Fraud Protection Configuration

End users' credentials are vulnerable to hackers. However, PortaBilling® offers protection to users with the help of fraud prevention tools. Fraud protection functionality is configured in three steps:

1. Fraud protection configuration in individual **products**, thereby allowing IP verification to be performed for all accounts using this product.
2. Configuration at the **customer** level using customer sites that can be assigned to certain accounts.
3. Configuration at the **account** level (optional).

Let's consider the following example: your customer's company is situated in Madrid, Spain. You would like to protect this customer from potential fraud. Since the company is situated in Spain and its employees mainly make calls from Madrid and other Spanish cities, you perform the fraud protection configuration so that calls made from Spain can be completed without restrictions. At the same time, calls made from other countries are considered suspicious and therefore, forbidden or screened.

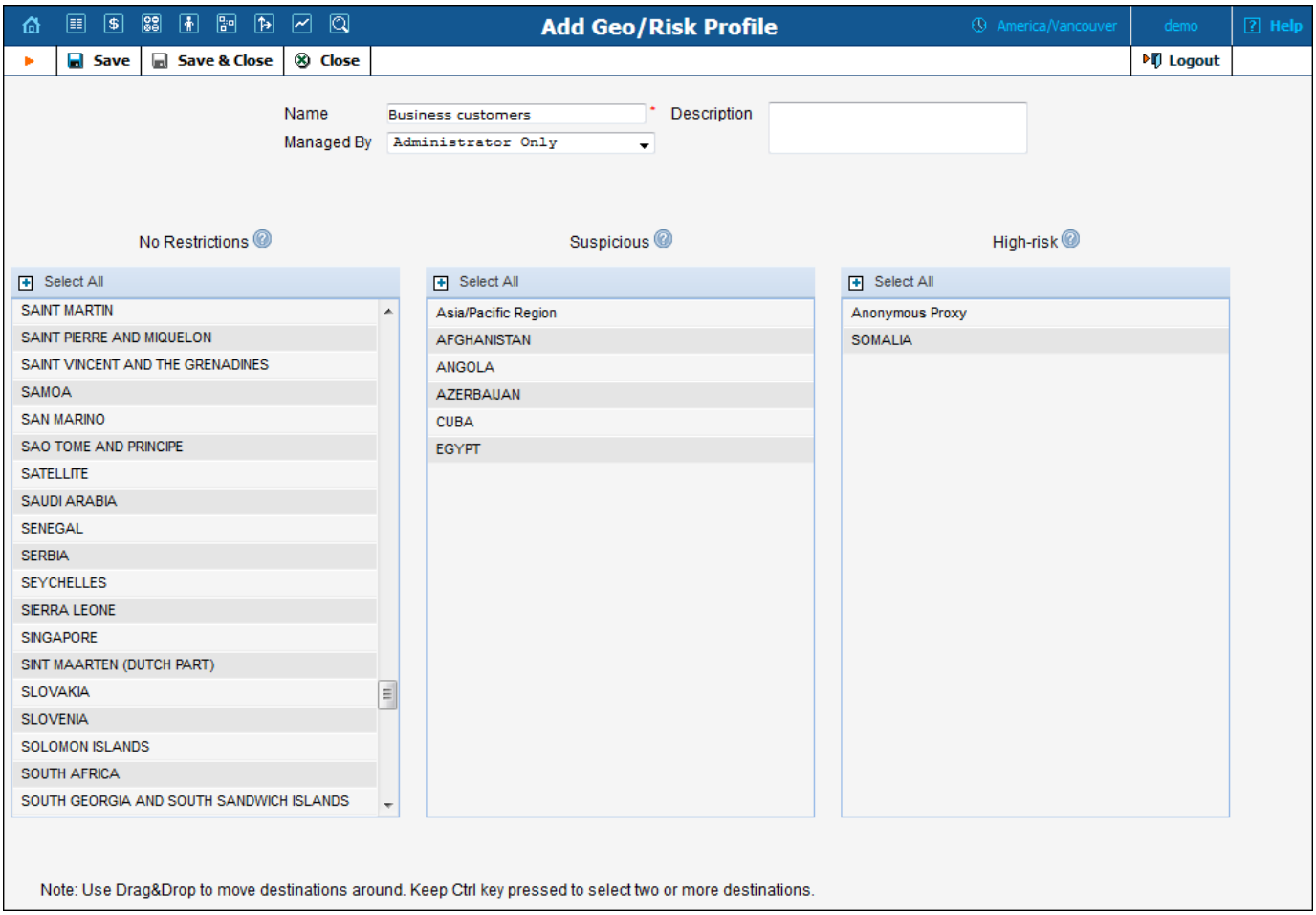
Checklist

Print this page and use it to check off the operations you have completed while performing the system setup according to the instructions in this chapter. Please be sure to perform all of the operations in the order designated (all of the boxes should be checked); otherwise the service will not work.

