call2unlockDB, 2FA), Password Delivery (Audio, SMS, Email), Password Complexity, etc (All the Property labels in Red). The disabled controls correspond to the settings already provided on the previous step

Max Number of Failed attempts	7	When users fails providing the PIN number, this is the max fails in one day. After failing this number of times this account will be included in a black list for security. Every night a cron process release the accounts from the black list (Default value: 5 Fails Attempts)
AD Password Lenght	8	Pasword Complexity: Length for the password. Will be used to generate temporary passwords. (Default 8)
AD Password Capitals	3	Pasword Complexity: Number of desired capital characters whitin the temporary passwords. (Default 3)
AD Password Loweres	2	Pasword Complexity: Number of desired lower characters whitin the temporary passwords. (Default 3)
AD Password Numerics	3	Pasword Complexity: Number of desired numeric characters whitin the temporary passwords. (Default 2)
AD Password Specials	0	Pasword Complexity: Number of desired special characters whitin the temporary passwords. (Default 0)
Delivery Mode	1. Only Audio ▼	Delivery Modes: Choose one mode from the list.
Numbers Of Chars First Media	8	Number of characters will be delivered in the first media. RULES: This number should be always grater than 1, or should be the same than the Password Lenght in case the delivery option includes only one media.
Numbers Of Chars Second Media	0	Number of characters will be delivered in the second media, RULES: Use only in case the delivery mode, consist in two diferent media,, otherwise set to 0. This number should be always grater than 1. The sum of this number plus the first chars media should be the same than Password Lenght
Administrators Email	admin@mydomain.com	Email address, or DL where the security notifications or alamrs will be sent to.

Save Configuration ...

Once you save all the parameters, click on “Apply Configuration and Generate IVR Script”, then the system will re-generate the IVR scripts based on this configuration.

CONGRATULATIONS!. Your Active Directory Infrastructure is completely integrated to call2unlock. You can access to all the settings provided on five last steps on the all in one window calles “LDAP CONFIGURATION”.

4. LDAP Configuration

If you already ran the LDAP Configuration Wizard from the last section, this LDAP configuration window, will present the whole collection of data, so you can edit and test all at once on this unique place.

Go to the “LDAP / CONFIGURATION” menu option. You should get a list of parameters like the one below. Most of the options are explained in the description column

Property	Value	Description
IP Address	10.0.2.230	Ip Address of the LDAP Server
Hostname	myadserver	Hostname of the LDAP Server
Type of LDAP Connection	1. Global Catalog ▼	<p>0. Active Directory Server. Use this option if you are going to use a unique Domain. Only the LDAP port will be used to connect the Active Directory Server.</p> <p>1. Global Catalog. Use this option if you have a Forest with multiple Domains. The Global catalog Port, on the root domain AD server will be used to search objects and the LDAP port to unlock and reset accounts. Please be sure to include the each domain name server into the /etc/hosts file .</p>
LDAP Port	636	LDAP port to Connect to LDAP (389 by default, 636 Recommended)
Global Catalog Port	3269	Global Catalog port (3268 by default, 3269 Recommended)
Adm accountname	Administrator	Account with admin privileges
Adm password		Password of the Account with admin priv.
Adm DC string	cn=Users,dc=cordiale,dc=net	DC String for the Account with admin priv. Example. cn=Adminuser,dc=domain,dc=com
User Attribute	employeeNumber	User property, that will be used by the user by dial tones from the phone. This should be numerical. Example: employeeNumber
Attribute Length	5	Standard lenght of the User attribute. This should be the same lenght for all the users. Ex:(In the attribute is 01903399, the Leght =8)

The following parameters should be provided.

IP Address: IP Address of the Active Directory Server. If you want to work with a complete domain forest, this IP is the root domain AD server with a Global Catalog running.

Hostname: Name of the Active Directory Server. (This value is just informative, will not be considered as a parameter for the LDAP connection).

Type of LDAP Connection: This selection allows us to work with a complete Active Directory Forest, including child domains, or directly with a single domain AD server.

0. Active Directory Server. Use this option if you are going to use a unique Domain. Only the LDAP port will be used to connect the Active Directory Server.

1. Global Catalog. Use this option if you have a Forest with multiple Domains. The Global Catalog Port, on the root domain AD server will be used to search objects and the LDAP ports to unlock and reset accounts on all the Domain Controllers

LDAP Port: LDAP port for your Active Directory. By default, 389. Call2unlock uses LDAPS (Secure Ldap) so 636 will be recommended.

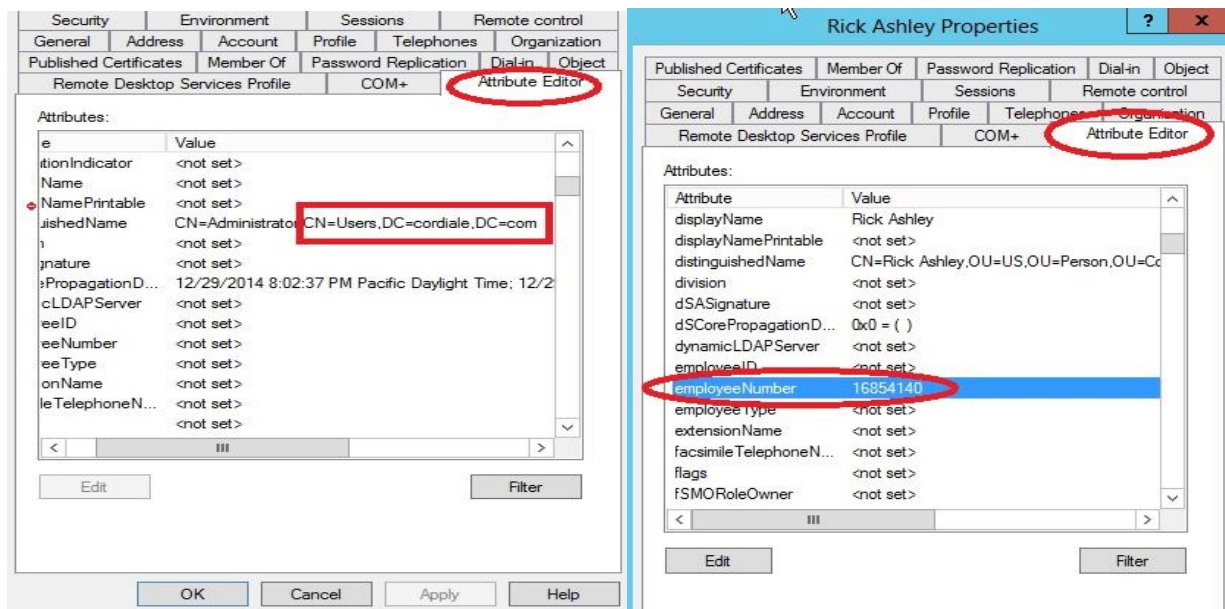
Global Catalog Port: Port used for the Global Catalog (In case 1. Global Catalog is selected as Type of LDAP Connection). Typically port 3269 for secure connections

Adm Accountname: This account should have enough privileges to unlock or reset accounts in your active directory. Typically a service account.

Adm Password: AD Password for the adm account.

