How to secure the server and prevent/limit frauds?

This example is written for the **Canistracci OIL** tenant. Create the objects with a **Docs Demo** prefix, test them on non-production numbers, and then adapt the same structure for the production tenant.

It is not a question with a simple answer. You'll be hacked. Sooner or later you'll be hacked and you'll loose some money. That must be taken into account. However you can work in making it happen as late as possible and to lose the least money as possible. I am continuously working in making the platform as secure as possible and giving you the tools to minimize the problems connected with an hack.

How you'll be hacked

You can be hacked in several ways:

- Remote phone hacking. In this case, the hacker gains access to a remote phone and steal the credentials. Unfortunately most phone web interfaces are completely insecure and they should never be reachable from Internet. Some contains hard coded credentials, others allows easy configuration download. Even if not reachable from Internet, an hacker can use a compromised PC inside the LAN to access phones (usually with default credentials) and then transmit out the credentials collected.

- Password guessing. Even if almost impossible using the predefined 16 char random passwords, it is important to not assign dictionary passwords to phone or web interface accounts

- Web interface weakness. It happened an unchecked input allows a very slow but effective way for an unauthenticated user to recover the passwords from the database. This problem has been fixed, but it is not possible to be sure at 100% about any other problems connected to the code or libraries used.

How you can make it harder

- You can restrict the network addresses a client can use by listing them in Configuration/Settings. In the same place you can also put some restrictions about the usage time, so after certain time, no outbound calls can be made from a phone
- If a client has no need for international calls, don't authorize them. You can setup two different class of routing profiles, allowing international calls only for the clients really needed them
- Use GeoIP filtering. If you have all "local" clients, you can list the countries allowed to connect to the PBX.
- Use Fail2ban. Even if brute forcing a password seems quite impossible, the current network speed can lead to unexpected success.
- Filter SIP scanner. If they don't know you are a PBX, they will not try to hack you.
- Filter SIP useragent. You can set a filter so if a different user agent is used for the extension, even if the password is correct, the extension is locked.

How you can minimize the cost of an hacking

- Set limits on your provider. Nowadays every provider allows you to define a max daily spending amount.
- Set daily limits for extension and tenant in Admin/Security/Call Limits. That will be the max amount of money you are ready to lose in case of an hacking. Unfortunately it seems there is a method to fool asterisk in believing the call has been terminated while it continues on the provider side. This kind of trick was seen in two cases, but no further analysis was possible, so it is not confirmed working in the current version.
- Set cost limit for destination. I have never found a client needing to call an Inmarsat phone or some erotic line in Palestine. Set a limit on how much an allowed destination can cost in Admin/Security/Call Limits. You'll automatically black list all destinations used when an hack is performed.

What else can go wrong?

- Your SIP trunk provider credentials can be stolen, so call will be placed directly bypassing your PBX and any limit you can have setup. In this case, it is always better to apply limits

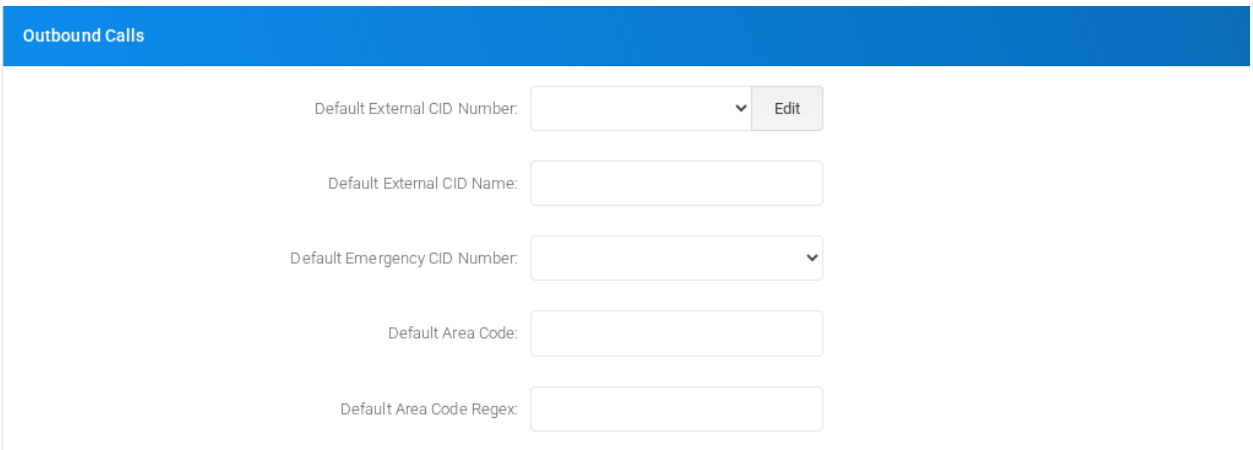
also on your provider account. Most of them allow you to setup an upper daily usage limit

- Your datacenter can lose your server. Your nightmare has became true. Your server is no more accessible and your datacenter is informing you that due to an hardware failure/human mistake your server is no more (but don't worry, they will refund your last month invoice). Don't smile... it happened to me when I ask to move to another hardware because the one they rented me was defective. After a couple of days they admit they have lost my hard disk during the move. Doing backup and storing them in a different location is the only way to survive such disaster due not only to the described case, but any case where the server became unavailable. For best protection against any volunteer nasty action, store a copy of your backup (once a week can be fine) in an offline device, like an USB disk.

- Your datacenter can be hit by a DDOS or suffer any other network problem. Your server is alive, your data are intact, but your clients are down because your datacenter network speed is like an old DSL line. You can't even move out your data to a new datacenter because the speed is not enough. This can be due to a DDOS or a physical sabotage. A secondary server in another datacenter can save your life.

- Your datacenter connectivity is perfect, your SIP provider connectivity is perfect. All this when tested from your office. Unfortunately when your PBX tries to communicate with your SIP provider, you have 10% packet loss and each one is blaming the other. Having all PBX servers in the same datacenter and using only one SIP provider can be a risky business.

- Your datacenter can burn to the ground and even if your servers were stored in different building, they are all lost. Even if you decide to operate your business from one very good datacenter, it can be a nice idea to leave one server in a separate datacenter, even if it is not really serving customers, but just as last resort backup. https://www.searchenginejournal.com/ovh-data-center-fire-darkens-thousands-of-sites-worldwide/398485/



Canistracci OIL example screen for How to secure the server and prevent/limit frauds?.

Validation

- Confirm the tenant selected in the top bar is Canistracci OIL before creating the example.
- Verify the created objects appear in the expected Configuration menu page.
- Place a controlled test call or run the related status check.
- Remove or disable temporary test numbers when the example is no longer needed.

Revision #5
Created 2026-06-02 22:01:12 UTC by Admin
Updated 2026-06-02 22:13:58 UTC by Admin