Operation	Done
Network configuration	
Create a Geo / Risk Profile.	[ ]
Rating configuration (Customer)	
Add the Geo / Risk Profile to a product.	[ ]
Perform the fraud protection configuration for a customer on the **Customer Sites** page.	[ ]
Account provisioning	
Check an account's fraud protection information and account's current status. Change the status if necessary.	[ ]
Perform the fraud protection configuration for an account (optional).	[ ]

Create Geo / Risk Profile

Create a Geo / Risk Profile so that calls made from Spain will not be restricted and calls made from other countries will be considered suspicious and therefore forbidden or screened.



1. In the **Networking** section of the PortaBilling main page, choose **Geo / Risk Profiles**.
2. On the **Geo / Risk Profiles** page, click the **Add** icon.
3. Fill in the Add Geo / Risk profile form:
   - **Name** – Type a Geo / Risk Profile name (e.g. business customers).
   - **Managed by** – Define whether this Geo / Risk profile will be used by an administrator or one of your resellers:
     - **Administrator Only** (default) means that this Geo / Risk profile will be applied to your direct customers, and is accessible only to your administrators.
     - **Select** a PortaBilling® reseller to assign this Geo / Risk profile for use by a particular reseller.
   - **Description** – Type a description of this Geo / Risk profile.
   - **No Restrictions** – All the countries are listed in this column by default.
   - **Suspicious** – Select countries from which a relatively low number of calls will be permitted without screening, and after which, the service will be screened.
   - **High-risk** – Select countries for which calls will be immediately screened.

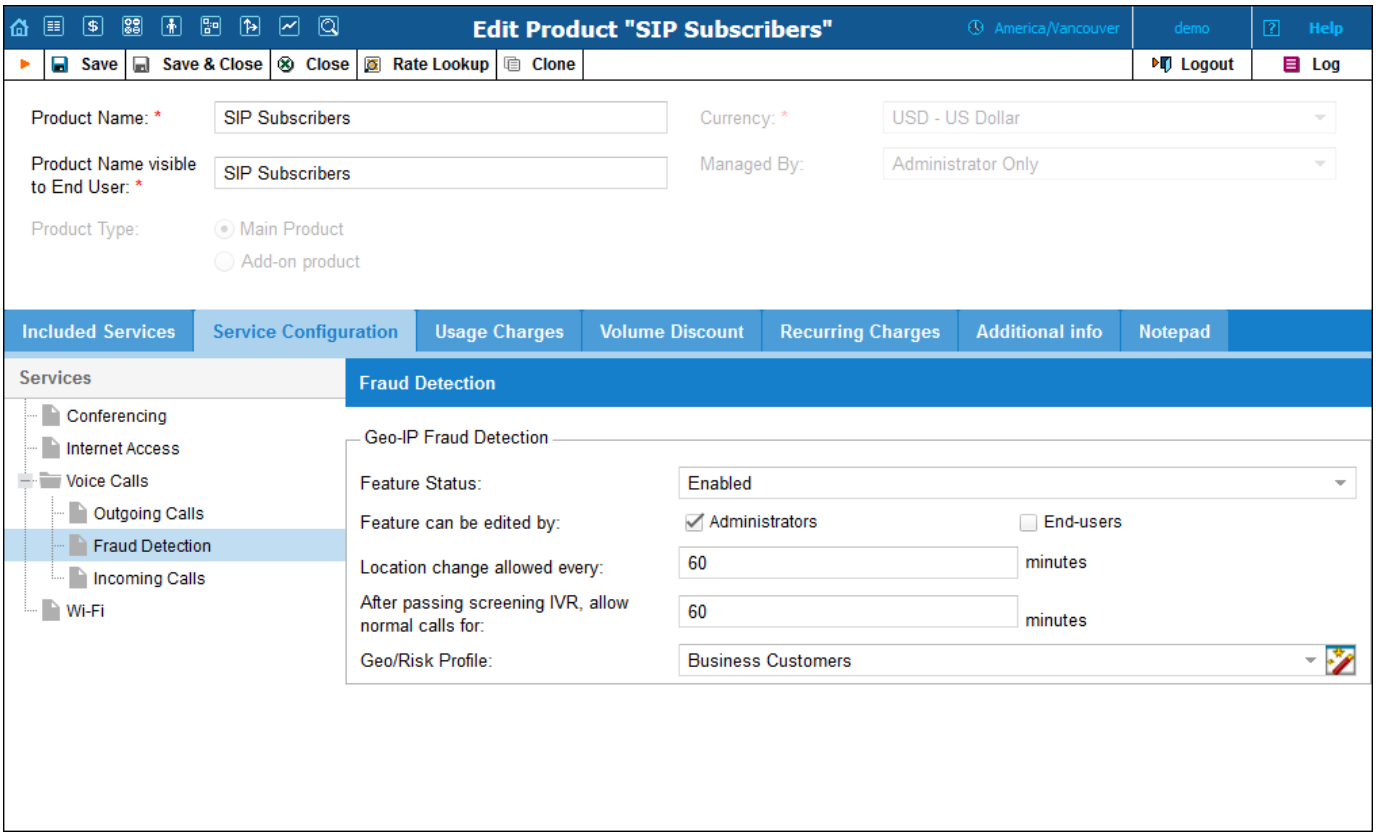
NOTE: The number of calls that can be made without screening is 5 by default and can be configured on the Configuration server.

