

**CALL2UNLOCK**

# Manual de Administración

V 4.0

## Contenido

DESCRIPCIÓN GENERAL DEL SISTEMA .....	3
Introducción.....	3
INSTALACIÓN Y CONFIGURACIÓN.....	7
1. Actualización de las credenciales web.....	14
2. Actualización de las credenciales de la base de datos.....	15
3. ASISTENTE DE CONFIGURACIÓN DE LDAP: .....	15
Probar el desbloqueo y restablecimiento de cuentas. ....	22
4. Configuración LDAP.....	27
Probar el desbloqueo y restablecimiento de cuentas. ....	33
5. CUENTAS DE ADMINISTRACION VIA LDAP .....	35
6. ASISTENTE DE CONFIGURACIÓN SIP: .....	36
7. CONFIGURACIÓN DE SU PBX CORPORATIVA .....	41
8. CONFIGURACIÓN SIP.....	41
9. PERFILES DE USUARIO.....	44
10. LISTA BLANCA.....	48
11. SINCRONIZACIÓN DE CUENTAS.....	49
12. EDICIÓN PARA USUARIOS FINALES .....	50
13. RADIUS – CONFIGURACIÓN MFA.....	52
14. PORTAL DE USUARIO FINAL: INTERFAZ DE INSCRIPCIÓN DE GOOGLE AUTHENTICATOR .....	54
15. AUTOSERVICIO WEB PARA USUARIOS FINALES.....	56
16. REPORTES.....	57
17. LICENCIAS .....	58
18. PROBANDO EL SERVICIO .....	59

## DESCRIPCIÓN GENERAL DEL SISTEMA

### Introducción

Call2Unlock es la primera solución de autoservicio LDAP que funciona a través de una simple llamada telefónica.

Un gran porcentaje de las llamadas que recibe una mesa de servicio o departamentos de soporte de TI están relacionadas con desbloquear o restablecer cuentas de usuario. Un sistema LDAP de autoservicio, hace posible esta tarea, sin la intervención de un humano.

Por lo general, los productos que resuelven este problema, tienen algunas desventajas, como la necesidad de instalar software en las PCs o muchas veces, exponer y comprometer la seguridad utilizando herramientas web o aplicaciones móviles accesibles desde internet.

Los usuarios de Call2Unlock solo necesitan marcar una extensión interna en el PBX de la compañía, o un DID público, y siguiendo algunas instrucciones, la cuenta de usuario se desbloqueará de forma segura. La información de "desafío" (ID de empleado, números PIN, tokens) podrían almacenarse en Active Directory, la base de datos Call2unlock, o en cualquier tipo de sistema de autenticación de dos factores hacia un servidor RADIUS. Call2unlock también proporciona su propia infraestructura RADIUS – Google Authenticator para este propósito.

Para implementar Call2Unlock para su organización, solo necesita:

- Microsoft Active Directory 2008 o superior (2008,2012,2016,2019,2022).
- Cualquier sistema PBX compatible con el protocolo SIP. (Si no cuenta con una PBX se podría proporcionar Call2Unlock Cloud Secure Phone Gateway en el Cloud).

### ¿Cómo funciona desde la perspectiva del usuario final?

**Situación 1:** *"Mi nombre es Juan Pérez, y trabajo para el departamento financiero, y mi cuenta generalmente se bloquea, porque fallo varias veces al escribir mi contraseña, y necesito ser desbloqueado a.s.a.p. Normalmente me alojo en mi oficina, dentro de la red de la empresa"*

Juan debe seguir los siguientes pasos.

1. Marque la extensión interna de Call2Unlock proporcionada por el administrador. Un IVR amigable le pedirá un número de identificación personal. (como un código de empleado o un número de ID)
2. El sistema le preguntará a Juan; qué acción necesita realizar (Desbloquear o Restablecer su contraseña)
3. Una vez que Juan, presione la opción 1 (desbloquear cuenta), el sistema encontrará la cuenta de Juan y reproducirá el mensaje "La cuenta que está intentando desbloquear es Juan Pérez, si esta es la cuenta que está intentando desbloquear, presione 1, de lo contrario presione 0 o cuelgue la llamada". Luego le pedirá a Juan un número PIN para confirmar la acción.
4. Una vez que el sistema recibe la opción (1) y el número PIN, el sistema dirá "Su cuenta se ha desbloqueado con éxito", e inmediatamente, el usuario podrá iniciar sesión en la red. **Este número PIN podría ser algo fijo almacenado en AD o la base de datos Call2Unlock, o un PIN + número de token (basado en el tiempo) proporcionado al usuario por la aplicación Google Authenticator.**

**Situación 2: "Ahora Juan, ha olvidado su contraseña, ha caducado, o sospecha que alguien más puede conocerla, por lo que necesita una nueva contraseña".**

Juan debe seguir los siguientes pasos.

1. Marque la extensión interna Call2Unlock proporcionada por el administrador, un IVR amigable le pedirá un número de identificación personal. (como un número de empleado)
2. El sistema le preguntará a Juan, qué acción necesita realizar (Desbloquear o Restablecer su contraseña)
3. Si Juan, elige ahora la opción 2 (restablecer contraseña), el sistema encontrará la cuenta de Juan y dirá "La cuenta que está intentando restablecer es Juan Pérez. Si esta es la cuenta que está intentando desbloquear, presione 1, de lo contrario, presione 0 o cuelgue la llamada".
4. Una vez que el sistema obtiene la tecla de opción (1), el sistema le pedirá a Juan un número de PIN, o de validación. Una vez proporcionado, el sistema le dirá a Juan "Su contraseña temporal ha sido enviada a su dirección de correo electrónico secundario".
5. Juan recibe su contraseña temporal en su correo electrónico secundario. Ahora puede iniciar sesión en la red con la contraseña temporal. Inmediatamente, el sistema de autenticación de Windows le pedirá a Juan que cree una nueva contraseña.

**\*\* El número PIN podría ser algo fijo almacenado en AD o la base de datos Call2Unlock, o un PIN + número de token (basado en el tiempo) proporcionado al usuario por la aplicación Google Authenticator.**

Call2Unlock puede enviar las contraseñas temporales de 4 formas diferentes el usuario final:

- Por Audio (Text To speech).

- Enviado a un correo electrónico secundario (como en el ejemplo anterior).

- Enviando un SMS al celular del empleado.

- Enviando una combinación utilizando dos formas de entrega. Por ejemplo, los primeros 3 caracteres por Audio y los segundos 5 caracteres en un SMS.

**\*\* La información personal como correo electrónico secundario, número de teléfono celular personal y/o cuenta de Google Authenticator, es información que el usuario final proporciona una vez es inscrito en el sistema.**

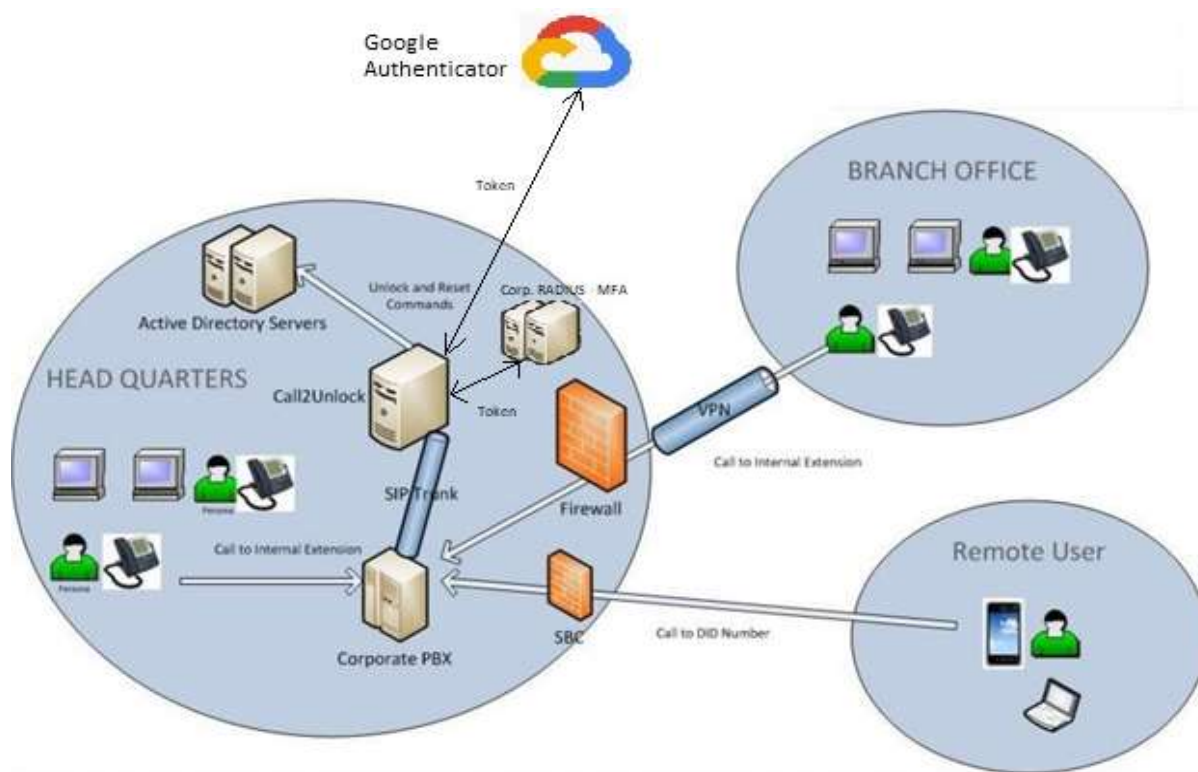
**Situación 3: "Juan está bloqueado y está trabajando desde casa, tratando de conectarse a la VPN de la empresa, y el mecanismo de autenticación válida que la cuenta no esté bloqueada, deshabilitada ni caduca, para acceder a la VPN, o peor aún, usa AD como medio de autenticación".**

-Juan podrá desbloquear o restablecer su cuenta usando las mismas opciones de los ejemplos anteriores. La única diferencia es que ahora va a marcar un número DID público configurado en el PBX de la compañía. Además, su número de teléfono personal ha sido incluido en una "lista blanca" solo para que teléfonos personales permitidos usen Call2Unlock desde la PSTN.

## ¿Cómo funciona desde la perspectiva del administrador de TI?

Para entender cómo funciona Call2Unlock, echemos un vistazo a su arquitectura

## Arquitectura



Call2Unlock tiene básicamente 5 componentes

1. **Motor IVR.** Este componente interactúa con la centralita corporativa de la empresa, enviando mensajes de audio al usuario y obteniendo las entradas DTMF del usuario
2. **Motor de comandos LDAP.** Este interactúa enviando los comandos apropiados a los servidores de Active Directory para realizar el desbloqueo o restablecimiento de las cuentas en una comunicación segura y cifrada.
3. **Herramienta de administración web:** Sitio web para administradores, para configurar el sistema, obtener informes y páginas de autoservicio para usuarios finales, donde pueden proporcionar información adicional como números PIN, teléfonos móviles personales y correos electrónico secundario.

**4. RADIUS - Google Auth. Platform:** Call2unlock proporciona su propia implementación de RADIUS - Google Authenticator, para ser utilizada como mecanismo de autenticación por los usuarios finales. Esta característica se configura al 100% desde la Herramienta de administración web. Por lo tanto, Call2unlock se puede utilizar no solo como una herramienta de autoservicio para cuentas de AD, sino también como una plataforma de autenticación de dos factores. También Call2Unlock se puede integrar con cualquier sistema de autenticación de dos factores compatible a RADIUS.

**5. Herramienta de autoservicio para usuarios web:** Dado que los usuarios pueden inscribir automáticamente sus cuentas en Google Authenticator App utilizando nuestros paneles de inscripción de usuarios web, también pueden desbloquear o restablecer sus cuentas utilizando su Google Authenticator app o el token proporcionado por su MFA de forma segura utilizando nuestra interfaz de autoservicio web.

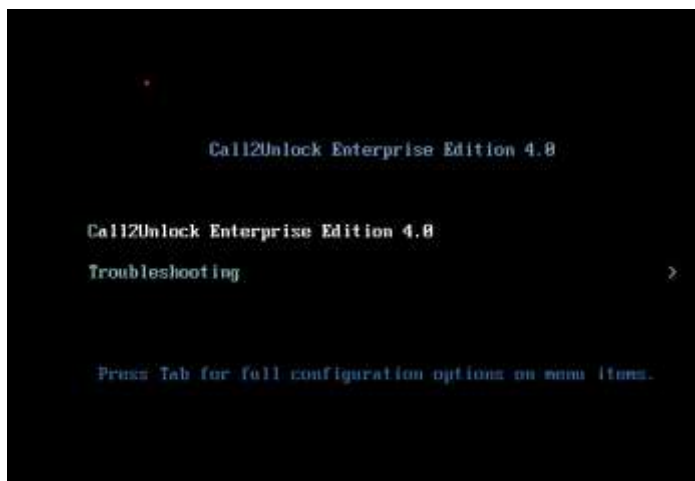
## INSTALACIÓN Y CONFIGURACIÓN

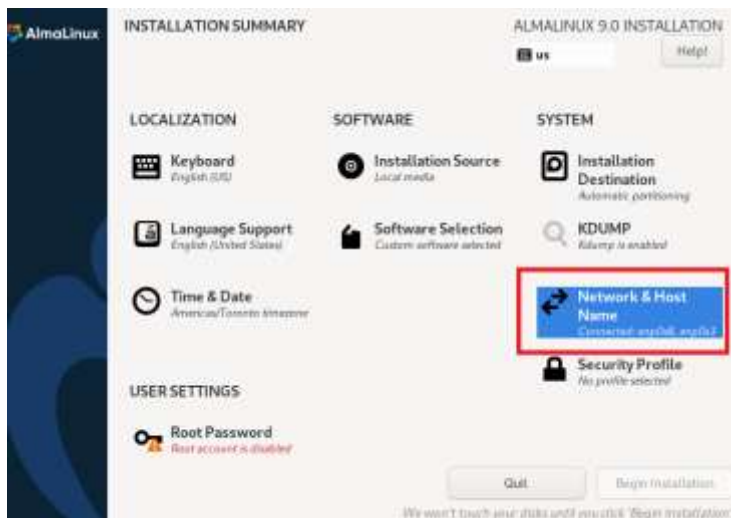
### Obtención del sistema

Llene el formulario en línea en <https://call2unlock.com>

Recibirá un email de Call2unlock con el enlace de la imagen ISO. Call2Unlock corre sobre el sistema operativo Linux, por lo que el instalador ISO llamado Call2UnlockEnt04.iso, es básicamente un AlmaLinux 9.0 Minimal ISO personalizado con todos los paquetes necesarios, los scripts y herramientas para la aplicación.

El proceso para instalar el ISO, es básicamente el mismo de la instalación de Linux. Esta ISO se puede instalar en cualquier servidor físico o virtual.