Adm DC string: This is the distinguished name of the OU where the Admin LDAP Account belongs. In order to get this information, go to your AD server, in “Active Directory Users and Computers”, go to “Attribute Editor”, and copy the distinguished name, but just from the OU, not taking the account name

In the picture below, from the string “cn=Administrator,cn=Users,dc=cordiale,dc=com” just “cn=Users,dc=cordiale,dc=com” has been taken



AD Servers List: This is the list of AD Servers List. If you are using the Global Catalog and a Multi-Domain Environment, write the IP, Server name and a semi-colon for each domain controller. This content will be added to the /etc/hosts file Example of Content of this field:

10.0.2.230 domain.net;

10.0.3.230 child1.domain.net;

10.0.4.230 child2.domain.net

The system will add at the end of the /etc/hosts file something like:

10.0.2.230 domain.net

10.0.3.230 child1.domain.net

10.0.4.230 child2.domain.net

User Attribute: Your accounts in your AD, should have one standard numeric parameter, which will be used to identify the accounts. In the example employeeNumber will be used.

Important:

- The parameter selected should be numeric.
- Should have a standard length for all the users

If you don't have in your AD, one numeric parameter that identifies the users, first consider including this attribute, and assign it every time new accounts are created. Run one script to populate this information for all your current users than does not have yet this attribute filled out.

There are several examples on the web, about scripts to update user accounts parameters. One basic example, is using the command:

Set-ADDUser {samaccountname} –employeeNumber {employenumber}.

So you can easily generate the list of commands in a spreadsheet and run the whole list on your Windows Power Shell

Example:

```
PS> Set-ADUser Bobama –employeeNumber 12345678
```

IMPORTANT:

When 1-Global Catalog, is selected as LDAP connection Type, some attributes like "EmployeeID" are not by default part of the Global Catalog Schema. (PAS or Partial Attribute Set)

Please, be sure the attributes selected are part of the Global Catalog.

You can consult this guide to include them on the Global Catalog.

<https://www.ntweekly.com/2017/10/12/add-attributes-global-catalog-server-windows-server-2016/>

Attribute Length: Number of digits that the parameter above has. Again, the values on the Users should have always the same length. In the example above, this number is 8.

Type of User Confirmation Attribute	1. In AD	<p>0. In Call2unlock DB. The system will use the PIN number generated by the user in the self service portal of call2unlock.</p> <p>1. In AD. Means that the confirmation pin is placed in the AD, and you will need to fill the User Attribute for Confirmation Information</p> <p>2. MFA Radius Server. Means that the user will validate with PIN + Token Number provided by the Second Factor Authentication provider (like Google Authenticator) thru a Radius Server. The Radius Server could be a local Radius running on the Call2unlock server or any external Radius server existent in the company. Go to the Radius Configuration Section to make this working</p>
User Attribute for Confirmation	employeeID	Just in case Type of User Confirmation Attribute is 'In AD'. User property, that will be used to confirm the action by the user by dial tones from the phone. This should be numerical. Example: 4 last digits of SSN, or employeeID
Attribute Length for Confirmation	4	Just in case Type of User Confirmation Attribute is 'In AD'. Standard length of the User attribute for confirmation. This should be the same length for all the users. Ex: (In the attribute is 1157, the length = 4)
Users DC String	dc=cordialo,dc=net	Branch on the LDAP directory, from where the system will try to find the users. Example ou=Person,ou=Corporate,dc=domain,dc=com
Group DC String	memberOf:1.2.840.113556.1.4.1941:=CN=c all 2 unlock users,DC=cordialo,DC=net	<p>Group to filter users, Only the users from this group will be able to use the system. Leave Blank if you are not using groups to filter Example: memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net</p> <p>For nested groups inside a Universal Group. Please add this string before your Group String memberOf:1.2.840.113556.1.4.1941:=</p> <p>So the complete Group DC including nested groups would be for the example: memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net</p>

Type of User Confirmation Attribute : Once the user is found in AD, in order to unlock or reset the password, the user should insert a PIN number. This attribute is used to determinate where this PIN number will be placed

0. Call2unlock Database
1. Active Directory (A User account attribute in AD)

2. MFA. Radius Server. You should previously configure the local or external RADIUS integration to make use of this feature. It is explained in the RADIUS configuration section of this manual

User Attribute for Confirmation: In case the option 1 (Active Directory) was selected as Type of User Confirmation Attribute, the name of the attribute should be specified here.

Attribute Length for Confirmation: Number of digits of the Attribute for confirmation. All the users should have this attribute with the same number of digits.

Users DC String: "DistinguishName" of the OU where the users are located. Users inside other OUs `

Example: If in the system we have as User DB String:

`ou=Person,ou=Corporate,dc=cordiale,dc=com`

It means that users in the following OU will be also included.

`ou=UK,ou=Europe,ou=Person,ou=Corporate,dc=cordiale,dc=com`

Group DC String: Group to filter users, Only the users from this group will be able to use the system. (Leave Blank if you are not using groups to filter

Example: `memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net`

IMPORTANT:

When 1-Global Catalog, is selected as LDAP connection Type, the Group DC String will be used to filter the users across the domain. So this group must be a "Universal Group".

NESTED GROUPS IN EACH DOMAIN

Another possibility is to enroll the members of some Global Groups you may already have in each AD server. In this case you just need to make those Global Groups members of the Universal Group. This is called "members of NESTED groups". In order to make the group filter reach the members of the NESTED groups, you have to include the code parameter "1.2.840.113556.1.4.1941"

Example:

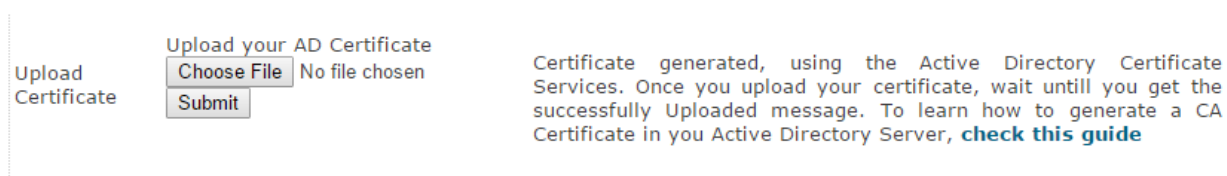
`memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net`

Max Number of Failed Attempts: If for some reason the user fails providing the correct PIN number, the system includes this user in a black list, and send an email alert to the administrator. On this field, the administrator configures the max number of failed attempts.

Administrator's Email: All the notifications, especially when a user has been included in the black list, will be sent to this email account. It could be a normal email or a distribution list.

**** Note:** Once one user is blacklisted, only the administrator can release the account, to be able to use call2unlock again. This option is available in the End User Edition module.

Upload Certificate: You should upload the pem certificate previously generated on your AD. This certificate is needed to perform actions like reset passwords from call2unlock.



