IP Tel

Preventing Toll Fraud

BEST PRACTICES

As part of Vocus' ongoing commitment to the security of our platform, we have seen an increase in attempted 'toll fraud' style attacks on unprotected user accounts. We'd like to take this opportunity to recommend options to enforce a security standard across your accounts and prevent unauthorised or unwanted charges to your accounts.

Customer Network Security

Please ensure that your Handsets/PBX are not exposed to the internet.

If remote management to CPE is required, utilising firewall rules to only allow access in from specific IP Addresses is recommended.

Malicious scanners often target common SIP ports over the internet; e.g. 5060, 5061, 5062.

Ensure that your devices/firewall are configured to trust SIP messaging from your SBC domain / SBC IP Address only.

CommPilot Provisioning Best Practices

The following are best practices to limit the extent of fraudulent calls that can occur if one of your endpoint handsets or user logins were to be compromised.

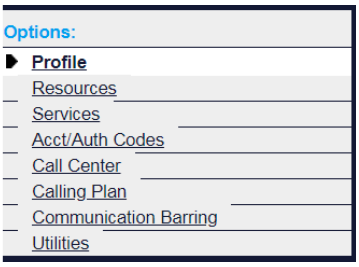
Call Processing Policy – Call Limits

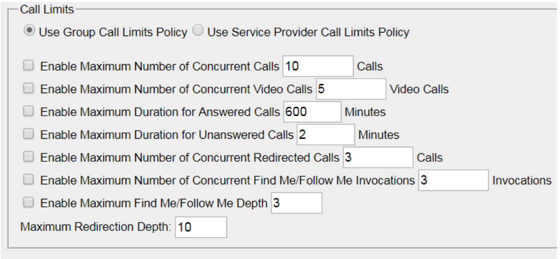
This option allows you to define the Call Limits on different calling scenarios. It can also be defined at different levels, such as Service Provider, Group and User levels under "Profile". Limits are applied on an individual user basis irrespective of being applied at Service Provider, Group or User level. Refer to the help option, located in the top tight corner within Commpilot, for further information on these options.

For example, if "Enable Maximum Number of Concurrent Calls = 10 Calls" is set on the group level, any given user in the group is only allowed to have a maximum of 10 concurrent calls. This might not be applicable for a Pilot User or Conferencing Bridge User in Broadsoft but is a good safety measure for a standard handset or SIP endpoint.

Limiting the "Maximum Number of Concurrent Redirected Calls" can be a useful setting to minimize the impact of toll fraud. These redirect calls are commonly used by hackers once login credentials have been breached. The concurrent redirected calls are not limited by Trunking Capacity in Trunk settings.

To set the limit, please tick the relevant box on each option and set a limit in the box.





Call Limits

● Use Group Call Limits Policy ○ Use Service Provider Call Limits Policy

□ Enable Maximum Number of Concurrent Calls 10 Calls

□ Enable Maximum Number of Concurrent Video Calls 5 Video Calls

□ Enable Maximum Duration for Answered Calls 600 Minutes

□ Enable Maximum Duration for Unanswered Calls 2 Minutes

□ Enable Maximum Number of Concurrent Redirected Calls 3 Calls

□ Enable Maximum Number of Concurrent Find Me/Follow Me Invocations 3 Invocations

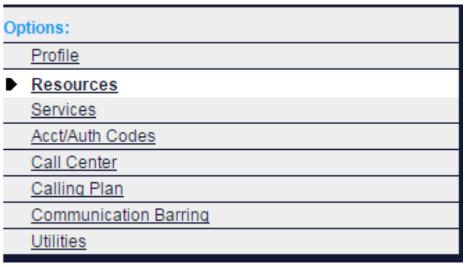
□ Enable Maximum Find Me/Follow Me Depth 3

Maximum Redirection Depth: 10

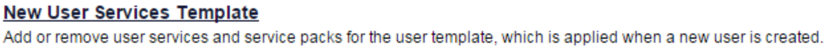
Service Templates

It is important to ensure that all users are created with a Service Pack, this will ensure a license is applied to each user and forces authentication for that SIP user. Lack of authentication is a big security risk and a major contributor towards Toll Fraud.

Service Templates allow a Service Pack or Service of your choosing to automatically be assigned to new users when they are created, forcing SIP users to use password authentication prior to being able to make calls. To do so, locate the Group where you would like to set up a Service Template, and browse to the 'Resources' section and select the 'New User Services Template' heading.