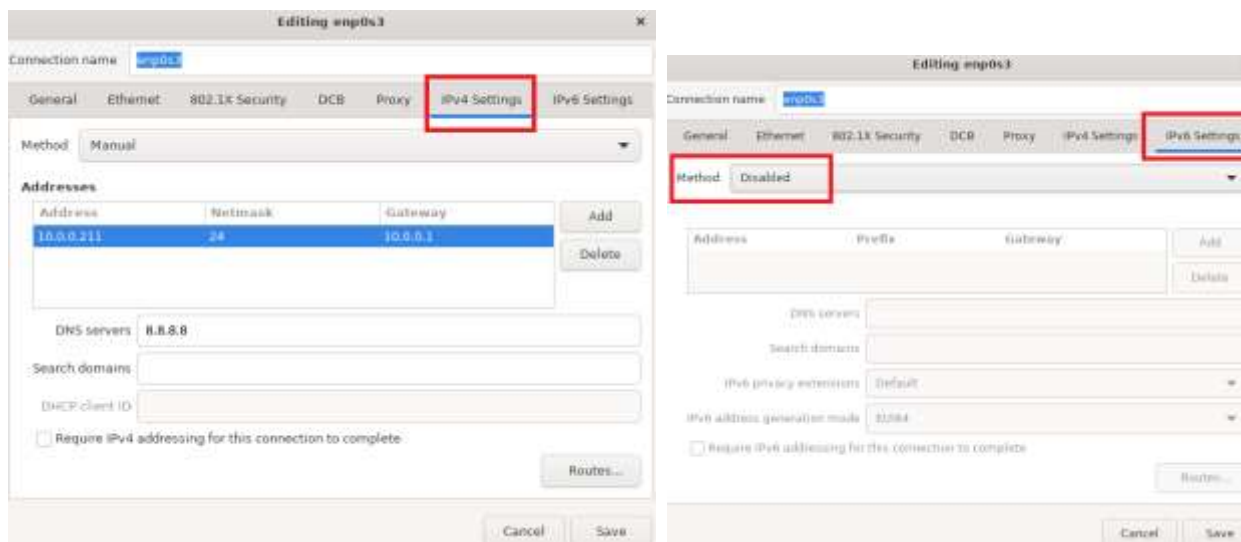
### IMPORTANTE:

Para obtener una instalación exitosa, es necesario proporcionar las direcciones IP, hostname, Default Gateway, etc, para las interfaces de red, durante la instalación.

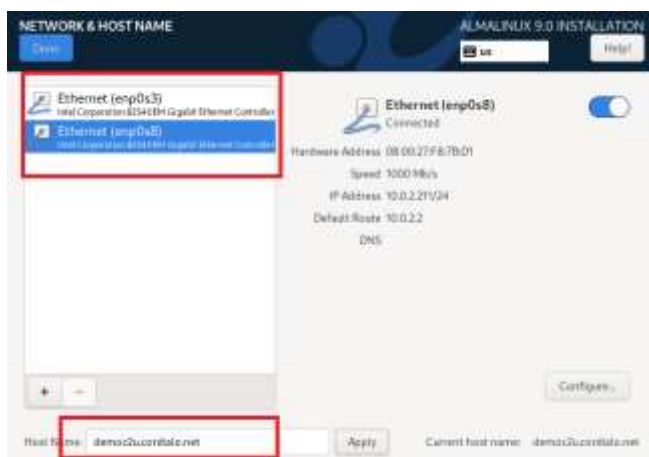
Se requiere asignar una dirección IPv4 estática a su NIC, como en el ejemplo

También es importante asignar un DNS accesible (preferiblemente interno), especialmente para que los servicios internos funcionen y también para resolver su infraestructura AD. Además, se recomienda deshabilitar IPv6.



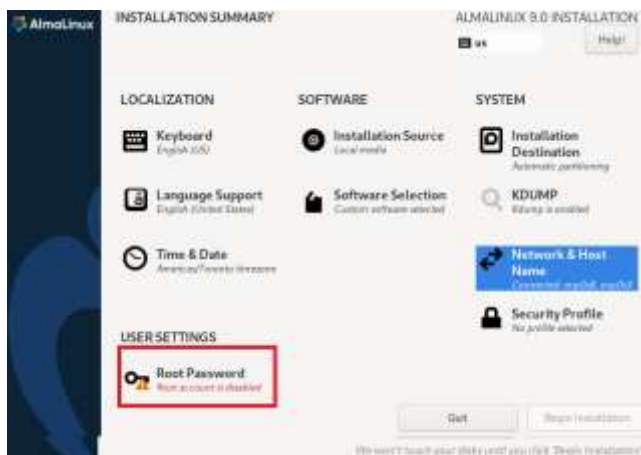


Repita los mismos pasos si va a configurar una interfaz NIC adicional. Dependiendo de la arquitectura de su red, podría ser recomendable dedicar una NIC para comunicarse con su infraestructura de AD y la otra NIC para la administración o el tráfico de VoIP.

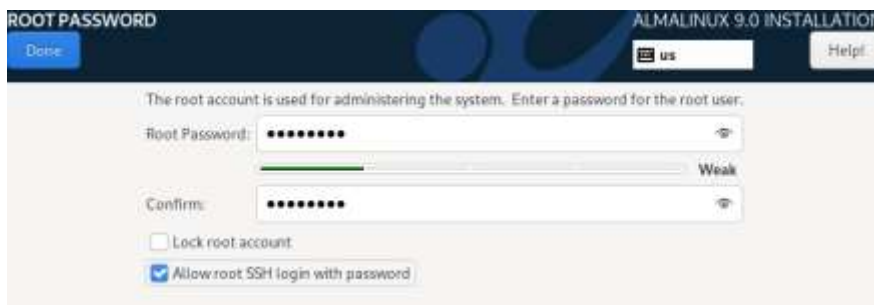


Luego debe asignar un nombre a su nuevo servidor Call2unlock.

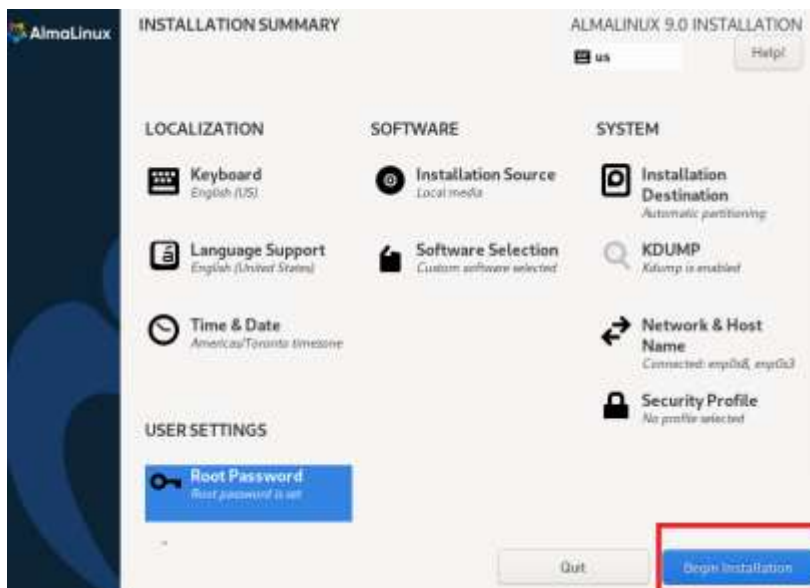
Finalmente, debe asignar una contraseña de root para el sistema.



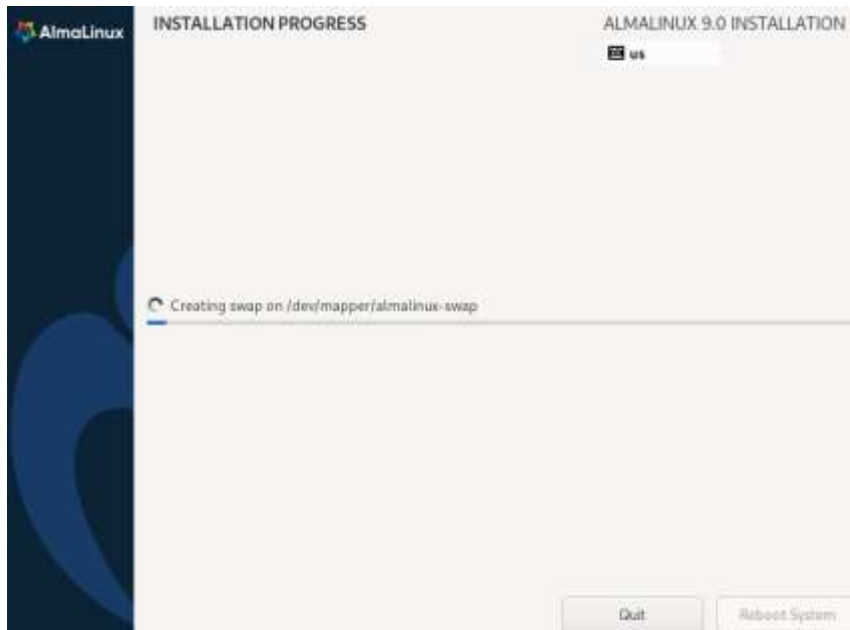
Es muy importante que marque la casilla “Allow root SSH login with password” para poder acceder al servidor via ssh. Más adelante, puede asignar llaves o certificados para la autenticación SSH. También desmarque “Lock root account” como en la imagen a continuación:



Una vez que haya completado los pasos anteriores, estará listo para comenzar la instalación. Haga clic en “Begin Installation”



Al igual que una instalación regular de Linux, solo tiene que esperar hasta que finalice la instalación.



### Validación de la instalación.

- Inicie una sesión ssh en su instancia de Call2Unlock. Debería obtener el banner de call2unlock similar a la imagen de abajo.
- Verifique que la PBX asterisk, esté en funcionamiento ejecutando "asterisk -rvvvv". Debería obtener una salida como esta:

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

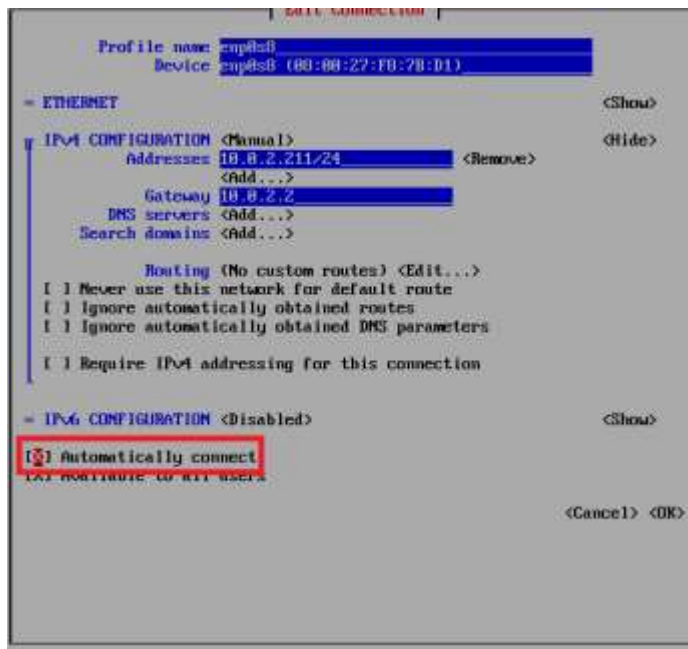
Activate the web console with: systemctl enable --now cockpit.socket