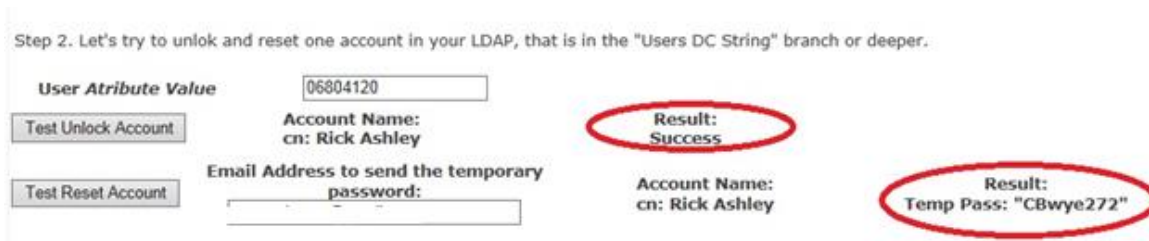
To generate this certificate following the manual , “Generating the AD Certificate”, that is available on the web site of Call2Unlock <http://www.call2unlock.com/documentation/>

Testing Connection: Click on “Save and Test”, and you should see “Changes Applied on Database” and also “Success”. If you get another message, review the parameters above. The message “Success”, indicates than so far, the connection to the LDAP is successful.



Testing Unlocking and Resetting Accounts.

Once the connection has been validated, you should test if the user provided in the last step, is able to unlock and reset accounts.



Testing Unlock:

If you get any error message instead of "Success", review the permissions of your Administrator Account or Service Account. If you got "Success" this means that the user account correspondent to the "EmployeeNumber" (we are using EmployeeNumber just as an example). You can test locking an account on purpose, and then trying to unlock it in this step, then validate on your AD that the account is actually unlocked.

Testing Reset:

You should see the temporary password created, next to the message "Success"

Important: Call2Unlock generates a random password that compliances with the basic security policies for Windows passwords. 8 characters or more, 1 or more numeric chars, 1 or more capital chars

Save Configuration:

Once all your test has been successful, press the button "Save Configuration".

You should get the message "System Updated Successfully" marked in red.

The configuration will be only saved if all the previous tests were successful, otherwise the call2unlock won't allow the user to save the configuration

The screenshot displays the Call2Unlock application interface. At the top, a 'Save and Test' button is visible. Below it, the text 'Changes Applied on Database' is shown. A 'Success' message is highlighted with a blue oval. The interface then prompts the user to 'Step 2. Let's try to unlock and reset one account in your LDAP, that is in the "Users DC String" branch or deeper.' Below this, there are two main sections. The first section, 'User Attribute Value', shows a text input field with '06804120'. Below it, a 'Test Unlock Account' button is present. The second section, 'Test Reset Account', shows a text input field for 'Email Address to send the temporary password:'. Below it, a 'Test Reset Account' button is present. To the right of these sections, there are two 'Result: Success' messages, each highlighted with a blue oval. The first result is for 'Account Name: cn: Rick Ashley'. The second result is for 'Account Name: cn: Rick Ashley' and 'Temp Pass: "CBwye272"'. Below these results, a note states: 'Note: The temporary password should be sent to the email provided by the user. Try to login to your Active Directory Using the temporary password. It should work. Also the system should ask you to change the temporary password.' At the bottom, there is a 'Step 4. Save Your Configuration. Be sure that you have test following the 2 steps above, successfully, otherwise the configuration wont be solved'. Below this, there are 'Save Configuration' and 'Cancel' buttons. A 'System Updated Successfully' message is highlighted with a red oval.

Save and Test

Changes Applied on Database

Success

Step 2. Let's try to unlock and reset one account in your LDAP, that is in the "Users DC String" branch or deeper.

User Attribute Value

06804120

Test Unlock Account

Account Name: cn: Rick Ashley

Test Reset Account

Email Address to send the temporary password:

Result: Success

Account Name: cn: Rick Ashley

Result: Temp Pass: "CBwye272"

Note: The temporary password should be sent to the email provided by the user. Try to login to your Active Directory Using the temporary password. It should work. Also the system should ask you to change the temporary password.

Step 4. Save Your Configuration. Be sure that you have test following the 2 steps above, successfully, otherwise the configuration wont be solved

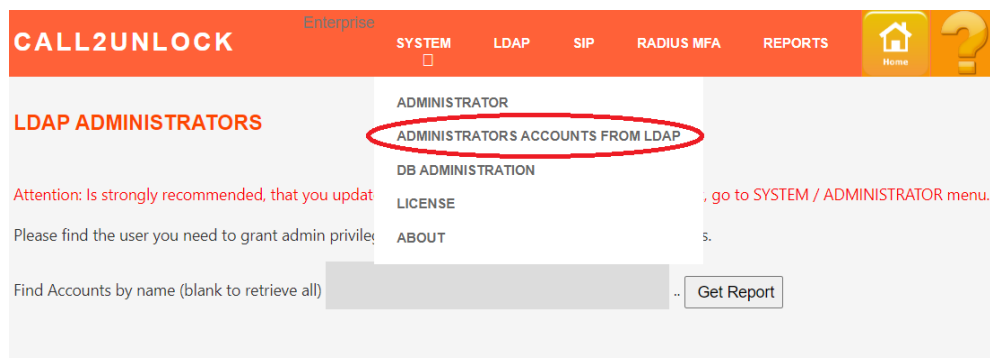
Save Configuration

Cancel

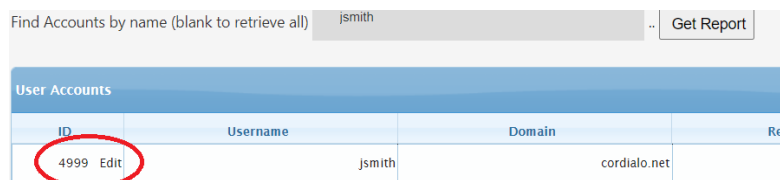
System Updated Successfully

5. LDAP ADMINISTRATORS

Once you have completed your LDAP configuration, you have your accounts synchronized with your AD. It's time to choose, which accounts will have admin privileges, so we won't have a unique root administrator account. To add a new Administrator user from your AD, go to SYSTEM/ADMINISTRATOR ACCOUNTS FROM LDAP



Then you can search for your user, and click on "Get Report". You will get the user list from your search. You have to Edit this account to assign it admin privileges.



USER ACCOUNT EDITION

Attention: Is strongly recommended, that you update the administrator account's password. To do it, go to SYSTEM / ADMINISTRATOR menu.



Now the new administrator account can go to the initial page <https://youripaddress>

Then the user should try to authenticate USING HIS/HER AD Credentials

If the authentication is successfully. (The user authenticated with the right AD password, and also he/she was already set as Administrator on the last step, the user should get the HOME page of the system, with the message at the top “Connection to LDAP service successfully”

6. SIP CONFIGURATION WIZARD:

This is the also a very important section. Here you should be able to configure and test the necessary parameters and credentials to integrate Call2unlock with your Corporate PBX. This assistant consists in a series of 03 steps that will guide you to trough the process and will detect any issues and the suggested remediation. **Previously, is necessary to create a SIP trunk account on your PBX, to be registered to the Call2unlock IP address (Asterisk PBX).** This configuration may be different on each PBX brand and model. For Cisco CUCM, you can consult this manual:

<https://www.thecollabguru.com/integrating-cucm-with-asterisk-using-sip-trunk/>

Step01: Connectivity Test. The System Verifies the involved ports are accessible from call2unlock to your IP PBX


Step02: SIP Registration: The System Verifies that the SIP trunk account created on your PBX is registered against call2unlock. So from the signaling prospective, the both PBX systems (Your IP PBX and Call2unlock) will communicate each other

Step03: Generate the Internal Dial plan: You will configure there the Prefix for the calls going from your IP PBX to Call2unlock, so Call2unlock can process the call through its IVR.