Options:
- Profile
- Resources
- Services
- Acct/Auth Codes
- Call Center
- Calling Plan
- Communication Barring
- Utilities



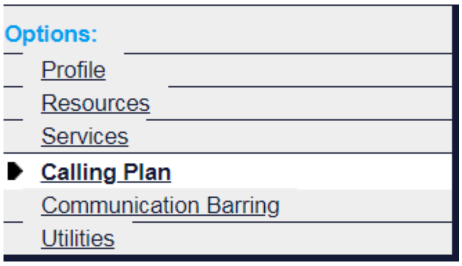
New User Services Template

Add or remove user services and service packs for the user template, which is applied when a new user is created.

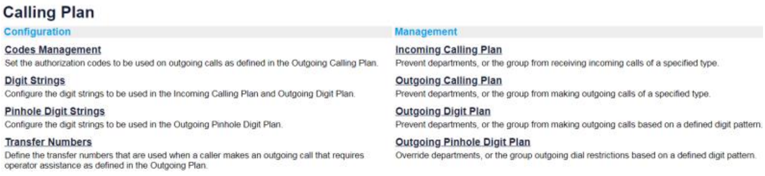
Choose the Service Pack you would like to have applied to all users automatically when they are created in Broadsoft.

Authorisation Code

Configuring this option will allow users to be prompted to enter an Authorisation Code (which can also be customised) after calling the number before an international call can be connected. Ensure that the 'Enhanced Outgoing Calling Plan' Group Service has been assigned to your Group first. Enhanced Group Services only comes with your Hosted PBX Premium Licenses or Collaboration License purchases. Enhanced Outgoing Calling Plan can be checked within Group Services under the 'Resources' and 'Services' headings at the Group level.



Options:
- Profile
- Resources
- Services
- Calling Plan
- Communication Barring
- Utilities



Calling Plan

Configuration

Codes Management
Set the authorization codes to be used on outgoing calls as defined in the Outgoing Calling Plan.

Digit Strings
Configure the digit strings to be used in the Incoming Calling Plan and Outgoing Digit Plan.

Pinhole Digit Strings
Configure the digit strings to be used in the Outgoing Pinhole Digit Plan.

Transfer Numbers
Define the transfer numbers that are used when a caller makes an outgoing call that requires operator assistance as defined in the Outgoing Plan.

Management

Incoming Calling Plan
Prevent departments, or the group from receiving incoming calls of a specified type.

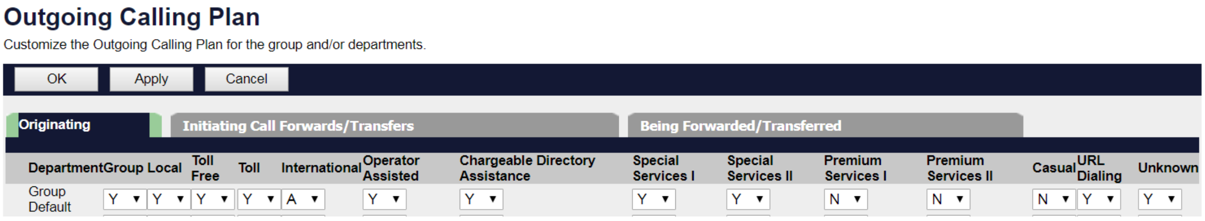
Outgoing Calling Plan
Prevent departments, or the group from making outgoing calls of a specified type.

Outgoing Digit Plan
Prevent departments, or the group from making outgoing calls based on a defined digit pattern.

Outgoing Pinhole Digit Plan
Override departments, or the group outgoing dial restrictions based on a defined digit pattern.

Once assigned, browse to the 'Calling Plan' heading at the Group level.

Enable the Auth Code for International calls under 'Outgoing Calling Plan' using 'A' in the drop-down.



Outgoing Calling Plan

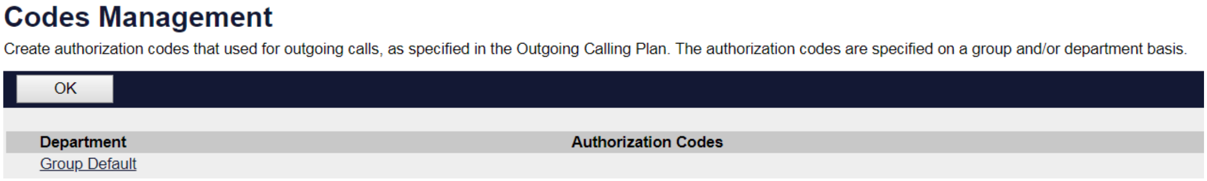
Customize the Outgoing Calling Plan for the group and/or departments.

