



## 1. Limiting trunk registrations

By implementing the following setting you can restrict SIP registrations solely to your PBX. This will prevent a breach if your SIP trunk authentication details are accessed by an unknown party and they try to register a SIP phone or PBX to your trunk.

The screenshot shows the Hostcomm web interface for managing extension Chris Key (0003\*001). The 'Tools' section contains various configuration options, with 'Provisioning and SIP' highlighted by a red circle. The 'Extension Overview' section shows the extension type as 'Phone terminal' and the phone terminal login as '0003\*001'.

The 'SIP Preferences' section includes the following settings:

- Provisioning template: Server default
- Phone time zone: GB-Belfast
- Use the same password with interface:
- Phone password: [Redacted] (at least 5 characters)
- Confirm phone password: [Redacted]
- DTMF: rfc2833
- A PBX is connected to this extension:  Enable for SIP trunking service
- Ping the extension to check its status:
- Allow re-invites from this extension:
- Extension publishes its own state:
- Force enable of MWI:
- Allowed codecs:  G.711 U-Law  G.711 A-Law  GSM
- Phone does not register, is located on IP: [Redacted] Port [Redacted] and [Redacted] has to [Redacted] authenticate
- Allow extension SIP connection only from IP: 88.123.345.56 (maximum class C (/24))
- Equipment description: [Redacted]

\* Required fields

Put the public IP address of your PBX / router / firewall in the box above. To identify your public IP address (NOT the one on the back of your router) search on Google using the search phrase “what is my public IP address”.

## 2. Strong Passwords

For SIP telephone registration Hostcomm recommends an alpha-numeric password with at least 9 digits. You can auto generate this type of password here:

<http://www.pctools.com/guides/password/>

The SIP trunk authentication details that are sent when you sign up include a 9 digit alpha-numeric password by default.

## 3. Firewall settings

Your firewall should be set to allow all traffic to and from specific IP addresses, for example:

- The Hostcomm gateway.
- The router addresses of your other offices.
- The home address of the administrator.

If you would like to tighten your firewall by more than just IP, you can limit it to the following ports to/from the Hostcomm gateway address:

UDP 5050 to 5070 for SIP

UDP 10000 to 20000 for the RTP streams

TCP 443 for HTTPS

## 4. Prepaid billing accounts

Limiting your liability in the event of a fraudulent breach of security can be achieved with a pre-pay billing account which is the default Hostcomm billing plan for SIP trunks, diallers and hosted telephony.

If your PBX is breached the maximum that can be spent is the remaining credit. This will be noticed by you quickly and any changes can be implemented before further fraudulent activity can continue.

## 5. Control panel Login encryption

Hostcomm's gateway servers (portals, control panels) have SSL encrypted logins. Please ensure that you login via an https: URL for example

**https://contact-pro6.co.uk**

This will ensure that your username and password cannot be viewed as you login.

## 6. Block ICMP (ping responses)

Hostcomm disables ICMP responses on all of its gateways. Some ICMP message types are however necessary for network administration. Unfortunately, hackers have found a way to turn a good network tool into an attack. The most common types of ICMP attacks are:

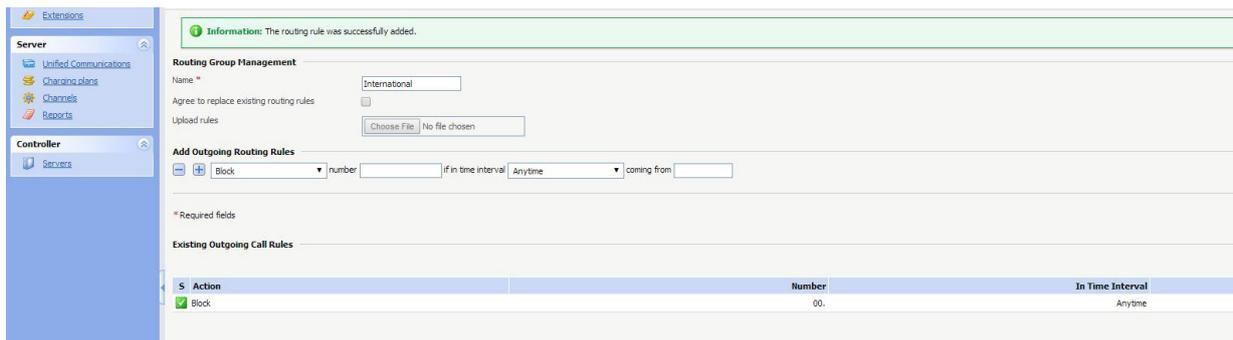
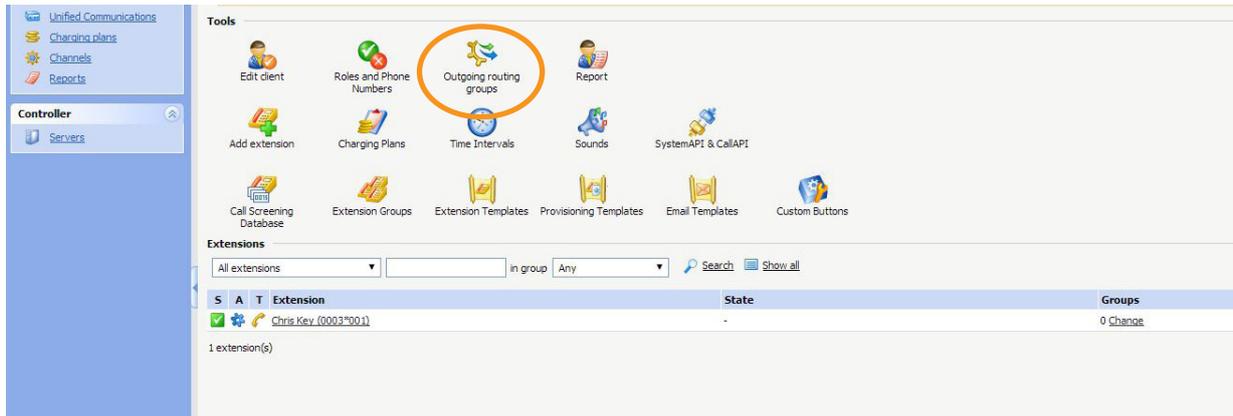
-  ICMP packet magnification (or ICMP Smurf): An attacker sends forged ICMP echo packets to vulnerable networks' broadcast addresses. All the systems on those networks send ICMP echo replies to the victim, consuming the target system's available bandwidth and creating a denial of service (DoS) to legitimate traffic.
-  Ping of death: An attacker sends an ICMP echo request packet that's larger than the maximum IP packet size. Since the received ICMP echo request packet is larger than the normal IP packet size, it's fragmented. The target can't reassemble the packets, so the OS crashes or reboots.
-  ICMP flood attack: A broadcast storm of pings overwhelms the target system so it can't respond to legitimate traffic.
-  ICMP nuke attack: Nukes send a packet of information that the target OS can't handle, which causes the system to crash.

## 7. Maximum registration attempts

Always limit the number of registration attempts on your PBX by IP address. Once the maximum has been reached, the IP address should be banned.

## 8. Disable International calling

If you don't make international calls disable them from your portal. You can do this by adding an outgoing call rule (00.) to block all calls beginning with 00 i.e. international calls. Please see below.



## 9. Disable ssh access using username / password authentication to your PBX

Linux servers typically allow ssh access on port 22. Ideally this type of access should be changed so that it requires a key exchange instead of username / password. Alternatively you can change the port number so something other than 22.

Unless necessary, don't expose port 22. Only allow ssh access to your PBX if you have to.

**TALK TO US... We are here to help.**

If you have any questions or require further information, please get in touch.

#### Contact us



**Phone**

0808 1684400  
0203 372 8420



**Sales enquiries**

[sales@hostcomm.co.uk](mailto:sales@hostcomm.co.uk)



**Fax**

01276 300 900



**Support enquiries**

[support@hostcomm.co.uk](mailto:support@hostcomm.co.uk)

#### Visit our website



[www.hostcomm.co.uk](http://www.hostcomm.co.uk)

#### Visit our offices

**Technical Support Office**

Edward House  
Unit A  
Grange Business Park  
Enderby Road  
Leicester  
Leicestershire  
LE8 6EP

**Head Office**

The Old Convent  
8 Broad street  
Ottery St Mary  
Exeter  
Devon  
EX11 1BZ

**Sales Office**

5 Barnfield Crescent  
Exeter  
EX1 1QT

**New York Office**

1133 Broadway  
New York  
NY 10010

#### Connect with us



[linkedin.com/company/hostcomm-ltd](https://www.linkedin.com/company/hostcomm-ltd)



[twitter.com/Hostcomm](https://twitter.com/Hostcomm)



[Google+](#)

**GET THE MOST  
FROM YOUR SERVICE**  
VISIT THE CUSTOMER PORTAL

[Go Now >](#)