Once all the 03 steps are completed, Call2unlock will generate the IVR script, which will be presented to the user every time he/she dials the Call2Unlock internal extension of DID phone number, getting the system ready to use.

Go to the “SIP / SIP CONFIGURATION ASSISTANT” menu option. You should get the Step1 page

Step01:



STEP 1. Let's verify you have connectivity to your IP PBX Infrastructure. The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
PBX IP Address	10.0.0.31	Ip Address of PBX, Publisher or Subscriber
SIP Signaling Protocol	1.UDP	0. TCP Protocol for Signaling. 1. UDP Protocol for Signaling.
Signaling Port	5060	Port Number for SIP Signaling (5060 by Default)

Test SIP Signaling port Test: Success

Save Update Status: Changes Applied on Database

NEXT STEP

PBX IP Address: IP address of your Corporate PBX

SIP Signaling Protocol: You have to select between TCP or UDP (according to what protocol your PBX uses for signaling).

Signaling Port: Port Number for Signaling (Most PBX will use 5060 or 5061)

Once you fill the required information, press “Test”. If no network issues (such as firewall blocking), you should get “Success” as result message.

If the test is successfully you will be able to Save your configuration. You will get “Changes Applied on Database” as message. Then click on NEXT STEP.

Step02:

```

graph LR
    Step1[Step1] --> Step2[Step2]
    Step2 --> Step3[Step3]

```

STEP 2. Let's try to register the SIP account to be used to send calls from your PBX to Call2Unlock. Please create the account with the credentials Provided in your PBX as a SIP Friend account. This step will create the account inside Call2unlock to be authenticated on your PBX. All the disabled controls corresponds to settings already provided on the previous step (Step1). The property names in red contain the enabled controls where you have to provide or update your settings

Property	Value	Description
PBX IP Address	10.0.0.31	Ip Address of PBX, Publisher or Subscriber
SIP Signaling Protocol	1.UDP	0. TCP Protocol for Signaling. 1. UDP Protocol for Signaling.
Signaling Port	5060	Port Number for SIP Signaling (5060 by Default)
PBX Account	cordial	Account name of the SIP trunk created in the Corporate PBX
PBX Account Password	Password of the Account of the SIP Trunk

Save

Test

Changes Applied on Database

SIP Trunk Authentication Test

SIP Config Pushed

Success

NEXT STEP

Only the controls with red labels are required. The ones in black labels are disabled and were already provided in the previous step (Step 1)

PBX Account: User account for the user created in the Corporate PBX

PBX Account Password: Password of the account created on the Corporate PBX

Once you fill the required information, press “Save”, you should get the message “SIP Config Pushed”, so the new SIP account has been also created in Call2unlock as SIP account.

Then click “Test”, to validate the account is registered on your Corporate PBX. You should get “Success” as result.

Step03:



STEP 3. Let's try to generate The Internal Dialplan to get the Calls From your PBX. Then you will need to send a call from your PBX to Call2unlock Trough the SIP trunk created on Step2. Once you get the Call2unlock Wellcome Audio, we can consider all the SIP Configurations completed. All the disabled controls corresponds to settings already provided on the previous stepw (Steps 1 and 2). The property names in red contain the enabled controls where you have to provide or update your settings

Prefix For Internal Calls	8888	This prefix will indetify if the calls comes from the internal PBX. This should be configured in the PBX dialplan
Allow All Internal	<input checked="" type="checkbox"/>	If is checked, users are allowed to call from every internall extension. If not, users are only allowed to call from their extensions, configured in thPrefix for PSTN Callse user Accounts module, by themselves or by the administrator
Prefix for PSTN Calls	9999	This prefix indicates the call is comming from the PSTN. This should ne configured in the PBX dialplan
Number of Digits for the Prefix	4	Number de digits for the prefix, to identify prefix from real numbers
Language for General Audios	es	Language for IVR instructions. All the messages will be displayed in this language en= English, es = Spanish.
Transfer to Help Desk Dialplan		Dialplan Instructions to Redirect the Call to Help Desk if the user has troubles to use the system. Single quotes are not allowed, user double quotes insted. Example \$AGI->set_callerid("544"); \$AGI->exec("Dial","SIP/c2u/121212");

Only the controls with red labels are required. The ones in black labels are disabled and were already provided in the previous step (Step 2)

Allow All Internal: Check this option, in case you want to allow all the employees to unlock their accounts from any internal extension. Otherwise, the users should provide the internal extension they are going to dial from, this can be done in the self-web portal, and will be explained later.

Prefix for Internal Calls: Prefix used for Internal extension, when sending calls from the PBX to Call2Unlock.

Prefix for PSTN Calls: Prefix used for external phones, when sending calls from the PBX to call 2 unlock

Number of Digits for the Prefix: Number of digits to be considered as just prefix for external calls.

Language for General Audios: Language for the general audios (en = English, es = Spanish)

Transfer to Help Desk Dial plan: Dial plan Instructions to Redirect the Call to Help Desk if the user has troubles to use the system. Example of Dial plan

```
set_callerid("544");  
exec("Dial","SIP/c2u/121212");
```

In that case Call2Unlock will redirect the call to the extension “121212” to the corporate PBX towards the SIP trunk called C2U. For more information about this configuration consult with Call2Unlock Support.

Once you fill the required information, press “Save”, you should get the message “SIP Config Pushed”

Now is time to send a call from your IP PBX (Using the Prefix). It is recommended opening an asterisk console (asterisk –rvvv) from an ssh session in call2unlock to check if we are getting the signaling messages. We should get audio as well (The welcome message from Call2unlock). If you get the signaling messages and dead air, please check the RTP ports

Important: Since Call2unlock uses asterisk as IP PBX, it is by default configured to get and send audio packages (RTP), in the range of 10000 and 20000 UDP. If your IP PBX uses a different range, (As an example Cisco CUCM uses the range UDP 16384 – 32767. It may require to adjust Call2unlock’s RTP ports to match the ones from your IP/PBX. It is usually located on the file /etc/asterisk/rtp.conf. Consult our experts if you need assistance on this configuration.

7. CONFIGURING YOUR CORPORATE PBX

Generally, in your PBX, you should execute the following 3 steps.