4. To add countries to the lists, select the required countries from the **No Restrictions** column and drag them to the respective column.

NOTE: You can choose two or more countries by keeping the <Ctrl> key pressed down. Click the **Select All** icon to select all the countries.

5. Click **Save & Close.**

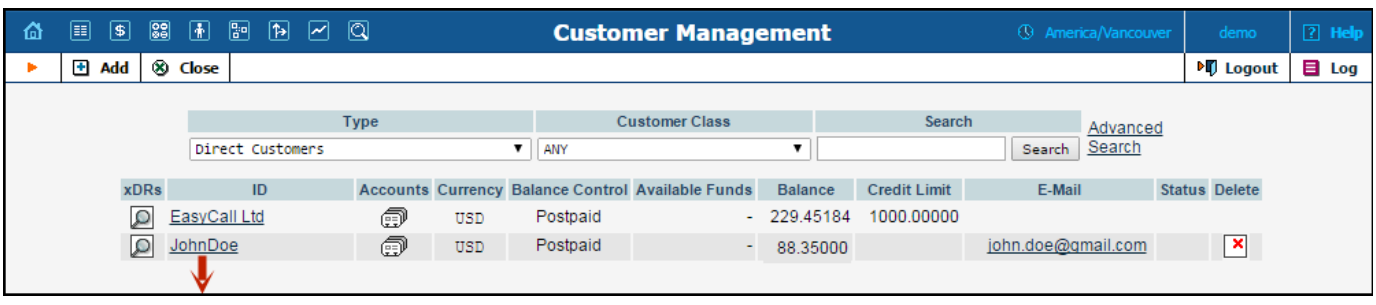
Assign the Geo / Risk profile that was created in the previous step to the product that will be used by the employees of the company.



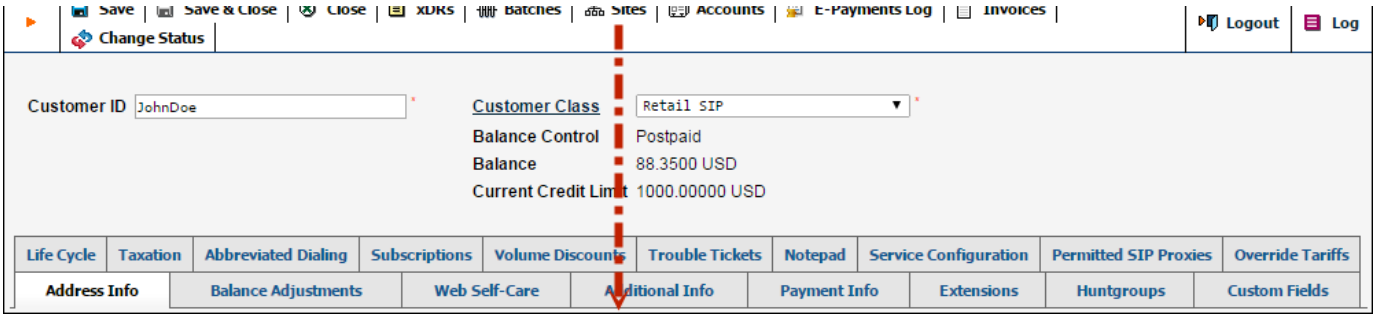
1. In the **Rating** section of the PortaBilling main page, choose **Products**.
2. Select the **Product** for which you would like to assign a Geo / Risk profile.
3. On the **Edit Product** page open the **Service Configuration** tab.
4. Select the **Fraud Detection** section under the **Voice Calls** service type.
5. Fill in the following fields:
   - **Feature Status** – Select **Enabled**.
   - **Geo / Risk Profile** – Assign the Business Customers **Geo / Risk Profile** that you created earlier.
   - **Location change allowed every** – Type 60 minutes here, so that an end user can change location during an interval of 60 minutes without needing to re-input their PIN.
   - **After passing screening IVR, allow normal calls for** – Type 60 minutes here, so that an end user can make calls for 60 minutes after passing the screening IVR without needing to re-input the PIN.
6. Click the **Save** icon to save changes.