OK
Apply
Cancel
Originating
Initiating Call Forwards/Transfers
Being Forwarded/Transferred

Department	Group	Local	Toll Free	Toll	International	Operator Assisted	Chargeable Directory Assistance	Special Services I	Special Services II	Premium Services I	Premium Services II	Casual	URL Dialing	Unknown
Group Default	Y ▼	Y ▼	Y ▼	Y ▼	A ▼	Y ▼	Y ▼	Y ▼	Y ▼	N ▼	N ▼	N ▼	Y ▼	Y ▼

Please note that such action needs to be done on both 'Originating' and 'Initiating Call Forwards/Transfers' tabs, the desired Auth Code can then be entered under "Codes Management" to finish the setup.

For flexibility, this option also allows different rules to be applied on the departmental level.



Codes Management

Create authorization codes that used for outgoing calls, as specified in the Outgoing Calling Plan. The authorization codes are specified on a group and/or department basis.

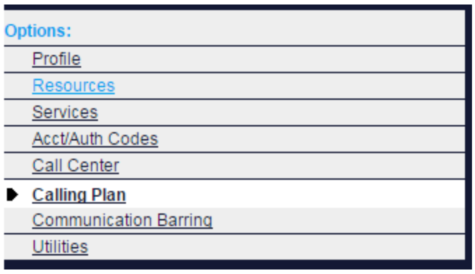
Department	Authorization Codes
Group Default	

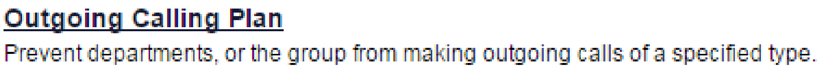
Calling Plans

International dialing can be disabled by default by creating an 'Outgoing Calling Plan'.

Ensure that the 'Outgoing Calling Plan' Group Service has been assigned to your Group first. Such group service is included with your SIP Line and Hosted PBX Standard licenses purchase. Outgoing Calling Plan Group Service can be checked under the 'Resources' and 'Services' headings at the Group level.

Once assigned, browse to the 'Calling Plan' heading at the Group level, and select 'Outgoing Calling Plan'. We suggest authorisation settings are completed on both 'Originating' and 'Initiating Call Forwards/Transfers' tabs under 'Outgoing Calling Plan'. Call Forwards and Transfers are a major source of Toll Fraud events and we should always disable the ability to forward calls to International destinations as a default setting. Exceptions to this rule can be made at the user level to minimise any exposure to potential fraud.

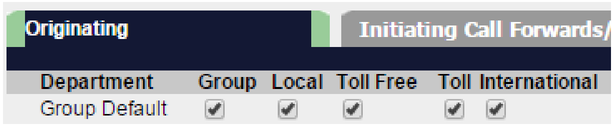




Outgoing Calling Plan

Prevent departments, or the group from making outgoing calls of a specified type.

Untick the box under 'International' to disable international calling for the group. Tick to enable.



Department	Group	Local	Toll Free	Toll	International
Group Default	☑	☑	☑	☑	☑

Important Provisioning Tips

- Most Toll Fraud events are related to unsecured SIP users or SIP trunks. Please ensure each user in the Broadsoft partition will have a minimum service pack assigned to ensure services are authenticated. Any SIP Trunk created will need to have "Enable Authentication" ticked with a strong authentication password (at least 12-16 characters combined with digits, lower case, upper case letters and special characters). The same standard needs to be applied to a standard SIP user Please note Users without a service pack assigned will not be protected by an authentication service and will be able to make outgoing calls without getting challenged by our SBC, this is a major security issue.

- A configured user can easily remain in the partition without any service pack assigned (and hence no authentication) when the Service Pack is reallocated between users. Please ensure a service pack is re-applied to such users or delete the user in question if the user is no longer required.

- Apart from the Authentication password, the web portal password is important too. If a user ID and web access password are compromised, a hacker can forward calls to fraudulent destinations via web services, such as 'Call Forwarding Always'. To avoid this situation set a strong password via User<Profile<Passwords<Set web access password.