1. **Create a SIP Trunk** : Be sure to set "UDP" as the "Outgoing Transport Type", and provide the Call2Unlock server IP address. It uses ports 5060 UDP for signaling and 10000 – 20000 for RTP.
2. **Create a Dial Plan**: Create an internal number where your associates will call, and redirect to the extension "8888" thru the new trunk created above. (8888 is the default value in the SIP configuration, **Prefix for Internal Calls**, you can change this in SIP / CONFIGURATION).
3. **Test the Trunk and Dialplan**:
 - Open the asterisk console in call2unlock executing in the Linux command prompt **"asterisk -rvvv"**
 - Send the call from your PBX. At least you should be able to receive traffic in the console, something similar like the output below, if you don't, review your SIP trunk and the dial plan in your PBX.

```
Call2Unlock*CLI>
== Using SIP RTP CoS mark 5
-- Executing [8888@fromcustomerpbx:1] Answer("SIP/9999-00000000", "") in new stack
> 0x7f1aac00e240 -- Probation passed - setting RTP source address to 192.168.0.3:20442
-- Executing [8888@fromcustomerpbx:2] Set("SIP/9999-00000000", "(CALLERID(num)=88880016961")
in new stack
-- Executing [8888@fromcustomerpbx:3] Set("SIP/9999-00000000", "CALLFROM=Internal") in new
stack
-- Executing [8888@fromcustomerpbx:4] AGI("SIP/9999-00000000", "zz_selfservicead1example.agi")
in new stack
Call2Unlock*CLI>
```

8. SIP CONFIGURATION

In this section you will configure the parameters of the sip trunk between Call2Unlock and your IP PBX. If you already ran the SIP Configuration Wizard from the last section, this SIP configuration window, will present the whole collection of data, so you can edit and test all at once on this unique window..

Go to "SIP / CONFIGURATION" menu option, and fill the following information:

PBX IP Address: IP address of your Corporate PBX

PBX Account: User account for the user created in the Corporate PBX

PBX Account Password: Password of the account in the Corporate PBX

Allow All Internal: Check this option, in case you want to allow all the employees to unlock their accounts from any internal extension. Otherwise, the users should provide the internal extension they are going to dial from, this can be done in the self-web portal, and will be explained later.

Prefix for Internal Calls: Prefix used for Internal extension, when sending calls from the PBX to call2unlock

Prefix for PSTN Calls: Prefix used for external phones, when sending calls from the PBX to call2unlock

Number of Digits for the Prefix: Number of digits to be considered as just prefix for external calls.

Language for General Audios: Language for the general audios (en = English, es = Spanish)

Transfer to Help Desk Dial plan: Dial plan Instructions to Redirect the Call to Help Desk if the user has troubles to use the system. (If he or she failed providing the pin or the ID) Example of Dial plan

```
set_callerid("544");  
exec("Dial","SIP/c2u/121212");
```

In that case Call2Unlock will redirect the call to the extension “121212” in the corporate PBX towards the SIP trunk called C2U. For more information about this configuration consult with Call2Unlock Support.

Custom Audios: In this section you can upload also custom audios, to replace the default ones on the system. You can listen the current ones, clicking in the link in blue at the right. And you can replace them choosing the files from the local computer, and clicking Submit, in each file.

The account that you are trying to unlock is	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Account
If you want to unlock this account, press 1. If this is not your account, press 0	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Confirmation
The account, has been successfully unlocked	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Success
The code you have dialed is duplicated. Please contact the system administrator	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Duplicated
There is not any user with that number. Please, be sure about the number, and call again	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Not Found
The pin number you have dialed, does not correspond to the current user	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Failed PIN
Please, insert your pin number	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Insert PIN
This telephone, is not allowed to use the System	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Phone not Allowed
Thank You!	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Thank you

The files should be saved as WAV file in 16 bit 8000 Hz mono.

After saving the changes, you should get the success message

Changes Applied on Database
System Updated Successfully

Step 2. Now test from your PBX sending a call to 30029190 using the trunk to call2unlock you have created into your PBX.

Is necessary to safe and re-generate the LDAP configuration also, every time changes are made in this section.

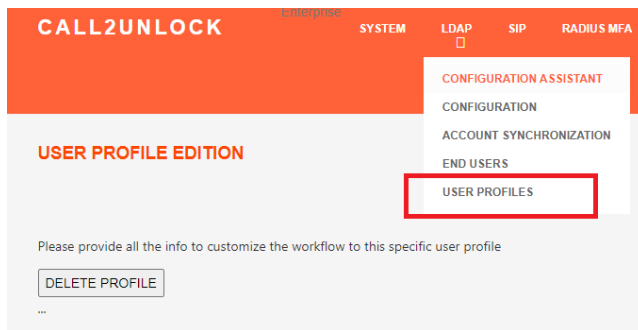
ALSO: If the Language has been changed, the whole system needs to be restarted

9. CUSTOM PROFILES

Many organizations require to assign different workflows for different group of users. For example:

Group	Location	Authentication	Delivery mode
C2uusers3	CN=c2uusers3,CN=Users,DC=td,DC=cordiali,DC=net	AD Pin	Email
C2uusers1	CN=c2uusers1,CN=Users,DC=cordiali,DC=net	C2U DB	SMS
C2uusers2	CN=c2uusers2,CN=Users,DC=td,DC=cordiali,DC=net	MFA Google Auth	Audio

To create see the list of profiles go to LDAP / USER PROFILES



If you still have not created any profile, the system by default will have all your users in a profile called "default". This default profile contains all the configurations provided to the LDAP configuration.




USER PROFILES

USER PROFILES ALLOW US TO DEFINE DIFERENT RULES OR WORKFLOWS FOR DIFERENT GROUP OF USERS

[NEW PROFILE](#)

User Profiles				
ID		ProfileName	Descritpion	ActiveUsers
1	Edit	default	default Profile	0
30	Edit	third	Users from the group c2uusers3 in the TD Chi	2001
31	Edit	c2uusers1	Users from the group c2uusers1 in the Main D	997
32	Edit	c2users2	Users from c2users2 from Located in Child TD	993

You can click on any element from the list to display the profile details:

Property	Value	Description
ID	31	Profile ID
Profile Name	c2uusers1 	Short name for the profile. Please only lower cases and regular characters
Profile Description	Users from the group c2uusers1 in the Main Domain Controller, AD Authentication (4 digits) and SMS Delivery	Provide a short description for this users profile
Group DC string for Profile Users	CN=c2uusers1,CN=Users,DC=cordiali,DC=net	Please, be sure this group is member of the main Group DC string configured on ldap configuration Otherwise no users will be part of this profile Also be sure that each user only belongs to one group assigned as profiler group, Otherwise the user will belong only to the last profile updated
User Attribute	employeeNumber	User property, that will be used by the user by dial tones from the phone. This should be numerical. Example: employeeNumber
Attribute Length	5	Standard lenght of the User attribute. This should be the same lenght for all the users. Ex:(In the attribute is 01903399, the Leght =8)
Type of User Confirmation Attribute	1. In AD 	<p>0. In Call2unlock DB. The systemm will use the PIN number generated by the user in the self service portal of call2unlock.</p> <p>1. In AD. Means that the confirmation pin is placed in the AD, and you will need to fill the User Attribute for Confirmation Information</p> <p>2. MFA Radius Server. Means that the user will validate with PIN + Token Number provided by the Second Factor Auhtentication provider (like Google Authenticator) thru a Radius Server. The Radius Server could be a local Radius running on the Call2unlock server or any external Radius server existent in the company. Go to the Radius Configuration Section to make this working</p>
User Attribute for Confirmation	employeeID	Just in case Type of User Confirmation Attribute is 'In AD'. User property, that will be used to confirm the action by the user by dial tones from the phone. This should be numerical. Example: 4 last digits of SSN, or employeeID
Attribute Length for Confirmation	4	Just in case Type of User Confirmation Attribute is 'In AD'.Standard lenght of the User attribute for confirmation This should be the same lenght for all the users. Ex:(In the attribute is 1157, the Leght =4)
Delivery Mode	3. Only SMS 	Delivery Modes: Choose one mode from the list

Also you can customize the audio messages for the IVR per each profile.

