

Advanced

Access Controls

Access control list can allow or deny ranges of IP addresses. There are several purposes for using the ACL.

providers - access control list

- The main purpose of the Providers list is for your voip provider (carrier) IP addresses to the CIDR.
- Be careful with what and how you use ACL.
- Most common mistakes result in calls not working between extensions and other undesirable results.
- Be sure to keep **providers** access control (formerly called domains) to default deny.
- Do not put your public ip or phone IP addresses in the domains access control list.
- Don't supply both the domain and the cidr on the same node.
- If adding a single IP address to the CIDR field make sure to add /32 on the end of the IP address.

Access Control Example

Goto Advanced > Access Controls. Click the edit icon for **providers** was renamed from **domains**. At the bottom under **nodes** click the plus icon. In the example below make sure to change the 12.34.56.0 to your VoIP providers IP address if adding to the Providers access control list.

Type choose allow
CIDR enter the 12.34.56.0/32
Domain (Leave Blank, used for advanced scenarios)
Description (Carrier Name)

Click save

Goto > Status > Sip Status and click **reloadacl**.

Under Status > log viewer you should notice the ip added. This can be seen also from command line fs_cli by using **reloadacl**

```
[NOTICE] switch_utils.c:545 Adding 12.34.56.0/32 (allow) [] to list domains
```

Unieke FAQ ID: #4047

Auteur: Helpdesk

Laatst bijgewerkt: 2022-11-28 10:08