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

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

[root@c2u24manual ~]#
```

**IMPORTANTE:** Si tiene más de una NIC, asegúrese de que todas estén habilitadas al booteo. Incluso si durante la instalación configuró esto, esto solo se aplica a la primera NIC. Para NIC #2 o #3, confirme que tiene esto habilitado o configúrelo ejecutando **nmtui** desde la línea de comandos de Linux. Asegúrese de que la opción “Automatically connect” esté marcada.



- Verifique el panel de configuración web e inicie sesión en ese panel. Abra un navegador web y vaya a [https://\[dirección ip\]](https://[dirección ip]). Use las credenciales predeterminadas para iniciar sesión (root / call2unlock). Debe cambiar esa contraseña más adelante.



¡Hecho!

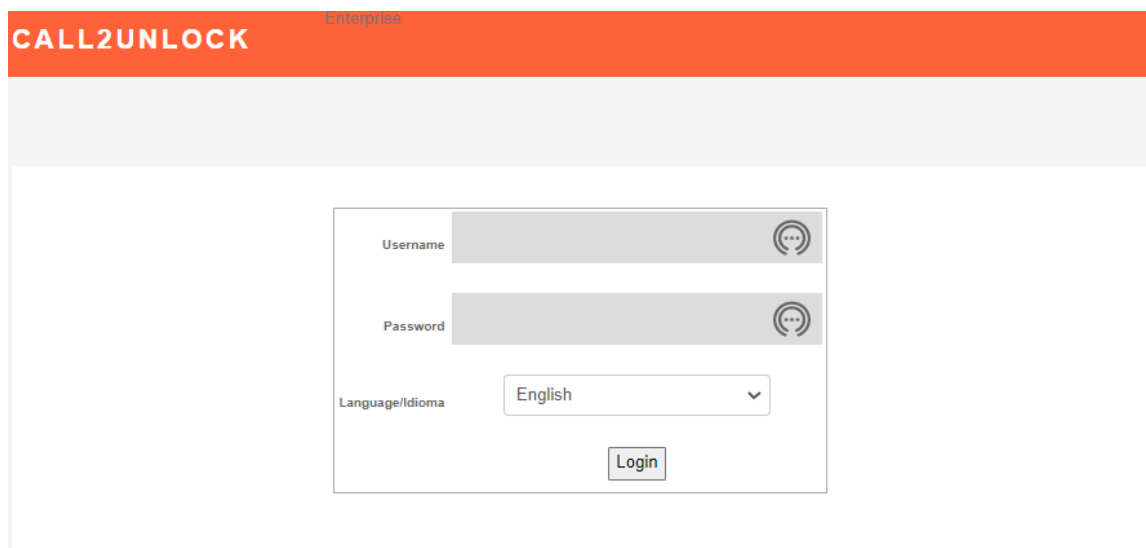
Una vez que haya verificado que asterisk se está ejecutando y que el panel web es accesible y puede iniciar sesión en el panel, estamos listos para configurar el sistema y para integrarlo con su sistema telefónico y su infraestructura de AD.

## Valores predeterminados

Una vez que tenga Call2Unlock en funcionamiento, se recomienda que cambie inmediatamente las credenciales predeterminadas proporcionadas.

## Configuración del sistema

Inicie sesión en la interfaz web de call2unlock <https://ipaddress>



The screenshot shows the web interface for CALL2UNLOCK Enterprise. At the top, there is an orange header with the text "CALL2UNLOCK" and "Enterprise" in smaller text 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 three input fields: "Username" and "Password", both with gray backgrounds and a circular icon with three dots to their right. Below these is a "Language/Idioma" dropdown menu with "English" selected. At the bottom of the form is a "Login" button.

Utilice las credenciales predeterminadas para iniciar sesión en el sistema u= root, p=call2unlock. Seleccione su idioma (En esta versión sólo disponible en inglés/español)

Una vez autenticado, el sistema lo llevará al sitio HOME. Un mensaje recomendando cambiar la contraseña de usuario predeterminada de la Interfaz Web aparecerá en rojo.



Nota: Estas credenciales se utilizan para iniciar sesión en la aplicación, por lo que la contraseña debe cambiarse lo más pronto posible. No confunda las credenciales de la aplicación con las credenciales de la base de datos. Las credenciales de la base de datos las cambiaremos en la opción “Administración de Base de Datos”, detallada más adelante.

## 1. Actualización de las credenciales web

Vaya a la opción de menú "SISTEMA / ADMINISTRADOR". La página de Administración cargará. Una vez que escriba una nueva contraseña y la envíe, aparecerá el mensaje "Cambios aplicados". El usuario debe volver a iniciar sesión en el sistema.



## 2. Actualización de las credenciales de la base de datos

De la misma manera que las Credenciales Web, debemos actualizar las credenciales de nuestra base de datos, con una contraseña segura. Vaya a "SYSTEMA/ADMINISTRACIÓN DE BASE DE DATOS", proporcione la contraseña de base de datos actual predeterminada y actualice la contraseña. Deberá reiniciar sesión en el sistema después de aplicar los cambios



## 3. ASISTENTE DE CONFIGURACIÓN DE LDAP:

Esta es la sección más importante. Aquí podrá configurar y probar los parámetros y credenciales necesarios para conectarse a su servidor de Active Directory, y también probar acciones como Desbloquear y restablecer contraseña. Este asistente consta de una serie de 05 pasos que lo guiarán a través del proceso y detectarán cualquier problema y las recomendaciones para su corrección. Previamente, es necesario crear una cuenta de servicio dedicada a call2unlock con suficientes privilegios para desbloquear y restablecer contraseñas.

**Paso 01:** Prueba de conectividad. El sistema verifica que se pueda acceder a los puertos involucrados desde call2unlock a su infraestructura de AD

**Paso 02:** Autenticación LDAP. El sistema verifica que su cuenta de servicio se puede autenticar a su Active Directory desde Call2Unlock

**Paso 03:** Prueba de desbloqueo y reseteo: El sistema validará que su cuenta de servicio tenga suficientes privilegios para desbloquear y resetear cuentas utilizando cuentas de usuario de prueba.

**Paso 04:** Recuperar objetos. Call2Unlock recuperará hacia su base de datos interna, las cuentas de usuario (Solo nombres de cuenta). Esos usuarios se filtran por los nombres de grupo y las unidades organizativas proporcionadas (OU) en ese asistente.

**Paso 05:** Proporcione el resto de parámetros de configuración, como: Lugar de validación de usuario (Active Directory, Call2unlockDB, 2FA), Entrega de contraseñas (audio, SMS, correo electrónico), Complejidad de contraseña, etc.

Una vez completados los 05 pasos, call2unlock generará el script IVR, que se presentará al usuario cada vez que marque la extensión interna asignada a Call2Unlock o el número de teléfono DID público. Vaya a la opción de menú "LDAP / ASISTENTE DE CONFIGURACIÓN". Debería obtener la página Step1

### Paso 01:

PASO 1. Verifiquemos que tenga conectividad con su infraestructura de Active Directory. Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración

Propiedad	Valor	Descripción
Dirección IP	10.0.2.231	Dirección IP del controlador de dominio principal
Nombre de Host	myadserver	Nombre de host del controlador de dominio principal
Tipo de conexión LDAP	1. Global Catalog	0. Servidor de directorio activo. Utilice esta opción si va a utilizar un Dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory. 1. Catálogo Global. Utilice esta opción si tiene un bosque con varios dominios. El puerto del catálogo global, en el servidor AD del dominio raíz, se utilizará para buscar objetos y el puerto LDAP para desbloquear y restablecer cuentas. Asegúrese de incluir la lista de sus servidores en el campo Lista de servidores AD.
Puerto LDAP	636	Puerto LDAP para conectarse a LDAP (389 por defecto, 636 recomendado)
Puerto de catálogo global	3269	Puerto de catálogo global (3268 por defecto, 3269 recomendado)
Lista de servidores AD	10.0.2.231 cordialo.net; 10.0.2.131 evt.cordialo.net; 10.0.2.31 lv.cordialo.net	Escriba su lista de servidores AD si está utilizando un catálogo global y un entorno multidominio. Escriba la dirección IP, el nombre del servidor y un punto y coma para cada controlador de dominio. Este contenido se agregará al archivo /etc/hosts Ejemplo: 10.0.2.230 domain.net; 10.0.3.230 child1.domain.net; 10.0.4.230 child2.domain.net  Por favor, elimine los espacios en blanco, especialmente al comienzo de cada fila.

Prueba de conexión Ldap: Success

Prueba de conexión del catálogo global: Success

Otros servidores AD:  
10.0.2.231 :Success  
10.0.2.131 :Success  
10.0.2.31 :Success

Estado de actualización: Changes Applied on Database

Se deben proporcionar los siguientes parámetros. (Todas las etiquetas de propiedad en rojo)

**Dirección IP:** Dirección IP del servidor principal de Active Directory. Si desea trabajar con un bosque de dominio completo, esta dirección IP es el servidor de AD de dominio raíz con acceso al Global Catalog.

**Nombre de host:** Nombre del servidor de Active Directory. (Este valor es solo informativo, no se considerará como un parámetro para la conexión LDAP).



**Tipo de conexión LDAP:** Esta selección nos permite trabajar con un bosque completo de Active Directory, incluidos dominios secundarios, o directamente con un único servidor AD de dominio.

*0. Active Directory Server.* Utilice esta opción si va a utilizar un dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory.

*1. Global Catalog.* Utilice esta opción si tiene un bosque con varios dominios. El puerto de Global Catalog en el servidor de AD del dominio raíz, se usará para buscar objetos y los puertos LDAP para desbloquear y restablecer cuentas en todos los Controladores de Dominio.

**Puerto LDAP:** puerto LDAP para Active Directory. Por defecto, 389. Call2unlock utiliza LDAPS (LDAP Seguro), por lo que se recomendará 636.

**Puerto de catálogo global:** Puerto utilizado para el catálogo global (en caso de que se seleccione 1. Global Catalog como Tipo de conexión LDAP). Normalmente, el puerto 3269 para conexiones seguras

**Lista de servidores de AD:** Esta es la lista de la lista de servidores de AD. Si usa el catálogo global y un entorno multidominio, escriba la dirección IP, el nombre del servidor y un punto y coma para cada controlador de dominio. Este contenido se agregará al archivo /etc/hosts Ejemplo de contenido de este campo:

**10.0.2.230 domain.net;**

**10.0.3.230 child1.domain.net;**

**10.0.4.230 child2.domain.net**

El sistema colocará al final del archivo /etc/hosts algo como:

**10.0.2.230 domain.net**

**10.0.3.230 child1.domain.net**

**10.0.4.230 child2.domain.net**

Una vez que haya completado la información, haga clic en el botón "Probar". El sistema probará los puertos y el destino para asegurarse de que call2unlock pueda comunicarse con su infraestructura de AD desde la perspectiva de red. Solo si no hay ninguna prueba "failed", el sistema le permitirá guardar y avanzar al Paso 2

Probar	Prueba de conexión Ldap:	Success
	Prueba de conexión del catálogo global:	Success
	Otros servidores AD:	10.0.2.231 :Success 10.0.2.131 :Success 10.0.2.31 :Success
Guardar	Estado de actualización:	Changes Applied on Database
SIGUIENTE PASO		

Paso 02:

Step1

Step2

Step3

Step4

Step5

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 setting

Propiedad	Valor	Descripción
Dirección IP	10.0.2.231	Dirección IP del controlador de dominio principal
Nombre de Host	myadserver	Nombre de host del controlador de dominio principal
Tipo de conexión LDAP	1.Global Catalog	0. Servidor de directorio activo. Utilice esta opción si va a utilizar un Dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory. 1. Catálogo Global. Utilice esta opción si tiene un bosque con varios dominios. El puerto del catálogo global, en el servidor AD del dominio raíz, se utilizará para buscar objetos y el puerto LDAP para desbloquear y restablecer cuentas. Asegúrese de incluir la lista de sus servidores en el campo Lista de servidores AD.
Puerto LDAP	636	Puerto LDAP para conectarse a LDAP (389 por defecto, 636 recomendado)
Puerto de catálogo global	3269	Puerto de catálogo global (3268 por defecto, 3269 recomendado)
Nombre de cuenta de administrador	scv_c2admin	Cuenta con privilegios de administrador
Contraseña de administrador	*****	Contraseña de la Cuenta de administrator
Adm DC string	cn=Users,dc=evl,dc=condialo,dc=net	DC String para la cuenta con administrador priv. Ejemplo cn=Adminuser,dc=domain,dc=com
Subir certificado	Cargue su Certificado AD Choose File No file chosen Submit	Certificado generado, utilizando los servicios de certificados de Active Directory. Una vez que cargue su certificado, espere hasta que reciba el mensaje Cargado correctamente. Para saber cómo generar un certificado de CA en su servidor de Active Directory, (Descargar desde aquí)

Guardar y Probar

Success . Changes Applied on Database

Success

SIGUIENTE PASO

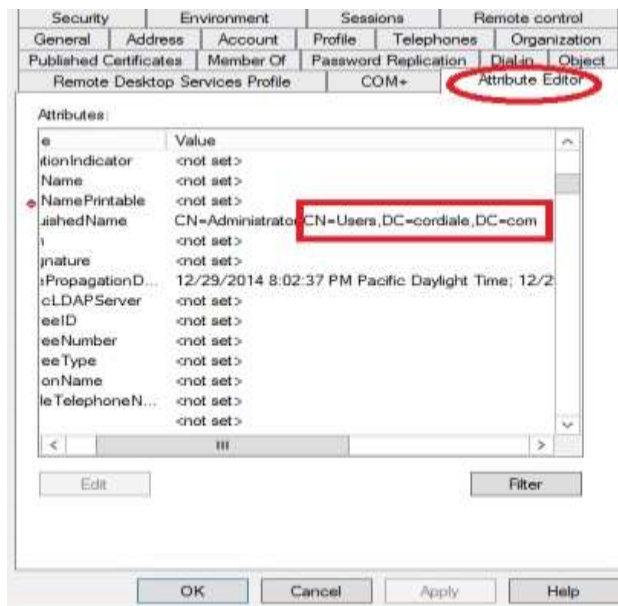
Se deben proporcionar los siguientes parámetros. (Todas las etiquetas de propiedad en rojo). Los controles deshabilitados corresponden a la configuración ya proporcionada en el paso anterior.

**Nombre de cuenta de Administrador:** Esta cuenta debe tener privilegios suficientes para desbloquear o restablecer cuentas en su directorio activo. Típicamente una cuenta de servicio

**Adm Password:** contraseña en AD para la cuenta de administrador

**Adm DC string:** Este es el nombre distintivo de la unidad organizativa a la que pertenece la cuenta LDAP de administrador. Para obtener esta información, vaya a su servidor de AD, en "Usuarios de Active Directory y equipos", vaya a "Editor de atributos" y copie el "DistinguishedName", pero solo de la unidad organizativa, sin tomar el nombre de la cuenta.

En la imagen de abajo, de la cadena "cn=Administrator,cn=Users,dc=cordiale,dc=com" solo se ha considerado "**cn=Users,dc=cordiale,dc=com**"

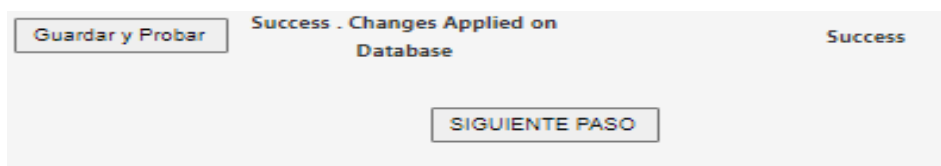


**Cargar certificado:** debe cargar el certificado de cliente pem generado previamente en su AD. Este certificado es necesario para realizar acciones como restablecer contraseñas desde call2unlock o simplemente para vincular a su directorio activo.

<p>Subir certificado</p>	<p>Cargue su Certificado AD</p> <div> <input type="button" value="Choose File"/> <span>No file chosen</span> </div> <div> <input type="button" value="Submit"/> </div>	<p>Certificado generado, utilizando los servicios de certificados de Active Directory. Una vez que cargue su certificado, espere hasta que reciba el mensaje Cargado correctamente. Para saber cómo generar un certificado de CA en su servidor de Active Directory, (Descargar desde aquí)</p>
--------------------------	--	---

Para generar estecertificado siguiendo el manual, "Generación del certificado AD", que está disponible en el sitio web de Call2Unlock <https://www.call2unlock.com>

Una vez que haya completado la información, haga clic en el botón "Guardar y probar". El sistema probará el enlace a su directorio activo, para validar que su cuenta de servicio pueda autenticarse en su Active Directory desde Call2Unlock, y también validar que la información proporcionada es precisa y el certificado es válido. Obtener el mensaje de éxito en la prueba "Success", le permitirá pasar al Paso 3



Paso 03:



PASO 3. Verifiquemos que puede desbloquear y resetear cuentas desde su AD, y si su cuenta de servicio tiene los privilegios. Si está conectando un árbol de dominio mediante el catálogo global, asegúrese de que el atributo de usuario sea parte del PAS y esté habilitado para ser replicado. Todos los controles deshabilitados corresponden a configuraciones ya proporcionadas en los pasos anteriores (1-2), se presentan solo como referencia. Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración

Propiedad	Valor	Descripción
Dirección IP	10.0.2.231	Dirección IP del controlador de dominio principal
Nombre de Host	myadserver	Nombre de host del controlador de dominio principal
Tipo de conexión LDAP	1.Global Catalog	0. Servidor de directorio activo. Utilice esta opción si va a utilizar un Dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory.  1. Catálogo Global. Utilice esta opción si tiene un bosque con varios dominios. El puerto del catálogo global, en el servidor AD del dominio raíz, se utilizará para buscar objetos y el puerto LDAP para desbloquear y restablecer cuentas. Asegúrese de incluir la lista de sus servidores en el campo Lista de servidores AD.
Puerto LDAP	636	Puerto LDAP para conectarse a LDAP (389 por defecto, 636 recomendado)
Puerto de catálogo global	3269	Puerto de catálogo global (3268 por defecto, 3269 recomendado)
Nombre de cuenta de administrador	scv_c2admin	Cuenta con privilegios de administrador
DC String de Usuarios Finales	dc=cordialo,dc=net	Rama en el directorio LDAP, desde donde el sistema intentará encontrar a los usuarios. Ejemplo ou=Person,ou=Corporate,dc=domain,dc=com
Atributo de usuario	employeeNumber	Propiedad de usuario, que será utilizada por el usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: employeeNumber
Longitud del atributo	5	Longitud estándar del atributo User. Esta debe tener la misma longitud para todos los usuarios. Ej:(En el atributo es 01903399, la Longitud =8)

Guardar Configuración

System Updated Successfully

Se deben proporcionar los siguientes parámetros. (Todas las etiquetas de propiedad en rojo). Los controles deshabilitados corresponden a la configuración ya proporcionada en el paso anterior.

**DC String de usuarios:** “DistinguishedName” de la unidad organizativa donde se encuentran los usuarios. Los usuarios dentro de otras unidades organizativas dentro de la unidad organizativa raíz también serán considerados.

Ejemplo: Si en el sistema tenemos como User OU String:

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

Esto significa que también se incluirán los usuarios de la siguiente unidad organizativa.

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

**Atributo de usuario:** Las cuentas en su AD deben tener un parámetro numérico estándar, que se utilizará para identificar las cuentas. En el ejemplo se utilizará `employeeNumber`.

Importante:

- El parámetro seleccionado debe ser numérico.
- Debe tener una longitud estándar para todos los usuarios

Si no tiene en su AD, un parámetro numérico que identifique a los usuarios, primero considere incluir este atributo, y asignarlo cada vez que se creen nuevas cuentas. Ejecute un script para completar esta información para todos sus usuarios actuales que aún no cuenten con este atributo.

Hay varios ejemplos en la web, sobre scripts para actualizar los parámetros de las cuentas de usuario. Un ejemplo básico es usar el comando:

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

Por lo tanto, puede generar fácilmente la lista de comandos en una hoja de cálculo y ejecutar toda la lista en Windows Power Shell

Ejemplo:

```
PS> Set-ADUser Bobama -numero empleado 12345678
```

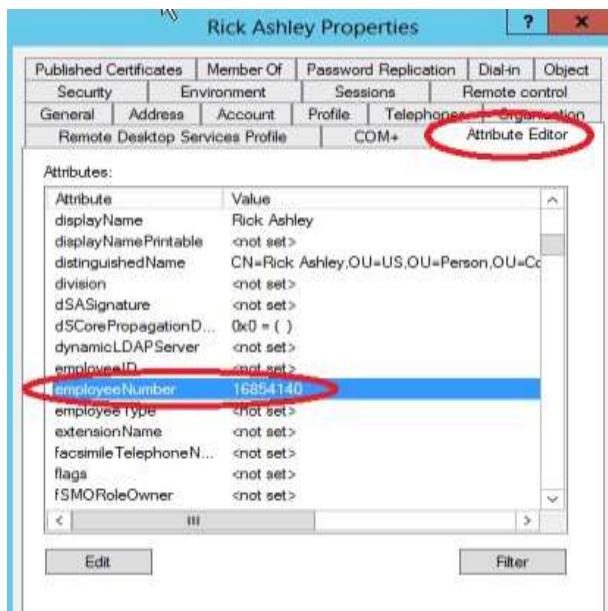
***IMPORTANTE:***

*Cuando se selecciona 1-Global Catalog, como Tipo de conexión LDAP, algunos atributos como "EmployeeID" no forman parte predeterminada del esquema de catálogo global. (PAS Partial Attribute Set)*

*Asegúrese de que los atributos seleccionados formen parte del Catálogo Global.*

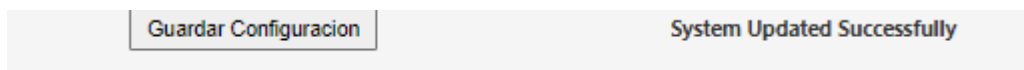
*Puede consultar esta guía para incluirlos en el Global Catalog.*

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



**Longitud del atributo:** Número de dígitos del parámetro numérico. Una vez más, los valores en los Usuarios deben tener siempre la misma longitud. En el ejemplo anterior, este número es 8.

**Guardar configuración:** Haga clic en "Guardar" y debería ver "Sistema actualizado correctamente" o "Success". Si recibe otro mensaje, revise los parámetros anteriores. El mensaje "Success", indica que hasta ahora, la conexión al LDAP es exitosa.



### Probar el desbloqueo y restablecimiento de cuentas.

Una vez validada la conexión, se debe comprobar si el usuario proporcionado en los últimos pasos, es capaz de desbloquear y restablecer las cuentas. Proceda a probar con una cuenta de usuario de prueba, proveyendo el numero para su "User Attribute". Haga clic en "Probar Desbloqueo" y "Probar Reseteo".



### Prueba de desbloqueo:

Si recibe algún otro mensaje en lugar de "Success", revise los permisos de su cuenta de administrador, o cuenta de servicio. Si obtuviste "Success" esto significa que la cuenta de usuario correspondiente al "employeeNumber" (estamos usando employeeNumber solo como ejemplo), puedo bloquearse exitosamente. Puede bloquear esta cuenta a propósito y luego intentar desbloquearla en este paso y comprobar en su Active Directory que efectivamente fue desbloqueada.

**Probar Reseteo:**

Debería ver la contraseña temporal creada, junto al mensaje "Success".

**Importante:** Call2Unlock genera una contraseña aleatoria que cumple con las políticas de seguridad básicas para la contraseña de Windows. 8 caracteres o más, 1 o más caracteres numéricos, 1 o más caracteres mayúsculas

Una vez finalizada la prueba de desbloqueo y reseteo, el sistema nos permitirá pasar al paso 4

**Paso 04:**

Step1

Step2

Step3

Step4

Step5

PASO 4. Obtenemos la lista de cuentas de usuario. Call2Unlock consultará sus objetos de usuario de AD filtrados por OU o grupos. En el caso de grupos universales o anidados entre un árbol de dominios (dominios principales y secundarios), obtendremos todas las cuentas en el dominio que coincidan con los criterios de estar dentro de los grupos anidados que pertenecen al conjunto en 'Cadena DC de grupo'. Todos los controles deshabilitados corresponden a configuraciones ya proporcionadas en los pasos anteriores (1-2-3), se presentan solo como referencia. Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración

Propiedad	Valor	Descripción
DC String de Usuarios Finales	dc=cordialo,dc=net	Rama en el directorio LDAP, desde donde el sistema intentará encontrar a los usuarios. Ejemplo <b>ou=Person,ou=Corporate,dc=domain,dc=com</b>  This field was populated on the Step3. If you need to update it, please run the Wizzard Again and update it on Step3
DC String del Grupo de Usuarios Finales	memberOf:1.2.840.113556.1.4.1941:=CN=all 2 unlock users,DC=cordialo,DC=net	Grupo para filtrar usuarios, solo los usuarios de este grupo podrán usar el sistema. (Deje en blanco si no está usando grupos para filtrar). Ejemplo: <b>memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net</b>  Para grupos anidados dentro de un Grupo Universal. Agregue esta cadena antes de su Cadena de grupo <b>memberOf:1.2.840.113556.1.4.1941:=</b>  Entonces, el grupo DC completo, incluidos los grupos anidados, sería para el ejemplo: <b>memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net</b>

Guardar Configuracion

...

En esta sección deberá proporcionar el grupo (en un entorno multidominio, podría ser un Grupo universal), incluirá todos los grupos anidados miembros del grupo padre.

**Group DC String del Grupo de Usuarios Finales:** Grupo para filtrar usuarios, solo los usuarios de este grupo podrán usar el sistema. (Deje en blanco si no está utilizando grupos para filtrar)

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

**IMPORTANTE:**

*Cuando se selecciona 1-Global Catalog como Tipo de conexión LDAP, se utilizará la cadena de DC de grupo para filtrar los usuarios en todo el dominio. Así que este grupo debe ser un "Grupo Universal".*

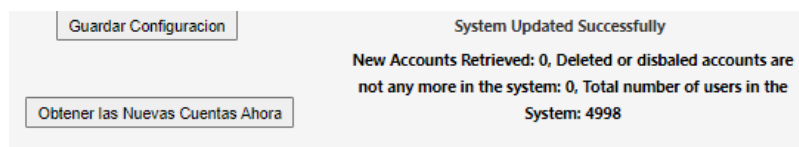
**GRUPOS ANIDADOS EN CADA DOMINIO**

*Otra posibilidad es inscribir a los miembros de algunos grupos globales que ya tenga en cada servidor de AD. En este caso, solo necesita hacer que esos Grupos Globales sean miembros del Grupo Universal. Esto se llama "miembros de grupos NESTED". Para que el filtro de grupo llegue a los miembros de los grupos NESTED, debe incluir el parámetro de código "1.2.840.113556.1.4.1941"*

*Example:*

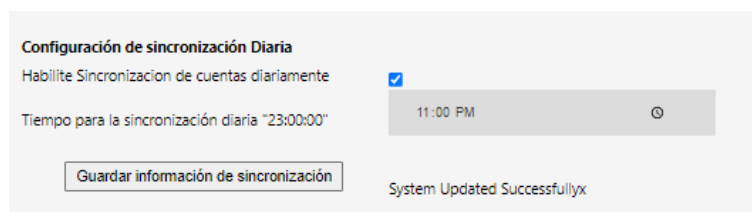
***memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net***

Una vez que haya guardado los cambios, haga clic en "Recuperar nuevas cuentas ahora". Si es la primera vez que se ejecuta el asistente, todas las cuentas se considerarán nuevas, de lo contrario, el sistema simplemente agregará las nuevas y eliminará de su base de datos interna las cuentas deshabilitadas.



A screenshot of a system update confirmation dialog. On the left, there are two buttons: "Guardar Configuración" at the top and "Obtener las Nuevas Cuentas Ahora" at the bottom. On the right, the text reads: "System Updated Successfully", "New Accounts Retrieved: 0, Deleted or disabled accounts are not any more in the system: 0, Total number of users in the System: 4998".

Este proceso se puede configurar para que se ejecute diariamente a una hora específica. Por lo tanto, las nuevas cuentas creadas en Active Directory podrán usar Call2Unlock a más tardar al día siguiente.



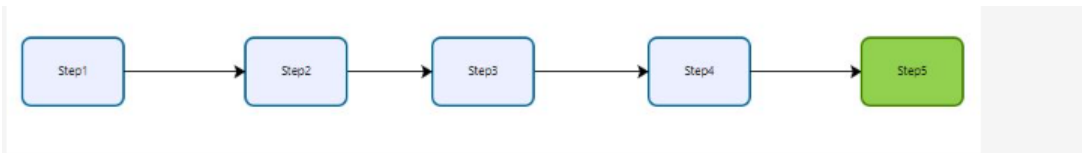
A screenshot of the "Configuración de sincronización Diaria" (Daily Synchronization Configuration) dialog. It has a title bar and a checkbox labeled "Habilite Sincronización de cuentas diariamente" which is checked. Below the checkbox, it says "Tiempo para la sincronización diaria '23:00:00'". To the right of this text is a time selection field showing "11:00 PM" with a clock icon. At the bottom left is a button labeled "Guardar información de sincronización". At the bottom right, it says "System Updated Successfullyx".



Finalmente puede hacer clic en "Ejecutar informe", para verificar que obtenemos la lista de cuentas. También puede buscar una cuenta específica utilizando el cuadro de filtro.

Una vez completado, podemos pasar al 5to y último paso de nuestro asistente de configuración LDAP.

Paso 05:



PASO 5. Casi Listo. Finalmente, completemos las opciones de seguridad y entrega y apliquemos los cambios. Algunos controles pueden estar deshabilitados, dado que ya proporcionó esa información en los pasos anteriores (1-4). Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración

Propiedad	Valor	Descripción
Atributo de usuario	employeeNumber	Propiedad de usuario, que será utilizada por el usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: EmployeeNumber
Longitud del atributo	5	Longitud estándar del atributo User. Esta debe tener la misma longitud para todos los usuarios. Ej:(En el atributo es 01903399, la Longitud =6)
Tipo de atributo de confirmación de usuario	2. MFA Radius Server	0. En Call2unlock DB. El sistema utilizará el número PIN generado por el usuario en el portal de autoservicio de call2unlock.  1. En AD. Significa que el pin de confirmación se coloca en el AD y deberá completar el Atributo de usuario para la información de confirmación  2. Servidor de Radius MFA. Significa que el usuario validará con PIN + Token Number proporcionado por el proveedor de autenticación de segundo factor (como Google Authenticator) a través de un servidor Radius. El servidor Radius podría ser un Radius local que se ejecuta en el servidor Call2unlock o cualquier servidor Radius externo existente en la empresa. Vaya a la sección de configuración de Radius para que esto funcione
Atributo de usuario para confirmación	employeeID	En caso de que el tipo de atributo de confirmación de usuario sea 'En AD'. Propiedad del usuario, que se utilizará para confirmar la acción del usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: 4 últimos dígitos del SSN o ID de empleado
Longitud de atributo para confirmación	4	En caso de que el Tipo de Atributo de Confirmación de Usuario sea 'En AD'. Longitud estándar del atributo de Usuario para confirmación Esta debe ser la misma longitud para todos los usuarios. Ej:(En el atributo es 1157, la Longitud =4)
DC String de Usuarios Finales	dc=oordialo,dc=net	Rama en el directorio LDAP, desde donde el sistema intentará encontrar a los usuarios. Ejemplo Example: ou=Person,ou=Corporate,dc=domain,dc=com

En este paso usted configurará el resto de parámetros de configuración, como: Lugar de validación de usuario (Active Directory, Call2unlockDB, 2FA), Entrega de contraseñas (Audio, SMS, Correo electrónico), Complejidad de contraseñas, etc. (Todas las etiquetas de propiedad en rojo). Los controles deshabilitados corresponden a la configuración ya proporcionada en el paso anterior.

Número máximo de intentos fallidos	7	Cuando los usuarios proporcionan el número PIN erróneo, este es el máximo de fallas en un día. Después de fallar esta cantidad de veces, esta cuenta se incluirá en una lista negra por seguridad. Cada noche, un proceso cron libera las cuentas de la lista negra (Valor predeterminado: 5 intentos fallidos)
Longitud de la contraseña de AD	8	Complejidad de la contraseña: longitud de la contraseña. Se utilizará para generar contraseñas temporales. (Predeterminado 8)
Numero de caracteres en Mayúsculas	3	Complejidad de la contraseña: número de caracteres en mayúscula deseados dentro de las contraseñas temporales. (Predeterminado 3)
Numero de caracteres en Minúsculas	2	Complejidad de la contraseña: número de caracteres en minúsculas deseados dentro de las contraseñas temporales. (Predeterminado 3)
Numero de caracteres Numéricos	3	Complejidad de la contraseña: número de caracteres numéricos deseados dentro de las contraseñas temporales. (Predeterminado 2)
Numero de caracteres especiales	0	Complejidad de la contraseña: número de caracteres especiales deseados dentro de las contraseñas temporales (predeterminado 0)
Modo de entrega:	1. Only Audio	Modos de entrega para contraseñas temporales: elija un modo de la lista
Números de caracteres para el primer medio	8	Número de caracteres que se entregarán en el primer medio, REGLAS: Este número debe ser siempre mayor a 1, o debe ser igual a la Longitud de la Contraseña en caso de que la opción de envío incluya un solo medio.
Números de caracteres para el segundo medio	0	Número de caracteres que se entregarán en el segundo medio, REGLAS: Usar solo en caso de que el modo de entrega consista en dos medios diferentes, de lo contrario establecer en 0. Este número debe ser siempre mayor que 1. La suma de este número más el primero los medios de caracteres deben ser los mismos que la longitud de la contraseña
Correo electrónico del Administrador	admin@mydomain.com	Dirección de correo electrónico o DL donde se enviarán las notificaciones o alarmas de seguridad.

...

Una vez que guarde todos los parámetros, haga clic en "Aplicar configuración y generar script IVR", luego el sistema volverá a generar los scripts IVR basados en esta configuración.

¡FELICIDADES!. Su infraestructura de Active Directory está completamente integrada a call2unlock. Puede acceder a todos los ajustes proporcionados en los cinco pasos anteriores en la ventana todo en uno llamada "CONFIGURACIÓN LDAP".

#### 4. Configuración LDAP

Si ya ejecutó el Asistente de configuración LDAP en la última sección, esta ventana de configuración LDAP mostrará toda la colección de datos, para que pueda editar y probar todos a la vez en este lugar único.

Vaya a la opción de menú "LDAP / CONFIGURACIÓN". Debería obtener una lista de parámetros como la siguiente. La mayoría de las opciones se explican en la columna de descripción

Propiedad	Valor	Descripción
Dirección IP	10.0.2.231 	Dirección IP del controlador de dominio principal
Nombre de Host	myadserver	Nombre de host del controlador de dominio principal
Tipo de conexión LDAP	1. Global Catalog 	0. Servidor de directorio activo. Utilice esta opción si va a utilizar un Dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory. 1. Catálogo Global. Utilice esta opción si tiene un bosque con varios dominios. El puerto del catálogo global, en el servidor AD del dominio raíz, se utilizará para buscar objetos y el puerto LDAP para desbloquear y restablecer cuentas. Asegúrese de incluir la lista de sus servidores en el campo Lista de servidores AD.
Puerto LDAP	636	Puerto LDAP para conectarse a LDAP (389 por defecto, 636 recomendado)
Puerto de catálogo global	3268	Puerto de catálogo global (3268 por defecto, 3269 recomendado)
Nombre de cuenta de administrador	sov_c2admin	Cuenta con privilegios de administrador
Contraseña de administrador		Contraseña de la Cuenta de administrator
Adm DC string	cn=Users,dc=evt,dc=cordialo,dc=net	DC String para la cuenta con administrador priv. Ejemplo cn=Adminuser,dc=domain,dc=com
Lista de servidores AD	10.0.2.231 cordialo.net;10.0.2.131 evt.cordialo.net;10.0.2.31 lv.cordialo.net	Escriba su lista de servidores AD si está utilizando un catálogo global y un entorno multidominio. Escriba la dirección IP, el nombre del servidor y un punto y coma para cada controlador de dominio. Este contenido se agregará al archivo /etc/hosts Ejemplo: Por favor, elimine los espacios en blanco, especialmente al comienzo de cada fila. Ejemplo 10.0.2.230 domain.net; 10.0.3.230 child1.domain.net; 10.0.4.230 child2.domain.net
Atributo de usuario	employeeNumber	Propiedad de usuario, que será utilizada por el usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: employeeNumber
Longitud del atributo	5	Longitud estándar del atributo User. Esta debe tener la misma longitud para todos los usuarios. Ej:(En el atributo es 01903399, la Longitud =8)

Se deben proporcionar los siguientes parámetros.

**Dirección IP:** Dirección IP del servidor de Active Directory. Si desea trabajar con un bosque de dominio completo, esta dirección IP es el servidor de AD de dominio raíz con un catálogo global en ejecución.

**Nombre de host:** Nombre del servidor de Active Directory. (Este valor es solo informativo, no se considerará como un parámetro para la conexión LDAP).

**Tipo de conexión LDAP:** Esta selección nos permite trabajar con un bosque completo de Active Directory, incluidos dominios secundarios, o directamente con un único servidor AD de dominio.

**0. Active Directory Server.** Utilice esta opción si va a utilizar un dominio único. Solo se utilizará el puerto LDAP para conectar el servidor de Active Directory.

**1. Global Catalog.** Utilice esta opción si tiene un bosque con varios dominios. El puerto de Global Catalog en el servidor de AD del dominio raíz, se usará para buscar objetos y los puertos LDAP para desbloquear y restablecer cuentas en todos los Controladores de Dominio.

**Puerto LDAP:** puerto LDAP para Active Directory. Por defecto, 389. Call2unlock utiliza LDAPS (LDAP Seguro), por lo que se recomendará 636.

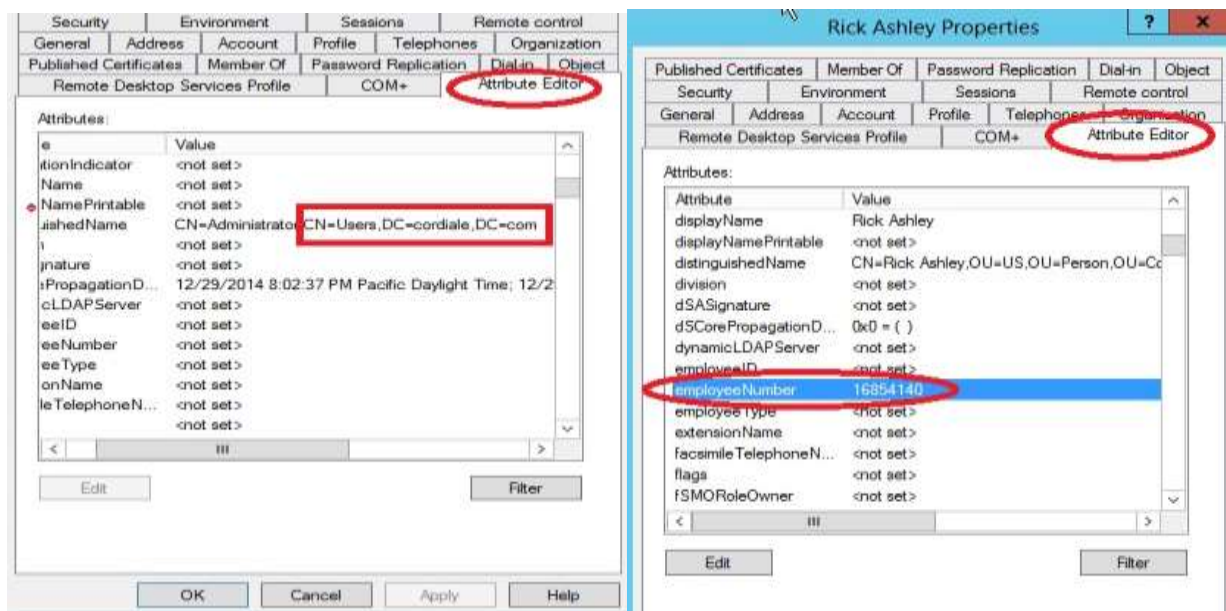
**Puerto de catálogo global:** Puerto utilizado para el catálogo global (en caso de que se seleccione 1. Global Catalog como Tipo de conexión LDAP). Normalmente, el puerto 3269 para conexiones seguras

**Nombre de cuenta de Administrador:** Esta cuenta debe tener privilegios suficientes para desbloquear o restablecer cuentas en su directorio activo. Típicamente una cuenta de servicio

**Adm Password:** contraseña en AD para la cuenta de administrador

**Adm DC string:** Este es el nombre distintivo de la unidad organizativa a la que pertenece la cuenta LDAP de administrador. Para obtener esta información, vaya a su servidor de AD, en "Usuarios de Active Directory y equipos", vaya a "Editor de atributos" y copie el "DistinguishedName", pero solo de la unidad organizativa, sin tomar el nombre de la cuenta.

En la imagen de abajo, de la cadena "cn=Administrator,cn=Users,dc=cordiale,dc=com" solo se ha tomado "cn=Users,dc=cordiale,dc=com"



**Lista de servidores de AD:** Esta es la lista de la lista de servidores de AD. Si usa el catálogo global y un entorno multidominio, escriba la dirección IP, el nombre del servidor y un punto y coma para cada controlador de dominio. Este contenido se agregará al archivo /etc/hosts Ejemplo de contenido de este campo:

**10.0.2.230 domain.net;**

**10.0.3.230 child1.domain.net;**

**10.0.4.230 child2.domain.net**

El sistema colocará al final del archivo /etc/hosts algo como:

**10.0.2.230 domain.net**

**10.0.3.230 child1.domain.net**

**10.0.4.230 child2.domain.net**

**Atributo de usuario:** Las cuentas en su AD deben tener un parámetro numérico estándar, que se utilizará para identificar las cuentas. En el ejemplo se utilizará employeeNumber.

Importante:

- El parámetro seleccionado debe ser numérico.
- Debe tener una longitud estándar para todos los usuarios

Si no tiene en su AD, un parámetro numérico que identifique a los usuarios, primero considere incluir este atributo, y asignarlo cada vez que se creen nuevas cuentas. Ejecute un script para completar esta información para todos sus usuarios actuales que aún no cuenten con este atributo.

Hay varios ejemplos en la web, sobre scripts para actualizar los parámetros de las cuentas de usuario. Un ejemplo básico es usar el comando:

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

Por lo tanto, puede generar fácilmente la lista de comandos en una hoja de cálculo y ejecutar toda la lista en Windows Power Shell

Ejemplo:

```
PS> Set-ADUser Bobama –número empleado 12345678
```

**IMPORTANTE:**

*Cuando se selecciona 1-Global Catalog, como Tipo de conexión LDAP, algunos atributos como "EmployeeID" no forman parte predeterminada del esquema de catálogo global. (PAS Partial Attribute Set)*

Asegúrese de que los atributos seleccionados formen parte del Catálogo Global.

Puede consultar esta guía para incluirlos en el Global Catalog.

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

**Longitud del atributo:** Número de dígitos que tiene el parámetro anterior. Una vez más, los valores en los Usuarios deben tener siempre la misma longitud. En el ejemplo anterior, este número es 8.

Tipo de atributo de confirmación de usuario	1. In AD	<p>0. En Call2unlock DB. El sistema utilizará el número PIN generado por el usuario en el portal de autoservicio de call2unlock.</p> <p>1. En AD. Significa que el pin de confirmación se coloca en el AD y deberá completar el Atributo de usuario para la información de confirmación</p> <p>2. Servidor de Radius MFA. Significa que el usuario validará con PIN + Token Number proporcionado por el proveedor de autenticación de segundo factor (como Google Authenticator) a través de un servidor Radius. El servidor Radius podría ser un Radius local que se ejecuta en el servidor Call2unlock o cualquier servidor Radius externo existente en la empresa. Vaya a la sección de configuración de Radius para que esto funcione</p>
Atributo de usuario para confirmación	employeeID	En caso de que el tipo de atributo de confirmación de usuario sea 'En AD'. Propiedad del usuario, que se utilizará para confirmar la acción del usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: 4 últimos dígitos del SSN o ID de empleado
Longitud de atributo para confirmación	4	En caso de que el Tipo de Atributo de Confirmación de Usuario sea 'En AD'. Longitud estándar del atributo de Usuario para confirmación Esta debe ser la misma longitud para todos los usuarios. Ej:(En el atributo es 1157, la Longitud =4)
DC String de Usuarios Finales	dc=cordiale,dc=net	Rama en el directorio LDAP, desde donde el sistema intentará encontrar a los usuarios. Ejemplo ou=Person,ou=Corporate,dc=domain,dc=com
DC String del Grupo de Usuarios Finales	memberOf:1.2.840.113556.1.4.1941:=CN=call2unlock:users,DC=cordiale,DC=net	<p>Grupo para filtrar usuarios, solo los usuarios de este grupo podrán usar el sistema. (Deje en blanco si no está usando grupos para filtrar). Ejemplo: memberOf=CN=fieldusers,CN=Users,DC=cordiale,DC=net</p> <p>Para grupos anidados dentro de un Grupo Universal. Agregue esta cadena antes de su Cadena de grupo memberOf:1.2.840.113556.1.4.1941:=</p> <p>Entonces, el grupo DC completo, incluidos los grupos anidados, sería para el ejemplo: memberOf:1.2.840.113556.1.4.1941:=CN=fieldusers,CN=Users,DC=cordiale,DC=net</p>

**Tipo de atributo de confirmación de usuario:** Una vez que el usuario se encuentra en AD, para desbloquear o restablecer la contraseña, el usuario debe insertar un número PIN. Este atributo se utiliza para determinar dónde se ubicará este número PIN

0. Call2unlock Database
1. Active Directory (Será un atributo de cuenta de usuario dentro de AD)



2. MFA. Radius Server. Debe configurar previamente la integración RADIUS local o externa para hacer uso de esta función. Se explicará en la sección de configuración RADIUS de este manual

**Atributo de usuario para confirmación:** En caso de que se seleccione la opción 1 (Active Directory) como tipo de atributo de confirmación, el nombre del atributo debe especificarse aquí.

**Longitud del atributo para la confirmación:** Número de dígitos del atributo para la confirmación. Todos los usuarios deben tener este atributo con el mismo número de dígitos.

**DC String de usuarios:** "DistinguishedName" de la unidad organizativa donde se encuentran los usuarios. Los usuarios dentro de otras unidades organizativas dentro de la unidad organizativa raíz también serán considerados.

Ejemplo: Si en el sistema tenemos como User OU String:

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

Esto significa que también se incluirán los usuarios de la siguiente unidad organizativa.

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

**Group DC String:** Grupo para filtrar usuarios, solo los usuarios de este grupo podrán usar el sistema. (Deje en blanco si no está utilizando grupos para filtrar)

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

#### **IMPORTANTE:**

*Cuando se selecciona 1-Global Catalog como Tipo de conexión LDAP, se utilizará la cadena de DC de grupo para filtrar los usuarios en todo el dominio. Así que este grupo debe ser un "Grupo Universal".*

#### **GRUPOS ANIDADOS EN CADA DOMINIO**

*Otra posibilidad es inscribir a los miembros de algunos grupos globales que ya tenga en cada servidor de AD. En este caso, solo necesita hacer que esos Grupos Globales sean miembros del Grupo Universal. Esto se llama "miembros de grupos NESTED". Para que el filtro de grupo llegue a los miembros de los grupos NESTED, debe incluir el parámetro de código "1.2.840.113556.1.4.1941"*

*Ejemplo:*

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



**Número máximo de intentos fallidos:** Si por alguna razón el usuario no proporciona el número PIN correcto, el sistema incluye a este usuario en una lista negra y envía una alerta por correo electrónico al administrador. En este campo, el administrador configura el número máximo de intentos fallidos.

**Correo electrónico del administrador:** Todas las notificaciones, especialmente cuando un usuario ha sido incluido en la lista negra, se enviarán a esta cuenta de correo electrónico. Podría ser un correo electrónico normal o una lista de distribución.

**\*\* Nota:** Una vez que un usuario está en la lista negra, solo el administrador puede liberar la cuenta, para poder usar call2unlock nuevamente. Esta opción está disponible en el módulo Edición de usuario Final

**Cargar certificado:** debe cargar el certificado pem generado previamente en su AD. Este certificado es necesario para realizar acciones como restablecer contraseñas desde call2unlock.

Subir certificado	Cargue su Certificado AD	Certificado generado, utilizando los servicios de certificados de Active Directory. Una vez que cargue su certificado, espere hasta que reciba el mensaje Cargado correctamente. Para saber cómo generar un certificado de CA en su servidor de Active Directory, (Descargar desde aquí)
	Choose File No file chosen	
	Submit	

Para generar este certificado siguiendo el manual, "Generación del certificado AD", que está disponible en el sitio web de Call2Unlock <http://www.call2unlock.com/documentation/>

**Prueba de conexión:** Haga clic en "Guardar y probar", y debería ver "Cambios aplicados en la base de datos" y también "Success". Si recibe otro mensaje, revise los parámetros anteriores. El mensaje "Success", indica que hasta ahora, la conexión al LDAP es exitosa.

Guardar y Probar	Changes Applied on Database	Success
------------------	-----------------------------	---------

### Probar el desbloqueo y restablecimiento de cuentas.

Una vez validada la conexión, se debe comprobar si el usuario proporcionado en el último paso, es capaz de desbloquear y restablecer las cuentas.

Valor de atributo de usuario	06801		
Probar Desbloqueo	Nombre de Cuenta cn: Jhon Smith	Resultado Success	
Probar Reseteo	Correo electrónico del Administrador admin@mycompany.com	Nombre de Cuenta cn: Jhon Smith	Resultado Success Temp Pass: "JChp30??"

### Prueba de desbloqueo:

Si recibe algún otro mensaje en lugar de "Success", revise los permisos de su cuenta de administrador, o cuenta de servicio. Si obtuviste "Success" esto significa que la cuenta de usuario correspondiente al "employeeNumber" (estamos usando employeeNumber solo como ejemplo), puedo bloquearse exitosamente. Puede bloquear esta cuenta a propósito y luego intentar desbloquearla en este paso y comprobar en su Active Directory que efectivamente fue desbloqueada.

### Probar Reseteo:

Debería ver la contraseña temporal creada, junto al mensaje "Success".

**Importante:** Call2Unlock genera una contraseña aleatoria que cumple con las políticas de seguridad básicas para la contraseña de Windows. 8 caracteres o más, 1 o más caracteres numéricos, 1 o más caracteres mayúsculas

### Guardar configuración:

Una vez que toda su prueba haya sido exitosa, presione el botón "Guardar configuración".

Debería recibir el mensaje "System Updated Successfully" (marcado en rojo en la imagen de abajo).

**La configuración solo se guardará si todas las pruebas anteriores fueron exitosas, de lo contrario, call2unlock no permitirá al usuario guardar la configuración**

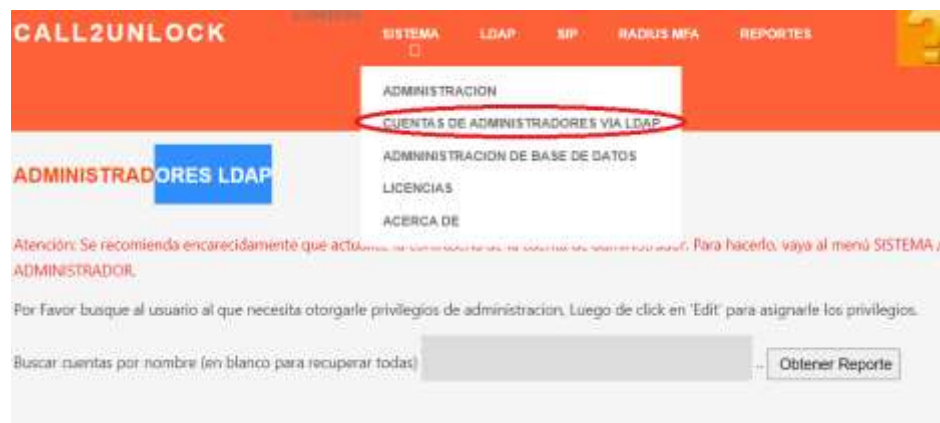
Nota: La contraseña temporal debe enviarse al correo electrónico proporcionado por el usuario. Intente iniciar sesión en Active Directory con la contraseña temporal. Debería de funcionar. Además, el sistema debería pedirle que cambie la contraseña temporal.

Paso 4. Guarde su configuración. Asegúrese de haber probado los 2 pasos anteriores con éxito, de lo contrario, la configuración no se aplicará

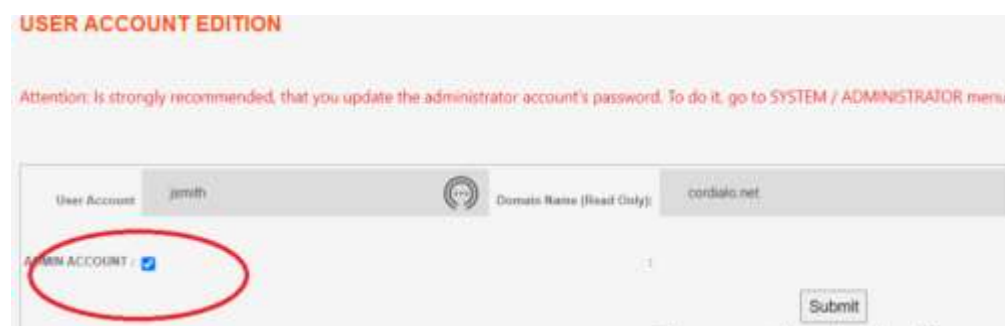


## 5. CUENTAS DE ADMINISTRACION VIA LDAP

Una vez que haya completado su configuración LDAP, tendrá sus cuentas sincronizadas con su AD. Es hora de elegir qué cuentas tendrán privilegios de administrador, por lo que no tendremos una única cuenta de administrador root única. Para agregar un nuevo usuario Administrador desde su AD, vaya a SISTEMA/CUENTAS DE ADMINISTRACION VIA LDAP



Luego puede buscar su usuario y hacer clic en "Obtener Reporte". Obtendrá la lista de usuarios de su búsqueda. Tiene que editar esta cuenta para asignarle privilegios de administrador.



Ahora la nueva cuenta de administrador puede ir a la página inicial <https://youripaddress>

Luego el usuario debera usar su cuenta de AD para autenticarse.

Si la autenticación es exitosa. (El usuario se autenticó con la contraseña de AD correcta, y también él/ella ya estaba configurado como Administrador en el último paso, el usuario debe obtener la página de INICIO del sistema, con el mensaje en la parte superior “Connection to LDAP service successfully”

## 6. ASISTENTE DE CONFIGURACIÓN SIP:

Esta es también una sección muy importante. Aquí podrá configurar y probar los parámetros y credenciales necesarias para integrar Call2unlock con su PBX corporativa. Este asistente consta de una serie de 03 pasos que lo guiarán a través del proceso y detectarán cualquier problema y la solución sugerida. **Previamente, es necesario crear una cuenta troncal SIP en su PBX, para estar registrado en la dirección IP Call2unlock (Asterisk PBX).** Esta configuración puede ser diferente en cada marca y modelo de PBX. Para Cisco CUCM, puede consultar este manual:

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

**Paso 01:** Prueba de conectividad. El sistema verifica que los puertos involucrados sean accesibles desde call2unlock a su IP PBX

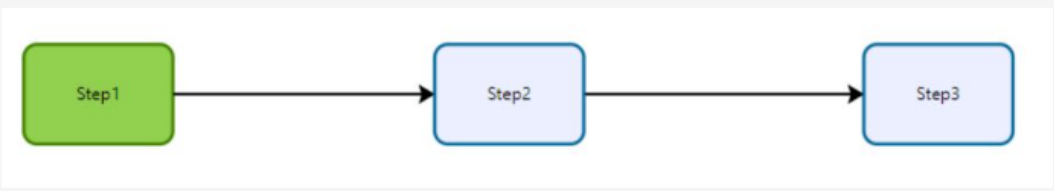
**Step02:** Registro SIP: El sistema verifica que la cuenta troncal SIP creada en su PBX esté registrada en call2unlock. Entonces, desde la perspectiva de señalización, los dos sistemas (su IP PBX y Call2unlock) se comunicarán entre sí.

**Step03:** Generar el plan de marcación interno: Allí configurará el prefijo para las llamadas que van desde su IP PBX a Call2unlock, para que Call2unlock pueda procesar la llamada a través de su IVR.

Una vez completados los 03 pasos, Call2unlock generará el script IVR, que se presentará al usuario cada vez que marque la extensión interna asignada a Call2Unlock o el numero telefónico DID, quedando el sistema listo para usar.

Vaya a la opción de menú "SIP / ASISTENTE DE CONFIGURACION SIP". Debería obtener la página Step1

## Paso 01:



PASO 1. Verifiquemos que tenga conectividad a su infraestructura IP PBX. Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración

Propiedad	Valor	Descripción
Dirección IP de la centralita	10.0.0.31	Dirección IP de PBX Publisher or Subscriber
Protocolo de señalización SIP	1.UDP	0. Protocolo TCP para señalización. 1. Protocolo UDP para señalización.
Puerto de señalización	5060	Número de puerto para señalización SIP (5060 por defecto)

Prueba de puerto de señalización SIP: Success

Estado de actualización: Changes Applied on Database

**Dirección IP de la centralita:** Dirección IP de su PBX corporativa

**Protocolo de señalización SIP:** Debe seleccionar entre TCP o UDP (según el protocolo que utilice su PBX para la señalización).

Call2Unlock V 4.0 Manual de Administración

**Puerto de señalización:** Número de puerto para señalización (la mayoría de las PBX usarán 5060 o 5061)

Una vez que complete la información requerida, presione "Probar". Si no hay problemas de red (como bloqueos de firewall), debería obtener el mensaje "Success" como resultado.

Si la prueba es exitosa, podrá guardar su configuración. Obtendrá "Changes Applied on Database" como mensaje. Luego haga clic en SIGUIENTE PASO.

## Paso 02:

Step1

Step2

Step3

PASO 2. Intentemos registrar la cuenta SIP que se usará para enviar llamadas desde su PBX a Call2Unlock. Cree la cuenta con las credenciales proporcionadas en su PBX como una cuenta SIP Friend. Este paso creará la cuenta dentro de Call2Unlock para ser autenticado en su PBX. Todos los controles deshabilitados corresponden a las configuraciones ya proporcionadas en el paso anterior (Paso 1). Los nombres de las propiedades en rojo contienen los controles habilitados en los que debe proporcionar o actualizar su configuración.

Propiedad	Valor	Descripción
Dirección IP de la centralita	10.0.0.133	Dirección IP de PBX Publisher or Subscriber
Protocolo de señalización SIP	1.UDP	0. Protocolo TCP para señalización. 1. Protocolo UDP para señalización.
Puerto de señalización	5060	Número de puerto para señalización SIP (5060 por defecto)
Nombre de la Troncal SIP	cordial	Es recomendable asignar el mismo nombre de la cuenta de usuario creada en la Corporate PBX.
Cuenta SIP en su PBX	cordial	Nombre de del usuario Trunk creado la Centralita Corporativa.
Contraseña de la cuenta PBX	*****	Contraseña de la Cuenta del Troncal SIP

Guardar

Probar

Estado de actualización: ...

Prueba de autenticación de troncales SIP ...

SIGUIENTE PASO

Solo se requieren los controles con etiquetas rojas. Los que están en las etiquetas negras están deshabilitados y ya se proporcionaron en el paso anterior (Paso 1)

**Nombre de la Troncal Sip:** Es recomendable asignar el mismo nombre de la cuenta de usuario creada en la Corporate PBX"

**Cuenta SIP en su PBX:** Cuenta de usuario para el usuario creado en la PBX corporativa

**Contraseña de la cuenta PBX:** Contraseña de la cuenta creada en la PBX corporativa

Una vez que complete la información requerida, presione "Guardar", debería recibir el mensaje "Configuración SIP Pushed", por lo que la nueva cuenta SIP también se ha creado en Call2unlock como cuenta SIP.

Luego haga clic en "Probar", para validar que la cuenta está registrada en su PBX corporativa. Debería obtener "Success" como resultado.

### Paso 03:

```

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

<b>Prefijo para llamadas internas</b>	8888	Este prefijo identificará si las llamadas provienen de la centralita interna. Esto debe configurarse en el plan de marcado de PBX
<b>Permitir todas las llamadas internas</b>	<input checked="" type="checkbox"/>	Si está marcado, los usuarios pueden llamar desde todas las extensiones internas. De lo contrario, los usuarios solo pueden llamar desde sus extensiones, configuradas en el módulo Prefijo para cuentas de usuario de llamadas PSTN, por sí mismos o por el administrador.
<b>Prefijo para llamadas PSTN (Telefonia Publica)</b>	9999	Este prefijo indica que la llamada proviene de la PSTN. Esto debería estar configurado en el plan de marcación de PBX.
<b>Número de dígitos para el prefijo</b>	4	Número de dígitos para el prefijo, para identificar el prefijo de los números reales telefonicos
<b>Idioma para audios generales</b>	es	Idioma para instrucciones IVR. Todos los mensajes se mostrarán en este idioma en= inglés, es = español.
<b>Plan de marcación para transferir a la mesa de ayuda</b>		Instrucciones de Dialplan para redirigir la llamada a la mesa de ayuda si el usuario tiene problemas para usar el sistema. No se permiten comillas simples, se aceptan comillas dobles de usuario. Ejemplo \$AGI->set_callerid("544"); \$AGI->exec("Dial","SIP/c2u/121212");

Solo se requieren los controles con etiquetas rojas. Los que están en las etiquetas negras están deshabilitados y ya se proporcionaron en el paso anterior (Paso 2)

**Permitir todas las llamadas internas:** Marque esta opción, en caso de que desee permitir que todos los empleados desbloqueen sus cuentas desde cualquier extensión interna. De lo contrario, los usuarios deben proporcionar la extensión interna desde la que van a marcar, esto se puede hacer en el portal self-web, y se explicará más adelante.

**Prefijo para llamadas internas:** Prefijo utilizado para la extensión interna, al enviar llamadas desde la PBX hacia Call2Unlock.

**Prefijo para llamadas PSTN:** Prefijo utilizado para teléfonos externos, al enviar llamadas desde el PBX hacia Call2Unlock.

**Número de dígitos para el prefijo:** Número de dígitos que se considerarán solo como prefijo para llamadas externas.

**Idioma para audios generales:** Idioma para los audios generales (en = inglés, es = español)

**Plan de Marcación para transferir a la mesa de ayuda:** Plan de marcado Instrucciones para redirigir la llamada al servicio de asistencia si el usuario tiene problemas para utilizar el sistema. Ejemplo de plan de marcado

`SIP/c2u/121212`

En ese caso, Call2Unlock redirigirá la llamada a la extensión "121212" hacia el PBX corporativo a través de la troncal SIP llamada c2u. Para obtener más información sobre esta configuración, consulte con nuestros especialistas.

Una vez que complete la información requerida, presione "Guardar", debería recibir el mensaje "SIP Config Pushed"

Ahora es el momento de enviar una llamada desde su IP PBX (usando el prefijo). Se recomienda abrir una consola de asterisk (asterisk –rvvv) desde una sesión ssh en call2unlock para comprobar si estamos recibiendo los mensajes de señalización. También deberíamos obtener audio (el mensaje de bienvenida de Call2unlock). Si recibe mensajes de señalización, pero la llamada es silenciosa, verifique los puertos RTP.

Importante: Dado que Call2unlock utiliza asterisk como IP PBX, está configurado de forma predeterminada para enviar y recibir paquetes de audio (RTP), en el rango de puertos 10000 y 20000 UDP. Si su IP PBX utiliza un rango diferente, (Como ejemplo Cisco CUCM utiliza el rango UDP 16384 – 32767. Es posible que deba ajustar los puertos RTP de Call2unlock para que coincidan con los de su IP / PBX. Por lo general, se encuentra en el archivo /etc/asterisk/rtp.conf. Consulte a nuestros expertos si necesita ayuda con esta configuración.



## 7. CONFIGURACIÓN DE SU PBX CORPORATIVA

Generalmente, en su PBX, debe ejecutar los siguientes 3 pasos.

1. **Crear una Troncal SIP** : Asegúrese de establecer "UDP" como el "Tipo de transporte saliente" y proporcione la dirección IP del servidor Call2Unlock. Utiliza los puertos 5060 UDP para la señalización y 10000 – 20000 para RTP.
2. **Crear un plan de marcado:** Cree un número interno donde llamen sus asociados y redirija a la extensión "8888" a través del nuevo tronco creado anteriormente. (8888 es el valor predeterminado en la configuración SIP, **Prefijo para llamadas internas**, puede cambiar esto en SIP / CONFIGURACIÓN).
3. **Prueba de Trunk y Plan de Marcado:**
  - Abra la consola de asterisk en call2unlock ejecutando el siguiente comando:  
**"asterisk -rvvv"**
  - Envíe la llamada desde su PBX. Al menos debería poder recibir tráfico en la consola, algo similar a la salida líneas abajo, si no la recibe, revise tu troncal SIP y el plan de marcación en su PBX.

*Call2Unlock\*CLI>*

*== Uso de SIP RTP CoS mark 5*

*-- Ejecutando [8888@fromcustomerpbx:1] Answer("SIP/9999-00000000", "") en una nueva pila*

*> 0x7f1aac00e240 -- Probation passed - setting RTP source address to 192.168.0.3:20442*

*-- Ejecutando [8888@fromcustomerpbx:2] Set("SIP/9999-00000000", "(CALLERID(num)=88880016961") en una nueva pila*

*-- Ejecutando [8888@fromcustomerpbx:3] Set("SIP/9999-00000000", "CALLFROM=Internal") en una nueva pila*

*-- Ejecución de [8888@fromcustomerpbx:4] AGI("SIP/9999-00000000", "zz\_selfservicead1example.agi") en una nueva pila*

*Call2Unlock\*CLI>*

## 8. CONFIGURACIÓN SIP

En esta sección configurará los parámetros de la troncal SIP entre Call2Unlock y su PBX IP. Si ya ejecutó el Asistente para configuración de SIP desde la última sección, esta ventana de configuración de SIP presentará toda la colección de datos, para que pueda editarlos y probarlos todos a la vez en esta pantalla única.

Vaya a la opción de menú "SIP / CONFIGURACIÓN" y complete la siguiente información:

**Dirección IP de PBX:** Dirección IP de su PBX corporativa

**Cuenta PBX:** Cuenta de usuario para el usuario creado en la PBX corporativa

**Contraseña de la cuenta PBX:** Contraseña de la cuenta en la PBX corporativa

**Permitir todo interno:** Marque esta opción, en caso de que desee permitir que todos los empleados desbloqueen sus cuentas desde cualquier extensión interna. De lo contrario, los usuarios deben proporcionar la extensión interna desde la que van a marcar, esto se puede hacer en el portal self-web, y se explicará más adelante.

**Prefijo para llamadas internas:** Prefijo utilizado para la extensión interna, al enviar llamadas desde la PBX hacia Call2Unlock.

**Prefijo para llamadas PSTN:** Prefijo utilizado para teléfonos externos, al enviar llamadas desde el PBX hacia Call2Unlock.

**Número de dígitos para el prefijo:** Número de dígitos que se considerarán solo como prefijo para llamadas externas.

**Idioma para audios generales:** Idioma para los audios generales (en = inglés, es = español)

**Plan de Marcación para transferir a la mesa de ayuda:** Plan de marcado Instrucciones para redirigir la llamada al servicio de asistencia si el usuario tiene problemas para utilizar el sistema. Ejemplo de plan de marcado

```
set_callerid("544");
```

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

En ese caso, Call2Unlock redirigirá la llamada a la extensión "121212" hacia el PBX corporativo a través de la troncal SIP llamada C2U. Para obtener más información sobre esta configuración, consulte con nuestros especialistas.

**Audios personalizados:** En esta sección puede cargar también audios personalizados, para reemplazar los predeterminados en el sistema. Puedes escuchar los actuales, haciendo clic en el enlace en azul a la derecha. Y puede reemplazarlos eligiendo los archivos de la computadora local y haciendo clic en Enviar, en cada archivo.