There is no a mobile phone assigned to this user in the system. Please contact the administrator	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	There is no a mobile phone
This account, has been temporarily disabled for security reasons. Please contact the administrator	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Account in Blacklist.
We are going to repeat again.	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Repat the Temporal password.
	IMPORTANT	<p>If the controls to upload the audio file is disabled. Is because that audio is general purpose. Please go to SIP Configuration and Upload that audio, if you need to customize it. Be aware that will impact all profiles</p> <p>ALSO: If the Language has ben changed, the whole system needs to be restarted. .</p>

At the bottom of this screen, you have the controls to "Save the Configuration". It will regenerate a custom IVR script dedicated to this profile, containing all the options

Also you have the button to retrieve the Users that match the group filter criteria, clicking on "Retrieve Accounts for the Profile". It will show you how many users from the total till be running this custom workflow

Changes Applied on Database
 Accounts that will move tho the profile: 997,
 Total number of users in the System: 3991

Find Accounts by name (blank to retrieve all the potential members of the Profile)

User Accounts				
ID		Username	Domain	Profile
1	Edit	dkapp	cordiali.net	c2uusers1
4	Edit	jam ith	cordiali.net	c2uusers1
2	Edit	nvillegas	cordiali.net	c2uusers1

Once you're done with your changes. You can apply the changes to the users of the profile. Meaning that those users will have the profile assigned to its entity ready to be read by the IVR.

Profile Updated for the selected users

CREATING CUSTOM PROFILES

On the same profile list screen, there is a button called “NEW PROFILE”. Once you click on that you have the form to complete the information for this new profile.

USER PROFILES

USER PROFILES ALLOW US TO DEFINE DIFERENT RULES OR WORKFLOWS FOR DIFERENT GROUP OF USERS

NEW PROFILE

User Profiles

ID	ProfileName	Description	ActiveUsers
1 Edit	default	default Profile	2001
31 Edit	c2users1	Users from the group c2users1 in the Main D	997
32 Edit	c2users2	Users from c2users2 from Located in Child TC	993

IMPORTANT: The profiles are attached to groups. These groups have to be members of the main “Nested Group”, configured on the general LDAP. Otherwise the system won’t allow you to create the profile, displaying the message “Group not part of Ca22Unlock users.”

ALSO: If the Language has ben changed, the whole system needs to be restarted. .

Save Configuration

Group not part of Call2unlock users

...

If the group is correct, you will get the message “Generating Group...”, then “Changes Applied on Database”. And finally “No Errors Reported Generating Audios

Save Configuration

Changes Applied on Database

No Errors Reported Generating Audios

Accounts that will move tho the profile: 2001,
Total number of users in the System: 3991

Retrieve Accounts for the Profile. Verify running the report below

Find Accounts by name (blank to retrieve all the potential members of the Profile)

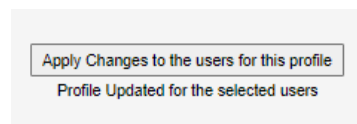
Get Report

User Accounts

ID	Username	Domain	Profile
6 Edit	aechevarria	td.cordiali.net	default
7 Edit	asaravia	td.cordiali.net	default
1993 Edit	root2002	td.cordiali.net	default
1994 Edit	root2003	td.cordiali.net	default

Is important to wait until you get the “No errors Reported Generating Audios”. During the process, the system is creating the custom IVR scripts, and creating a copy of all the default audios to the new profile filter. Later on, you can modify those audio files editing the profile (It was explaining on the Editing Profiles option)

In the same way than Editing profiles, especially because you’re creating a new profile and you want your users getting this profile now, you have to “Apply Changes to the users for this profile” at the very bottom of the page



Important: The users are synchronized daily. It will be explained on the section “Account Synchronization”. If during the day, users where disabled, created or moved to a different group, all those changes will be reflected on the system at the end of the day. Or at the time the automatic synchronization is configured

10. WHITE LIST

with that prefix, should validate that the telephone numbers where the calls come from are in a whitelist. In this way, only allowed telephones will be able to use the system from the PSTN.

In order to retrieve all numbers in the whitelist, you should go to the menu “SIP / WHITE LIST” write %, as a filter and press “Get Report”.

To insert a new number, click on the link “New Allowed Number”

. Find Whitelist Number (Write % to retrieve all) .. [Get Report](#) [New Allowed Number](#)

Whitelisted Numbers		
ID	Anynumber	Description
5 Edit	4558907893	Test Phone1
6 Edit	6549098843	Phone Test 2

The numbers can be updated or deleted also, clicking in “Edit” in every row.

11. ACCOUNT SYNCHRONIZATION

In this section, you will be able to retrieve all the new user accounts created on your Active directory, to call2Unlock.

The objective of this configuration is to create the necessary records for the self-service user portal, which is the place where the end users will configure their secondary email and personal PIN numbers, for the unlock process.

After the first retrieving of the accounts, every time you retrieve accounts, new accounts will be appended to the call2unlock local database. Also disabled or deleted AD accounts will be deleted from the call2unlock database. So the number of users valid for the license is always about current active accounts.

Go to the “LDAP / ACCOUNT SYNCHRONIZATION” Menu option.

Once on the User Accounts section, press the button “Retrieve New Accounts”. Next you should have the message about how many new accounts have been retrieved, how many accounts have been removed, and how many are in total.

CALL2UNLOCK Enterprise

SYSTEM LDAP SIP REPORTS

LDAP ACCOUNT SYNCHRONIZATION

CONFIGURATION
ACCOUNT SYNCHRONIZATION
END USERS

In this section the system will retrieve and synchronize the accounts from your LDAP server to the call2Unlock Database. Once in the local database, the administrator can edit the secondary email of the user (where the temporary password will be sent), and also the numerical PIN code.

New Accounts Retrieved: 502, Deleted or disbaled accounts are not any more in the system: 0, Total number of users in the System: 502

Retrieve New Accounts Now

Dayli Synchronization Configuration

Enable Retrieve and Synchronize accounts daily ☐

Time for Daily Synchronization "23:00:00" 11:00 PM

Save Synchro Info

So far you have executed the synchronization manually, but you will want the system executing this as a daily routine, because every day new accounts are created and disabled. In order to schedule the daily synchronization, check the box “Enable Retrieve and Synchronize accounts daily”, and select the time of the day to execute this, and click on the button “Save Synchro info”

Dayli Synchronization Configuration

Enable Retrieve and Synchronize accounts daily ☒

Time for Daily Synchronization "23:00:00" 11:00 PM

[Save Synchro Info](#)

System Updated Successfullyx

You can then try to find the accounts from the database, writing a search string with the name of the user and pressing the button "Get Report"

Find Accounts by name (blank to retrieve all) .. [Get Report](#)

12. END USERS EDITION

In this section you can find and edit the end user records, to provide or update some data regarding to them. Go to "LDAP / END USERS". Then writing a search string with the name of the user and pressing the button "Get Report"

CALL2UNLOCK Enterprise **SYSTEM** **LDAP** SIP REPORTS

END USER LIST AND EDITION

CONFIGURATION
ACCOUNT SYNCHRONIZATION
END USERS

List of all the users retrieved from the AD. Click on "Edit" on the row user which you want to update or modify.

