

# How to prevent frauds using SIP devices against VoipNow

A common fraud scenario implies that a large number of calls to expensive destinations have been placed using your VoipNow system within a short amount of time. This can be done either by the legitimate user of a SIP extension or by a cracker who registers their own device to the extension.

## Step-by-step guide

There are several protective measures that you can take to prevent attempts of fraud:

### Update your system regularly

Ensure that VoipNow and the operating system are up-to-date.

### Use credit limits

To prevent accounts from exceeding a certain amount of credit, you need to set specific credit limits in your charging plan. This should be done even if you're not a service provider and you're not using Billing to charge your clients.

You need to always use money limits on extensions. When the fraud is attempted by the extension owner, it may be one of the few measures that can prevent it. Also, it's important that you do not rely on concurrent call limits to protect your system.

### Create strong SIP passwords

It's better to let the system automatically generate passwords.

### Restrict access

- Whenever possible, allow extensions to register only from specific IPs.
- Never expose hardware phones directly to the Internet and do not use default credentials for their web interfaces. Also, keep their firmware up-to-date.

### Restrict traffic

- Use iptables firewall rules to restrict traffic. More info can be found [here](#). You can also further restrict SIP access to certain IP addresses (providers and customer locations).
- Use fail2ban to block IPs that fail to register many times. For setup recommendations, please see this [article](#)
- Use [Pike](#) to detect abnormal traffic

### Restrict calls

- Restrict international calls using routing rules and/or your charging plan.
- Restrict calls outside business hours.
- Monitor call patterns and set up thresholds to alert you in case of unusual activities (high numbers of call attempts per hour, for example).

### Keep an eye on your extensions

- Monitor the number of newly created extensions/users.
- Check the permissions of VoipNow entities (creating new extensions, etc). You should never give accounts the possibility to create unlimited accounts, make unlimited calls etc. This can be controlled from the "Roles and phone numbers" section of each account.
- Do not use 1111 or 1234 as voicemail passwords (or other very common ones).
- Remove unused or unnecessary extensions as soon as possible.
- Do not leave test extensions in place.

## Related articles

- [How to prevent frauds using SIP devices against VoipNow](#)
- [The provisioning process in VoipNow](#)
- [Understanding SIP devices provisioning permissions](#)
- [How to block specific countries from accessing your server](#)
- [How to force MWI notifications for phones that do not subscribe to the service](#)