Audios personalizados	Reemplazar Nuevo	Escuchar la actual
Bienvenido. Call2Unlock Selfservice. Por favor ingrese su codigo	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Bienvenido
La cuenta que está tratando de desbloquear es	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Cuenta
Si desea desbloquear esta cuenta, presione 1. Si desea restablecer su contraseña, presione 2. Si esta no es su cuenta, presione 0.	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Confirmación
La cuenta, ha sido desbloqueada con exito	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Exito
El código que ha ingresado está duplicado en el sistema. Por favor contacte el administrador.	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Duplicado
No hay ningún usuario que corresponda al código ingresado. Por favor verifique y llame de nuevo	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	No encontrado
La clave que ha ingresado, no corresponde a la cuenta ingresada. Intente de nuevo	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	PIN fallido
Por favor, ingrese su clave.	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Insertar PIN

Los archivos deben guardarse como archivo WAV en mono de 16 bits 8000 Hz.

Después de guardar los cambios, debería recibir el mensaje de éxito

Changes Applied on Database
System Updated Successfully

Es necesario Guardar y volver a generar la configuración LDAP también, cada vez que se realizan cambios en esta sección.

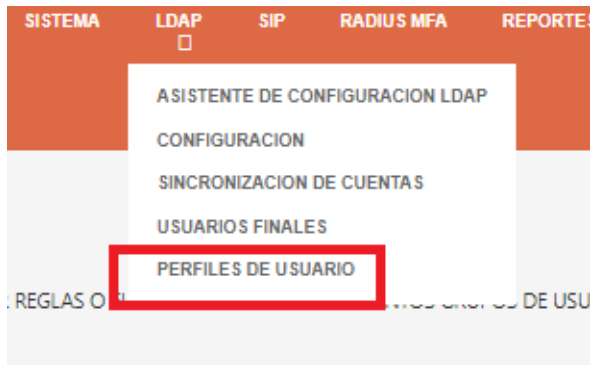
TAMBIÉN: Si se ha cambiado el idioma, es necesario reiniciar todo el sistema

## 9. PERFILES DE USUARIO

Muchas organizaciones requieren asignar diferentes flujos de trabajo para diferentes grupos de usuarios. Por ejemplo:

Group	Location	Authentication	Delivery mode
C2users3	CN=c2users3,CN=Users,DC=td,DC=cordiali,DC=net	AD Pin	Email
C2users1	CN=c2users1,CN=Users,DC=cordiali,DC=net	C2U DB	SMS
C2users2	CN=c2users2,CN=Users,DC=td,DC=cordiali,DC=net	MFA Google Auth	Audio

Para crear vea la lista de perfiles vaya a LDAP / PERFILES DE USUARIO



Si aún no has creado ningún perfil, el sistema por defecto tendrá a todos tus usuarios en un perfil llamado "default". Este perfil predeterminado contiene todas las configuraciones proporcionadas para la configuración LDAP.

### PERFILES DE USUARIO

LOS PERFILES DE USUARIO NOS PERMITEN DEFINIR REGLAS O FLUJOS DISTINTOS PARA DISTINTOS GRUPOS DE USUARIOS

[NUEVO PERFIL](#)

User Profiles				
ID		ProfileName	Description	ActiveUsers
1	Edit	default	default Profile	0
31	Edit	c2users1	Users from the group c2users1 in the Main D	997
33	Edit	c2users3	Users from the group c2users3 in the TD Chi	2001
32	Edit	c2users2	Users from c2users2 from Located in Child TD	993

Puede hacer clic en cualquier elemento de la lista para mostrar los detalles del perfil.:

Propiedad	Valor	Descripción
ID	31	Profile ID
Nombre de Perfil	c2uusers1 	Nombre corto para el perfil. Por favor solo ingrese caracteres simples en minúscula
Description del Perfil	Users from the group c2uusers1 in the Main Domain Controller, AD Authentication (4 digits) and SMS Delivery	Proporcione una breve descripción para el perfil de este usuario.
DC string para el grupo de Usuarios del Perfil	CN=c2uusers1,CN=Users,DC=cordiali,DC=net	Por favor, asegúrese de que este grupo sea miembro de la cadena DC del grupo principal configurada en la configuración Idap. De lo contrario, ningún usuario formará parte de este perfil. También asegúrese de que cada usuario solo pertenezca a un grupo asignado como grupo de perfiles. De lo contrario, el usuario pertenecerá solo al último perfil actualizado
Atributo de usuario	employeeNumber	Propiedad de usuario, que será utilizada por el usuario mediante tonos de marcación desde el teléfono. Este debe ser numérico. Ejemplo: <b>employeeNumber</b>
Longitud del atributo	5	Longitud estándar del atributo User. Esta debe tener la misma longitud para todos los usuarios. Ej:(En el atributo es 01903399, la Longitud =8)
Tipo de atributo de confirmación de usuario	1. In AD 	<p>0. En Call2unlock DB. El sistema utilizará el número PIN generado por el usuario en el portal de autoservicio de call2unlock.</p> <p>1. En AD. Significa que el pin de confirmación se coloca en el AD y deberá completar el Atributo de usuario para la información de confirmación</p> <p>2. Servidor de Radius MFA. Significa que el usuario validará con PIN + Token Number proporcionado por el proveedor de autenticación de segundo factor (como Google Authenticator) a través de un servidor Radius. El servidor Radius podría ser un Radius local que se ejecuta en el servidor Call2unlock o cualquier</p>

También puedes personalizar los mensajes de audio para el IVR para cada perfil.

Este usuario no tiene asignado un numero movil en el sistema, comuniquese con el administrador	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	No numero movil asignado
Esta cuenta ha sido deshabilitada temporalmente por razones de seguridad. Por favor contacte al administrador	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Cuenta en lista negra.
Vamos a repetir una vez mas	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/>	Repita la contraseña temporal.
	IMPORTANTE	Si en control para cargar el audio esta deshabilitado, se debe a que el audio es de caracter general. Si desea personalizar ese audio, hagalo desde el panel SIP Configuracion. Tenga en cuenta que ese cambio impactara a todos los perfiles  TAMBIÉN: Si se ha cambiado el idioma, es necesario reiniciar todo el sistema. .

En la parte inferior de esta pantalla, tienes los controles para "Guardar la configuración". Regenerará un script IVR personalizado dedicado a este perfil, que contiene todas las opciones.

También tienes el botón para recuperar los Usuarios que coinciden con los criterios de filtro del grupo, haciendo clic en "Recuperar Cuentas para el Perfil". Le mostrará cuántos usuarios del total están ejecutando este flujo de trabajo personalizado.

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

Encontrar Usuarios por nombre (Deje en blanco para obtener todos los potenciales miembros del perfil)

User Accounts					
ID		Username	Domain	Profile	Re
1	Edit	dkapp	cordiali.net	c2uusers1	
4	Edit	jamith	cordiali.net	c2uusers1	

Una vez que haya terminado con sus cambios. Puede aplicar los cambios a los usuarios del perfil. Es decir, esos usuarios tendrán el perfil asignado a su entidad listo para ser leído por el IVR

Profile Updated for the selected users

## CREAR PERFILES PERSONALIZADOS

En la misma pantalla de lista de perfiles, hay un botón llamado “NUEVO PERFIL”. Una vez que hagas clic en él tendrás el formulario para completar la información de este nuevo perfil.

**PERFILES DE USUARIO**

LOS PERFILES DE USUARIO NOS PERMITEN DEFINIR REGLAS O FLUJOS DISTINTOS PARA DISTINTOS GRUPOS DE USUARIOS

**NUEVO PERFIL**

User Profiles

ID	ProfileName	Description	ActiveUsers
1 Edit	default	default Profile	0
31 Edit	c2users1	Users from the group c2users1 in the Main D	997
33 Edit	c2users3	Users from the group c2users3 in the TD Chi	2001
32 Edit	c2users2	Users from c2users2 from Located in Child TD	993

**IMPORTANTE:** Los perfiles están adscritos a grupos. Estos grupos tienen que ser miembros del “Grupo Anidado” principal, configurado en la configuración de LDAP . De lo contrario, el sistema no le permitirá crear el perfil, mostrando el mensaje “El grupo no forma parte de los usuarios de Call2Unlock.

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

Save Configuration

Group not part of Call2unlock users

...

Si el grupo es correcto, aparecerá el mensaje “Generando grupo...” y luego “Cambios aplicados en la base de datos”. Y finalmente "No se informaron errores al generar 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

Es importante esperar hasta que aparezca el mensaje “No se reportaron errores al generar audios”. Durante el proceso, el sistema crea los scripts IVR personalizados y crea una copia de todos los audios predeterminados para el nuevo filtro de perfil. Posteriormente podrás modificar esos archivos de audio editando el perfil (Se explica en la opción Editar perfiles)

De la misma manera que Editar perfiles, especialmente porque está creando un nuevo perfil y desea que sus usuarios obtengan este perfil ahora, debe "Aplicar cambios a los usuarios para este perfil" en la parte inferior de la página.

Aplicar los cambios para los usuarios de este perfil

Profile Updated for the selected users

Importante: Los usuarios se sincronizan diariamente. Se explicará en la sección “Sincronización de Cuentas”. Si durante el día, los usuarios fueron deshabilitados, creados o movidos a un grupo diferente, todos esos cambios se reflejarán en el sistema al final del día. O en el momento en que se configura la sincronización automática

## 10. LISTA BLANCA

Si estamos permitiendo llamadas desde la PSTN al sistema (hacia el prefijo configurado en la PBX), todas aquellas llamadas identificadas con ese prefijo, deberían validar que los números de teléfono de donde provienen las llamadas están en una lista blanca. De esta manera, solo los teléfonos permitidos podrán usar el sistema desde la PSTN.

Para mostrar todos los números en la lista blanca, debe ir al menú "SIP / WHITE LIST" escribir %, como filtro y presionar "Get Report".

Para insertar un nuevo número, haga clic en el enlace "Insertar Nuevo número a la lista blanca"

Escriba un número de teléfono para encontrarlo (en blanco para traer todos)

Get Report

Insertar nuevo número a la lista blanca

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

Los números también se pueden actualizar o eliminar, haciendo clic en "Edit" en cada fila



## 11. SINCRONIZACIÓN DE CUENTAS

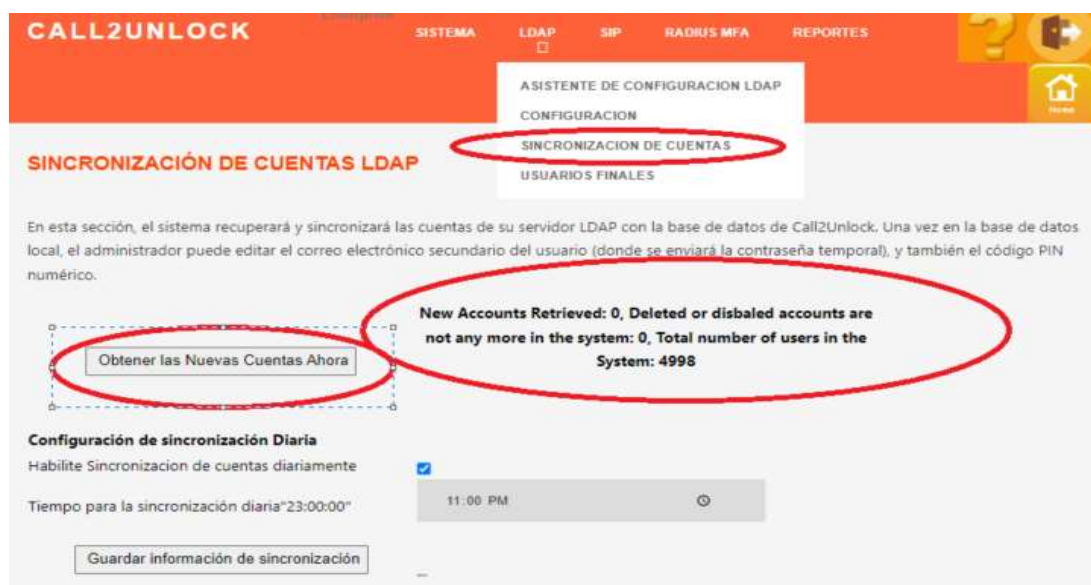
En esta sección, podrá recuperar todas las nuevas cuentas de usuario creadas en su Active directory, hacia Call2Unlock.

El objetivo de esta configuración, es crear los registros necesarios para el portal de usuario de autoservicio, que es el lugar donde los usuarios finales configurarán su correo electrónico secundario y números PIN personales, para el proceso de desbloqueo.

Después de la primera recuperación de las cuentas, cada vez que recupere cuentas, las nuevas cuentas se agregarán a la base de datos local de call2unlock. También las cuentas AD deshabilitadas o eliminadas se eliminarán de la base de datos call2unlock. Por lo tanto, el número de usuarios válidos para la licencia son solo de cuentas activas actuales.

Vaya a la opción de menú "LDAP / SINCRONIZACIÓN DE CUENTA".

Una vez en la sección Cuentas de usuario, presione el botón "Obtener las Nuevas Cuentas Ahora". A continuación, debe recibir el mensaje sobre cuántas cuentas nuevas se han recuperado, cuántas cuentas se han eliminado y cuántas hay en total.



Hasta ahora ha ejecutado la sincronización manualmente, pero querrá que el sistema ejecute esto como una rutina diaria, porque cada día se crean y deshabilitan nuevas cuentas. Para programar la sincronización diaria, marque la casilla "Habilitar recuperar y sincronizar cuentas diariamente", seleccione la hora del día para ejecutar esto, y haga clic en el botón "Guardar información de sincronización"

**Configuración de sincronización Diaria**

Habilite Sincronización de cuentas diariamente ☒

Tiempo para la sincronización diaria "23:00:00" 11:00 PM

[Guardar información de sincronización](#)

System Updated Successfully

Luego puede intentar encontrar las cuentas de la base de datos, escribiendo una cadena de búsqueda con el nombre del usuario y presionando el botón "Obtener informe"

Buscar cuentas por nombre (en blanco para recuperar todas) Obtener Reporte

ID	Username	Domain	Retrievedate	Inter
1	pcruz	cordialio.net	2023-01-22 20:55:18	

## 12. EDICIÓN PARA USUARIOS FINALES

En esta sección puede encontrar y editar los registros de los usuarios finales, para proporcionar o actualizar algunos datos relativos a ellos. Vaya a "LDAP / USUARIOS FINALES". Luego escriba una cadena de búsqueda con el nombre del usuario y presione el botón "Obtener Reporte"

**CALL2UNLOCK** Enterprise

SISTEMA LDAP SIP RADIUS MFA REPORTES

ASISTENTE DE CONFIGURACION LDAP

CONFIGURACION

SINCRONIZACION DE CUENTAS

**USUARIOS FINALES**

**LISTA DE USUARIOS FINALES Y EDICIÓN**

Lista de todos los usuarios recuperados del AD. Haga clic en 'Edit' en la fila del usuario que desea actualizar o modificar.

Buscar cuentas por nombre (en blanco para recuperar todas) Obtener Reporte

Se mostrará una cuadrícula con los resultados de la consulta. Puede ordenar la lista por cualquiera de las columnas, configurar la paginación (por defecto 10) y exportar todos los registros a un archivo csv, que se puede abrir en unExcel d más tarde.

User Accounts				
ID		Username	Domain	Retrieve date
1	Edit	rcruz	cordialo.net	2023-01-22 20:55:18
2	Edit	root2	cordialo.net	2023-01-22 20:55:18
3	Edit	root3	cordialo.net	2023-01-22 20:55:18
4	Edit	root4	cordialo.net	2023-01-22 20:55:18
5	Edit	root5	cordialo.net	2023-01-22 20:55:18
6	Edit	root6	cordialo.net	2023-01-22 20:55:18
7	Edit	root7	cordialo.net	2023-01-22 20:55:18
8	Edit	root8	cordialo.net	2023-01-22 20:55:18
9	Edit	root9	cordialo.net	2023-01-22 20:55:18
10	Edit	root11	cordialo.net	2023-01-22 20:55:18

Siempre puede editar la cuenta de usuario, presionando "Editar" con el enlace en la primera columna de cada fila de cuenta de usuario.