Find Accounts by name (blank to retrieve all) .. [Get Report](#)

A grid with the results of the query will be displayed. You can order the list by any of the columns, configure the paging (by default 10), and export all the records to a csv file, that can be opened in and Excel later.

User Accounts				
ID	Username	Retrieve date	InternalPhone	
1 Edit	user151	2016-02-07 01:11:57		
2 Edit	user407	2016-02-07 01:11:57		
3 Edit	user152	2016-02-07 01:11:57		
4 Edit	user408	2016-02-07 01:11:57		
5 Edit	user153	2016-02-07 01:11:57		
6 Edit	user409	2016-02-07 01:11:57		
7 Edit	user154	2016-02-07 01:11:57		
8 Edit	user410	2016-02-07 01:11:57		
9 Edit	user155	2016-02-07 01:11:57		
10 Edit	user411	2016-02-07 01:11:57		

Export to CSV Page 1 of 51

Find Accounts by name (blank to retrieve all) Get Report

You can always edit the users account, pressing “Edit” with is the link on the first column in every user account row.

Once you click on the Edit link, you will be able to edit the user’s information;

USER ACCOUNT EDITION

User Account

mvela

Secondary Email

mvelad@contosito.com

4 digits PIN (Just numbers):

6076

InternalPhone Allowed:

3334

External Phone Allowed:

9283893839

Account in Blacklist?:

☐

Submit

After Submit the form, you will get the message “Changes Applied for the User”

The end users are also allowed to edit this information thru the self wen enroll site:

<http://ipaddress/userlogin.php>

The information provided for the users are:

- Secondary Email
- 4 Digits PIN (Apply just in case the PIN are configured to be stored in call2unlock database).. See LDAP configuration.
- Internal Phone Allowed: Internal Extension from where the user is able to use the system
- External Phone Allowed: External CallerID number, from where the user is able to use the system
- **Account in blacklist: This will be checked in case the user has failed the max number of attempts providing the PIN number. Unchecking this, the user will be released from the black list and will be ready to use again the system.**

Important: The system does not allow more than one user with the same External Phone allowed.

The External Phones should be also included in the white list

13. RADIUS – MFA CONFIGURATION.

This feature allows the system to make use of an external source of authentication like an external RADIUS server, or the local implementation of RADIUS and Google Authenticator.

Configuring this feature is a very good practice in terms of security, because the “challenge” information requested to the end user is not something fixed (like a PIN number created by the user or provided by the administrator), is in most cases a PIN number + a Token number that changes every given seconds. This token is associated with the user’s account.

Go to “RADIUS MFA / CONFIGURATION” menu option

Property	Value	Description
Radius Location	0. Local (localhost) ▼	Please Indicate if your radius server will local (on this Call2unlock server), or any other server on your existing infrastructure
Server Name or IP	localhost	If the server is Local or (localhost), once saving this changes, press the button 'Start-Restart Radius'
Radius Port	18120	Default port 18120. Update this value according to your Radius Server configuration
Raduis Client Secret	testing123	Place this secret in your radius configuration for this client (Call2unlock server IP), if you are using an external server

Save Changes

...

Then fill the following information:

Radius Location: We have to select if the RADIUS server is an existing RADIUS server (Option 1), or we are going to configure the local RADIUS (Option 0), integrated to Google Authenticator.

Server Name or IP: IP address of the RADIUS server, (localhost if is the local one).

Radius Port: Indicate the port the RADIUS server specified is listening.

Radius Client Secret: We have to provide the secret created for the IP address of the Call2unlock server, located on of the RADIUS client's configuration,

Once you complete providing this information, press the button "Save Changes"

The next step will be Starting the RADIUS service (In case of the local RADIUS). **It will start the service and be sure ntp is also running.** This is important because any token based system is time sensitive. You have to press "Start/Restart Local Radius" and "Test Connectivity". If everything is working fine, we have to get "OK – Running" and "OK – Connected" as Result messages.

Step 2. PLEASE SAVE THE CHANGES FROM THE STEP BEFORE. If you have chosen Local as Location of your Radius Server, start or restart the local Radius Server. If it runs successfully, you will be able to continue to step 3.

The screenshot shows two steps of a configuration process. Step 2 includes a button labeled 'Start/Restart Local Radius' and a red-bordered box containing the text 'Result: OK - Running'. Step 3 includes a button labeled 'Test Connectivity' and a red-bordered box containing the text 'Result: OK - Connected'.

The next step will be testing an account authentication using the RADIUS server. This test is valid for the local RADIUS with Google Auth. And the external RADIUS.

Providing the AD username, the PIN + Token you have to get the message "OK Authenticated"

Then, open an ssh session and execute the commands listen in the Step 4.

Step 4. Lets Test the Authentication using a Test Account and valid PIN + Token, provided by the MFA platform, such as google Authenticator
First Enroll a test user to Google Authenticator. Log into the console as root and execute the following commands

```
[root@myserver ~]# adduser test1 (You can use any username, avoid using a user name already existing in your AD)
[root@myserver ~]# passwd test1 (create a 4 digits pin number. example 5566)
[root@myserver ~]# cd /home/test1
[root@myserver ~]# su test1
[test1@myserver ~]$ google-authenticator
```

Follow the instructions and once the QR code is displayed, add a new account on your Google Auth app in your phone. Scan the QR code and you already have the test account ready.

Finally the SSH console will show you the QR code to add it to Google Authenticator APP. Providing the username created in the previous step, the PIN (password) + Google Authenticator Token, you have to get the message "OK Authenticated"

The screenshot shows a web-based authentication interface. It has two input fields: 'User Name for Test' and 'PIN+Token'. Below these is a button labeled 'Test Authentication'. To the right of the button, the result is displayed as 'Result: OK - Authenticated', which is enclosed in a red rectangular box.

14. END USER PORTAL – GOOGLE AUTHENTICATOR ENROLLMENT INTERFACE

This is the web site where your end users will configure their secondary email address, the 4-digit PIN number, and also enroll their Google Authenticator account, if the RADIUS-MFA has been selected as challenge information to provide. This information will be used by call2unlock at the time of the reset the password. This feature is just available for the Enterprise Edition of Call2Unlock.

You should deliver the URL to the users, so they can login to <https://ipaddress/userlogin.php>

This is an LDAP authentication against your AD server, so the users should be first retrieved to call2unlock, and the account should be unlocked, in order for the user to be able to log in.

You should provide on PIN code and one secondary email to the user. Once saved, back to the User Accounts List

User Account	<input type="text"/>
Secondary Email:	<input type="text"/>
4 digits PIN (Just numbers):	<input type="text"/>
External Phone Allowed:	<input type="text"/>

<https://chart.googleapis.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/jsmith@c5umfa.cordiale.net%3Fsecret%3DDDNMQN>



Generate-Regenerate Google Auth Account

If you Don't see the QR Code after pressing this button, please copy and paste the URL to your browser. If you can visualize the QR Code scan it usign your Google Auth App.

