

# FAQ T640 T440 Unban IP Address from Fail2Ban [IPtables]

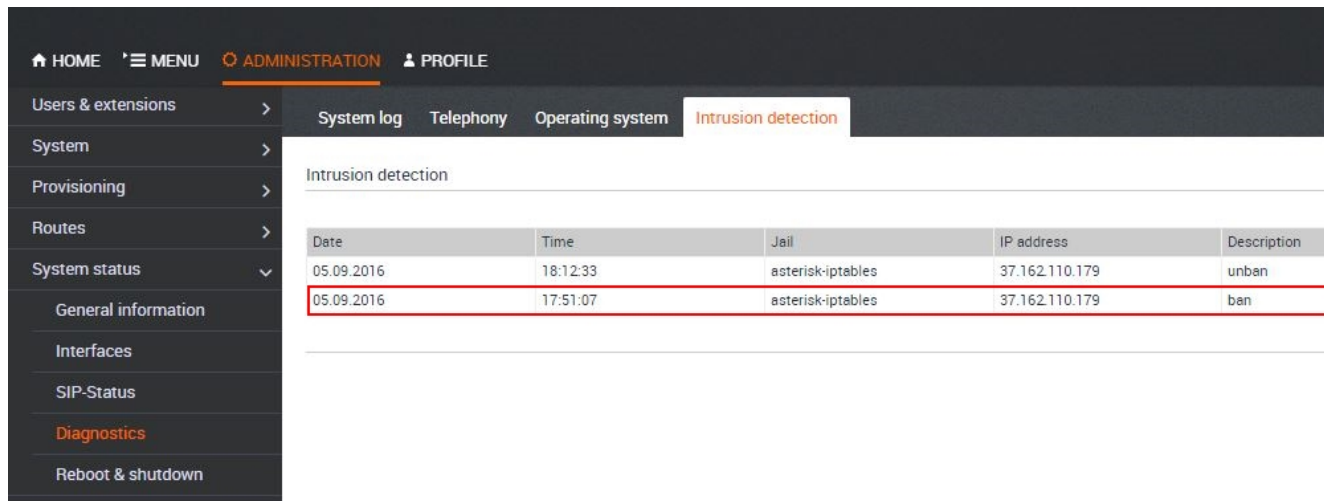
## Introduction

By default, the PBX will put the IP address of the device on the Blacklist when 4 wrong attempts are made within 6 hours. They are then blocked for 24 hours.

Here is explained how to remove an IP address from the Blacklist when auto-banned by Fail2Ban.

## Open Tx40 web-interface

- In the web-interface of the T640/T440 go to: **Administration - System status - Diagnostics - Intrusion detection**



The screenshot shows the web interface of the Tx40 device. The left sidebar contains a menu with options: HOME, MENU, ADMINISTRATION (selected), and PROFILE. Under ADMINISTRATION, there are sub-menus: Users & extensions, System, Provisioning, Routes, System status (expanded), General information, Interfaces, SIP-Status, Diagnostics (selected), and Reboot & shutdown. The main content area shows the 'Intrusion detection' tab selected. Below the tab is a table with the following data:

Date	Time	Jail	IP address	Description
05.09.2016	18:12:33	asterisk-iptables	37.162.110.179	unban
05.09.2016	17:51:07	asterisk-iptables	37.162.110.179	ban

## Open SSH console

- Type : ***iptables -L -n***

```
root@galilei:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
fail2ban-ASTERISK all  --  0.0.0.0/0             0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target     prot opt source                destination
REJECT     all  --  37.162.110.179        0.0.0.0/0             reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0             0.0.0.0/0
```

Using this command you can find which IP address is banned and why. Note the IP address you want to unban.

- Type : ***fail2ban-client status***

```

root@galilei:~# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:          asterisk-iptables
root@galilei:~# fail2ban-client set asterisk-iptables unbanip 37.162.110.179
37.162.110.179

```

Now you know in which jail the IP Address is inserted and then unban it using : **fail2ban-client set [jail-name] unbanip [IP address]**

There is no more IP Address in jail.

```

root@galilei:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
fail2ban-ASTERISK all  --  0.0.0.0/0             0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target     prot opt source                destination
RETURN     all  --  0.0.0.0/0             0.0.0.0/0
root@galilei:~#

```

We can see it in Web interface.

[HOME](#)
[MENU](#)
[ADMINISTRATION](#)
[PROFILE](#)

Users & extensions >
System >
Provisioning >
Routes >
System status v

General information
Interfaces
SIP-Status
Diagnostics
Reboot & shutdown

System log
Telephony
Operating system
Intrusion detection

Intrusion detection

Date	Time	Jail	IP address	Description
05.09.2016	18:12:33	asterisk-iptables	37.162.110.179	unban
05.09.2016	17:51:07	asterisk-iptables	37.162.110.179	ban

## How to change the 4 attempts to higher value.

- Open SSH console.
- edit the asterisk.conf file "nano /etc/fail2ban/jail.d/asterisk.conf"

#### **asterisk.con**

```
[asterisk-iptables]
enabled = true
backend = auto
filter = asterisk
action = iptables-allports[name=ASTERISK, protocol=all]
logpath = /var/log/voip.log
# if more than 4 attempts are made within 6 hours, ban for 24 hours
maxretry = 4
findtime = 21600
bantime = 86400
```

- Change the maxretry to other value. The higher the value, the more insecure it get's.

- [Introduction](#)
- [Open Tx40 web-interface](#)
- [Open SSH console](#)
- [How to change the 4 attempts to higher value.](#)