Una vez que haga clic en el enlace Editar, podrá editar la información del usuario

#### EDICIÓN DE CUENTA DE USUARIO

Cuenta de usuario:	root4	Email Secundario:	
PN de 4 dígitos (solo números):	3129	Nombre de dominio (solo lectura):	cordialo.net
Teléfono interno permitido:		Teléfono externo permitido:	
¿Cuenta en lista negra?: <input type="checkbox"/>			
			Submit

Después de enviar el formulario, recibirá el mensaje "Cambios aplicados para el usuario"

Los usuarios finales también pueden editar esta información a través del sitio de auto-enrollment:

<http://ipaddress/userlogin.php>

La información proporcionada a los usuarios es:

Call2Unlock V 4.0 Manual de Administración

- Correo electrónico secundario
- PIN de 4 dígitos (Aplicar en caso de que el PIN esté configurado para almacenarse en la base de datos call2unlock). Consulte Configuración de LDAP.
- Teléfono interno permitido: extensión interna desde donde el usuario puede usar el sistema
- Teléfono externo permitido: External CallerID number, desde donde el usuario puede utilizar el sistema
- **Cuenta en lista negra: Esto se verificará en caso de que el usuario haya fallado el número máximo de intentos proporcionando el número PIN. Desmarcando esto, el usuario será liberado de la lista negra y estará listo para usar nuevamente el sistema.**

**Importante:** El sistema no permite más de un usuario con el mismo teléfono externo permitido.

Los teléfonos externos también deben incluirse en la lista blanca

### 13. RADIUS – CONFIGURACIÓN MFA.

Esta característica permite al sistema hacer uso de una fuente externa de autenticación como un servidor RADIUS externo, o la implementación local de RADIUS y Google Authenticator.

La configuración de esta función es una muy buena práctica en términos de seguridad, porque la información de "desafío" solicitada al usuario final no es algo fijo (como un número PIN creado por el usuario o proporcionado por el administrador), es en la mayoría de los casos un número PINber + un número de token que cambia cada segundo. Este token está asociado a la cuenta del usuario.

Vaya a la opción de menú "RADIUS MFA / CONFIGURATION"

Propiedad	Valor	Descripción
Ubicación del servidor Radius	0. Local (localhost) ▾	Indique si su servidor Radius será local (en este servidor Call2unlock) o cualquier otro servidor en su infraestructura existente
Nombre del servidor o IP	localhost	Si el servidor es Local o (localhost), una vez guardados estos cambios, presione el botón 'Start-Restart Radius'
Puerto de Radius	18120	Puerto predeterminado 18120. Actualice este valor de acuerdo con la configuración de su servidor Radius
Password del cliente Radius	testing123	Coloque este password en su configuración de radio para este cliente (IP del servidor Call2unlock), si está utilizando un servidor externo

Gaurdar

A continuación, provea la siguiente información:

**Ubicación RADIUS:** Tenemos que seleccionar si el servidor RADIUS es un servidor RADIUS existente (Opción 1), o vamos a configurar el RADIUS local (Opción 0), integrado a Google Authenticator.

**Nombre del servidor o IP:** Dirección IP del servidor RADIUS, (localhost si es el local).

**Puerto Radius:** Indique el puerto que el servidor RADIUS especificado está escuchando.

**Radius Client Secret:** Tenemos que proporcionar el "secret" creado para la dirección IP del servidor Call2unlock, ubicado en la configuración del cliente RADIUS,

Una vez que haya terminado de proporcionar esta información, presione el botón "Guardar cambios"

El siguiente paso será iniciar el servicio RADIUS (en el caso del RADIUS local). Iniciará el servicio y se **asegurará de que ntp también se esté ejecutando**. Esto es importante porque cualquier sistema basado en token es sensible al tiempo. Tienes que pulsar "Iniciar/Reiniciar Radius Local" y "Prueba de Conectividad". Si todo funciona bien, tenemos que obtener los mensajes "OK - Running" y "OK - Connected" como resultado.

Paso 2. GUARDE LOS CAMBIOS DEL PASO ANTERIOR. Si ha elegido Local como ubicación de su servidor Radius, inicie o reinicie el servidor Radius local. Si se ejecuta correctamente, podrá continuar con el paso 3.

Iniciar/Reiniciar Radius Local	Resultado OK - Running
--------------------------------	---------------------------

Paso 3. Probemos la conectividad entre Call2Unlock y el servidor Radius.

Prueba de conectividad	Resultado OK - Connected
------------------------	-----------------------------

El siguiente paso será probar la autenticación de una cuenta utilizando el servidor RADIUS. Esta prueba es válida para el RADIUS local con Google Auth. Y el RADIUS externo.

Luego abra una sesión ssh, y ejecute los comandos listados en el Paso 4.

Paso 4. Probemos la autenticación usando una cuenta de prueba y un PIN + Token válido, proporcionado por la plataforma MFA, como Google Authenticator

Primero, inscriba a un usuario de prueba en Google Authenticator. Inicie sesión en la consola como root y ejecute los siguientes comandos:

```
[root@myserver ~]# adduser test1 (Puede usar cualquier nombre de usuario, evite usar un nombre de usuario que ya exista en su AD)
[root@myserver ~]# passwd test1 ( Cree un número pin de 4 dígitos, ejemplo 5566)
[root@myserver ~]# cd /home/test1
[root@myserver ~]# su test1
[test1@myserver ~]$ google-authenticator
```

Siga las instrucciones y una vez que se muestre el código QR, agregue una nueva cuenta en su aplicación Google Auth en su teléfono. Escanee el código QR y ya tienes lista la cuenta de prueba.

Finalmente la consola SSH le mostrara el código QR para auto añadirla a Google Authenticator APP. Proporcionando el nombre de usuario creado en el paso anterior, el PIN (password) + Google Authenticator Token, tiene para obtener el mensaje "OK Authenticated"

Nombre de usuario para la prueba	test1
PIN+Token	
Prueba de Autenticación	Resultado OK - Authenticated

## 14. PORTAL DE USUARIO FINAL: INTERFAZ DE INSCRIPCIÓN DE GOOGLE AUTHENTICATOR

Este es el sitio web donde los usuarios finales configurarán su dirección de correo electrónico secundaria, el número PIN de 4 dígitos, y también inscribirán su cuenta de Google Authenticator, si el RADIUS-MFA ha sido seleccionado como información de desafío para proporcionar. Esta información será utilizada por call2unlock en el momento del restablecimiento de la contraseña.

Debe indicarle a los usuarios la URL, para iniciar sesión en <https://ipaddress/userlogin.php>

Se trata de una autenticación LDAP contra el servidor de AD, por lo que los usuarios deben recuperarse primero en call2unlock y la cuenta debe estar desbloqueada, para que el usuario pueda iniciar sesión.

Debe proporcionar un código PIN y un correo electrónico secundario al usuario. Una vez guardado, vuelva a la Lista de cuentas de usuario

Cuenta de usuario	
Domnio (solo lectura)	ext cordialtel
Email secundario:	<input type="text"/>
PIN de 4 dígitos (solo números)	
Teléfono externo permitido:	<input type="text"/>

<https://chart.googleapis.com/chart?chs=200x200&chld=M:0&cht=qr&chl=otpauth://totp/tel@rescate.cordiale.net?secret=3DK4I7AC5Z4J7I>



**Generar-regenerar cuenta de Google Authenticator**

Si no ve el código QR después de presionar este botón, copie y pegue la URL en su navegador. Si puede visualizar el código QR, escanéelo con su aplicación Google Auth.

La información proporcionada a los usuarios es:

- Correo electrónico secundario
- Teléfono interno permitido: Extensión interna desde donde el usuario puede usar el sistema. En caso de que se marque "Todas las llamadas internas" en la configuración SIP, esta entrada no se disipará.
- Teléfono externo permitido: Número de teléfono personal, desde donde el usuario puede utilizar el sistema. En caso de que el prefijo externo en la configuración SIP esté vacío, no se permiten llamadas externas, esta entrada no se mostrará.
- PIN de 4 dígitos. En caso de que tengamos habilitado RADIUS local, este número PIN será la contraseña creada en el entorno local para RADIUS.

**Una vez que el usuario presione el botón "Generar-Regenerar cuenta de Google Auth.", el sistema procederá a solicitar un código QR de Google Auth. Por lo tanto, el usuario solo necesita agregar la nueva cuenta en la aplicación Google Auth. Mobile y escanear el código QR para que la cuenta y los tokens funcionen.**

**Importante:** El sistema no permite más de un usuario con el mismo teléfono externo permitido.

**Losteléfonos externos también deben incluirse en la lista blanca (consulte la sección Configuración SIP), o es necesario que el usuario final notifique al administrador sobre los cambios en el teléfono externo.**

## 15. AUTOSERVICIO WEB PARA USUARIOS FINALES

Dado que call2unlock ahora admite la integración de RADIUS y Google Auth., ahora proporciona un autoservicio web a los usuarios finales, como alternativa al IVR o al sistema de integración telefónica. Los usuarios deben dirigirse a esta URL:

<https://ipaddress:4443>

Nótese que esta opción utiliza un Puerto diferente (4443) al resto de la aplicación, en caso que su institución requiera acceder a esta opción desde internet. Así en las reglas NAT de acceso de su Firewall especificando acceso a solo este Puerto se evita exponer las herramientas de configuración.



The screenshot shows a web interface titled "CALL2UNLOCK WEB SELF SERVICE". It contains three input fields: "Username" with a circular icon to its right, "Pin + Token (MFA):" with a circular icon to its right, and "Language/Idioma:" with a dropdown menu showing "English". Below these fields is a "Login" button.

Como puede apreciar, esta web requiere la autenticación contra RADIUS (PIN + Token). Una vez autenticado correctamente, el usuario podrá desbloquear o restablecer la cuenta utilizando la siguiente interfaz:



The screenshot displays the 'PORTAL DE AUTO SERVICIO - MFA' interface. It features two main sections: 'Desbloquea tu cuenta' (Unlock your account) and 'Establece tu nueva contraseña' (Set your new password). The 'Desbloquea tu cuenta' section includes a 'Desbloquear cuenta' button and a 'Success' message. The 'Establece tu nueva contraseña' section includes a 'Cuenta de usuario' field with the value 'luis', two password input fields labeled 'Establece la nueva contraseña' and 'Repita la contraseña', a 'Cambiar' button, and a 'Success Temp Pass: [redacted]' message.

El usuario tendrá las 2 opciones, Desbloquear y Restablecer.

En caso de restablecimiento, la nueva contraseña se proporcionará y actualizará en Active Directory.

Cada acción realizada por el usuario final en la herramienta de autoservicio web se registrará en los reportes explicados en el siguiente capítulo.

## 16. REPORTES

Un registro de llamadas detallado está disponible, donde debería poder ver cuántas cuentas se han desbloqueado o reseteado, qué cuentas y la hora exacta.

Vaya a "REPORTES/REPORTES DE SERVICIO CDRS". Una vez en la sección Informes, elija una fecha de inicio y una fecha de fin, y presione "Mostrar registros"

**REPORTES DE SERVICIO CDR**

Fecha de inicio: 01/24/2023 Fecha de Fin: 01/24/2023

Mostrar Registros

ID	Uniqid	CallerID	CallerID	CallDate	User	Domain	Action	Result
1		WEB	SELF_SERVICE	2023-01-24 13:45:10	test1		MFA_web_login	SUCCESS
2		WEB	SELF_SERVICE	2023-01-24 13:48:28	test1		MFA_web_login	SUCCESS
3		WEB	SELF_SERVICE	2023-01-24 13:50:00	test1		MFA_web_login	SUCCESS
4		WEB	SELF_SERVICE	2023-01-24 14:05:52	test1	ext.cordialia.net	unlock	SUCCESS
5		WEB	SELF_SERVICE	2023-01-24 14:06:29	test1	ext.cordialia.net	reset	SUCCESS
6	1674587569.0		9999	2023-01-24 14:12:56	Not Found		unlock	NO USER
7	1674588421.2		9999	2023-01-24 14:27:03	Not Found		unlock	NO USER
8	1674588937.4		9999	2023-01-24 14:35:43	Not Found		unlock	NO USER
9	1674589060.8		9999	2023-01-24 14:38:24	test1	ext.cordialia.net	unlock	SUCCESS

Exportar a CSV Page 1 of 1 10 View 1 of 9

Como puede ver en la imagen de arriba, la cuadrícula muestra el número de registros. También puede descargar la cuadrícula a una hoja de cálculo haciendo clic en "Exportar a csv". También puede cambiar el número de registros que la cuadrícula puede mostrar en el combo de selección junto al número de páginas.

## 17. LICENCIAS

La información de licencias debe cargarse en este módulo. Vaya a la opción de menú "Licencia" y complete la siguiente información

**Clave de licencia:** El número de clave proporcionado por Call2Unlock. Este número se genera de acuerdo con su nombre de dominio y el número de usuarios de su Active Directory. (Las cuentas debajo de la unidad organizativa raíz que ha configurado en la configuración LDAP).

**Número máximo de usuarios:** Debe seleccionar un intervalo del combo que corresponde al número de usuarios de su directorio activo.

**Nombre de dominio:** El nombre de su dominio. La licencia será válida solo para su servidor AD.

## LICENCIA

Cargue o reemplace la licencia solicitada, llenando el texto con la clave provista por Call2Unlock

Lea la documentación para aprender cómo generar un certificado [\(Aprenda aquí\)](#)

Propiedad	Valor	Descripción
Clave de licencia	2094000044536	Clave de licencia proporcionada por Call2Unlock
Número máximo de usuarios	1,000 - 5,000	Rango del Número de usuarios en su Active Directory
Nombre de dominio	mydomain.com	Nombre de dominio

Una vez aplicada la licencia, reinicie el servidor call2unlock desde el sistema operativo ejecutando "**sudo shutdown -r now**"

## 18. PROBANDO EL SERVICIO

Para probar y comenzar a usar Call2unlock, realizaremos 2 pruebas básicas.

### Prueba 1.

**Validaremos si Call2Ulock funciona correctamente independientemente del sip trunk a su PBX**

1. Descargue un Softphone gratuito (como Xlite, puede descargarlo desde <http://www.counterpath.com/x-lite-download/>)
2. Configure la siguiente extensión en el softphone.  
No importa qué softphone esté utilizando, los parámetros más importantes son:  
Extensión: 9999    CallerID 0016960  
Contraseña: 123456  
Dominio : Call2Unlock dirección IP

El siguiente ejemplo, es una configuración para xlite

Account	Voicemail	Topology	Presence	Storage	Security	Advanced
<b>User Details</b>						
Display Name	9999					
User name	9999					
Password	•••••					
Authorization user name	9999					
Domain	Call2Unlock IP Address					
<b>Domain Proxy</b>						
<input checked="" type="checkbox"/> Register with domain and receive incoming calls						
Send outbound via:						
<input type="radio"/> domain <input type="radio"/> proxy Address <input type="text"/> <input checked="" type="radio"/> target domain						

3. Marque 8888 y siga las instrucciones para desbloquear y/o restablecer cualquier cuenta en su directorio activo.
4. Es una buena idea abrir una consola de asterisk para ver los registros en tiempo real.

**"asterisk -rvvv"**

*Call2Unlock\*CLI>*

## Prueba 2.

**Validaremos si su PBX está enviando correctamente las llamadas a Call2Unlock. Por lo tanto, validaremos si el IVR Call2Unlock está disponible desde las extensiones de su teléfono.**

1. Marque las extensiones configuradas en su PBX que envían la llamada a Call2 Unlock, desde cualquier extensión en su PBX y siga las instrucciones para desbloquear y / o restablecer cualquier cuenta en su directorio activo
  - Una vez más, es una buena idea abrir una consola de asterisk para ver los registros en tiempo real.

**"asterisk -rvvv"**

*Call2Unlock\*CLI>*

2. Disfrute de su nuevo Servicio 😊