The information provided for the users are:

- Secondary Email
- Internal Phone Allowed: Internal Extension from where the user is able to use the system. In case “All Internal Calls are allowed” is checked in the SIP configuration, this input won’t be displayed.
- External Phone Allowed: Personal Phone number, from where the user is able to use the system. In case the External Prefix in the SIP configuration is empty, external calls are not allowed, this input won’t be displayed.
- 4 Digits PIN. In case we have local RADIUS enabled, this PIN number will be the password created in the local environment for RADIUS.

Once the user presses the Button “Generate-Regenerate Google Auth. Account”, the system will proceed to request a Google Auth. QR code. So the user just need to add the new account in the Google Auth. Mobile app, and scan the QR code to get the account and tokens working.

Important: The system does not allow more than one user with the same External Phone allowed.

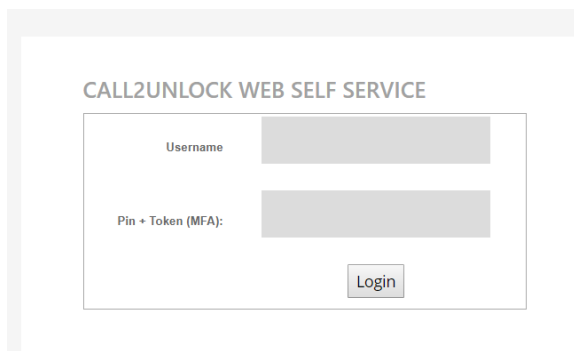
The External Phones should be also included in the white list (See the SIP Configuration Section) , o is necessary that the End User notify the administrator, about changes in the External Phone

15. END USER WEB SELF SERVICE

Since call2unlock now supports RADIUS and Google Auth. integration, it now provides a web self service tool for the end users, as an alternative to the IVR or telephone integration system. So the users have to go to this URL:

<https://ipaddress:4443>

Notice we use a different port here (4443) , in case your company needs this option available from the internet, so in your NAT Firewall rules you specify access only to this port and avoid exposing the whole configuration tool.

The screenshot shows a web browser window displaying the 'CALL2UNLOCK WEB SELF SERVICE' login page. The page has a light gray background. At the top, the title 'CALL2UNLOCK WEB SELF SERVICE' is displayed in a dark gray font. Below the title, there is a login form with two input fields: 'Username' and 'Pin + Token (MFA):'. Both fields are currently empty and have a light gray background. Below the 'Pin + Token (MFA):' field, there is a 'Login' button with a dark gray background and white text. The entire login form is enclosed in a thin gray border.

As you can see, this web requires the authentication against RADIUS (PIN + Token). Once successfully authenticated, the user will be able to unlock or reset the account using the following interface:

USER WEB SELF SERVICE - MFA

Unlock your account

Success	Unlock Account
---------	----------------

Set your new password

User Account	rcruz
New Password:	*****
Repeat Password:	*****
<div>Change</div>	
Your Password has been updated. Please log out from the systems and use this new one	

The user will have the 2 options, Unlock and Reset.

In case of Reset, the new password will be provided and updated in Active Directory.

Every single action performed by the end user in the web self-service tool, will be recorded in the logs and reports explained in the next chapter.

16. REPORTS

A Detailed Call Record is available, where you should be able to see how many accounts have been unlocked or reseated, which accounts and the exact time.

Go to “REPORTS/ SERVICE CDRS”. Once on the Reports section, pick up a start date and an end date, and press “Retrieve Records”

Detail of Calls

Start Date .. End Date Retrieve Records

ID	Uniqueid	CallerID	Calldate	User	Action	Result
16	1421026687.8	9999	2015-01-11 20:38:12	aduser	unlock	NO USER
17	1421026699.10	9999	2015-01-11 20:38:39	aduser	unlock	SUCCESS
18	1421026978.12	9999	2015-01-11 20:43:15	aduser	unlock	SUCCESS
19	1421027337.14	9999	2015-01-11 20:49:11	aduser	unlock	SUCCESS
20	1421027574.16	9999	2015-01-11 20:53:15	aduser	unlock	SUCCESS
21	1421028563.18	9999	2015-01-11 21:09:40	aduser	unlock	SUCCESS
22	1421028943.20	9999	2015-01-11 21:15:57	aduser	unlock	SUCCESS

Export to CSV Page 1 of 4 10 View 1 - 10 of 31

As you can see in the picture above, the grid shows the number of records, and also you can download the grid to a spreadsheet clicking on “Export to csv”. Also you can change the number of records that the grid can show on the selection combo next to the number of pages.

17. LICENSE

The licenses information should be loaded on this module. Go to “License” menu option, and fill the following information

License Key: The key number provided by Call2Unlock. This number is generated according to your domain name, and the number of users from your Active Directory. (The accounts underneath of the root OU that you have configured on your LDAP configuration).

Max Number of Users: You should select one interval from the combo, correspondent to the number of users of your active directory.

Domain Name: The name of your Domain. The license is valid just for your AD. Server.

License

Load or replace the license requested, filling the text with the key provided by Call2Unlock

[Click here to learn how to request and load a valid license.](#)

Property	Value	Description
License Key	<input type="text" value="2094007050"/>	License key provided by Call2Unlock
Max Number of Users	<input type="text" value="2501 - 10000"/>	Range of the Number of users in your Active Directory
Domain Name	<input type="text" value="mydomain.com"/>	Domain Name.

Changes Applied on Database **System Updated Successfully**

Once Applied the License, restart the call2unlock server from the operative system running **“sudo shutdown –r now”**

18. TESTING THE SERVICE

In order to test and start using Call2unlock, we will perform 2 basic tests.

Test 1.

We will validate if Call2Ulock is working correctly regardless the sip trunk to your PBX

1. Download a free Softphone (like Xlite, you can download if from <http://www.counterpath.com/x-lite-download/>)
2. Configure the following extension in the softphone.

No matter what softphone you are using, the most important parameters are:

Extension: 9999 CallerID 0016960

Password: 123456

Domain : Call2Unlock IP address

The example below, is a configuration for xlite

Account	Voicemail	Topology	Presence	Storage	Security	Advanced
---------	-----------	----------	----------	---------	----------	----------

User Details

Display Name

9999

User name

9999

Password

••••••

Authorization user name

9999

Domain

Call2Unlock IP Address

Domain Proxy

☒ Register with domain and receive incoming calls

Send outbound via:

☐ domain
☐ proxy Address
☒ target domain

3. Dial 8888 and follow the instructions to unlock and/or reset any account on your active directory.
4. Is a good idea to open an asterisk console to see the logs in real time.
"asterisk -rvvv"

*Call2Unlock*CLI>*

Test 2.

We will validate if your PBX is sending correctly the calls to Call2Unlock. So we will validate if the Call2Unlock IVR is available from your phone extensions.

1. Dial the extensions configured in your PBX that send the call to Call2Unlock, from any extension in your PBX and follow the instructions to unlock and/or reset any account on your active directory
 - Again, Is a good idea to open an asterisk console to see the logs in real time.
"asterisk -rvvv"

*Call2Unlock*CLI>*

2. Enjoy your new Service 😊