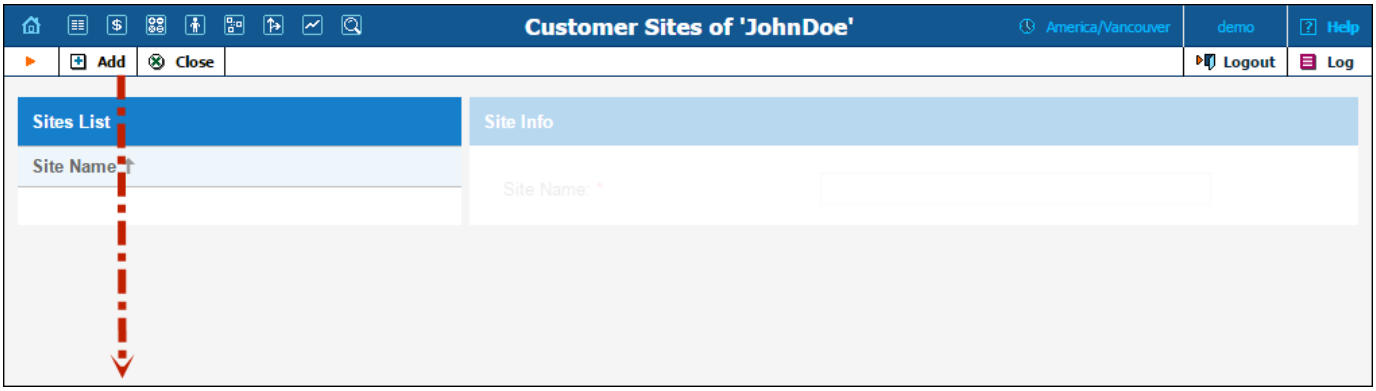
Fraud Protection Configuration on Customer Sites

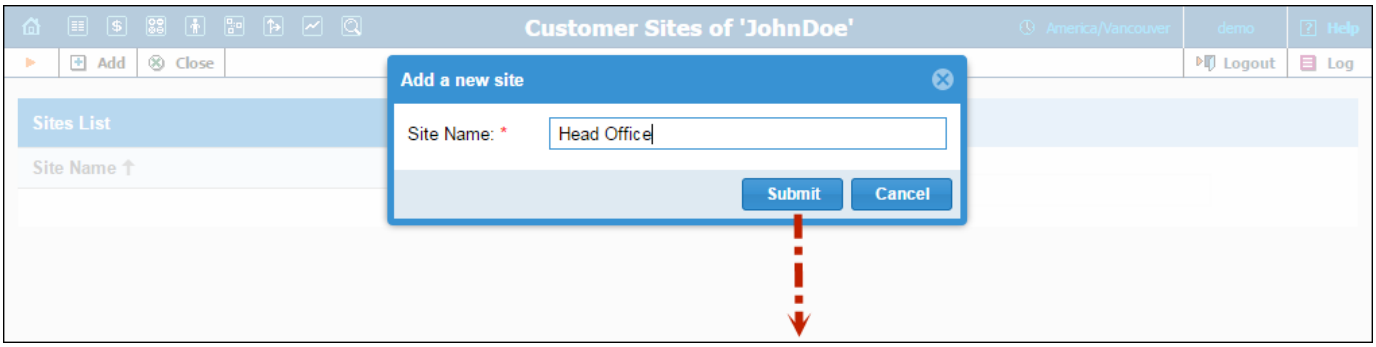
Perform the fraud protection configuration on the customer site so that the settings will be applied to all of this site's accounts.

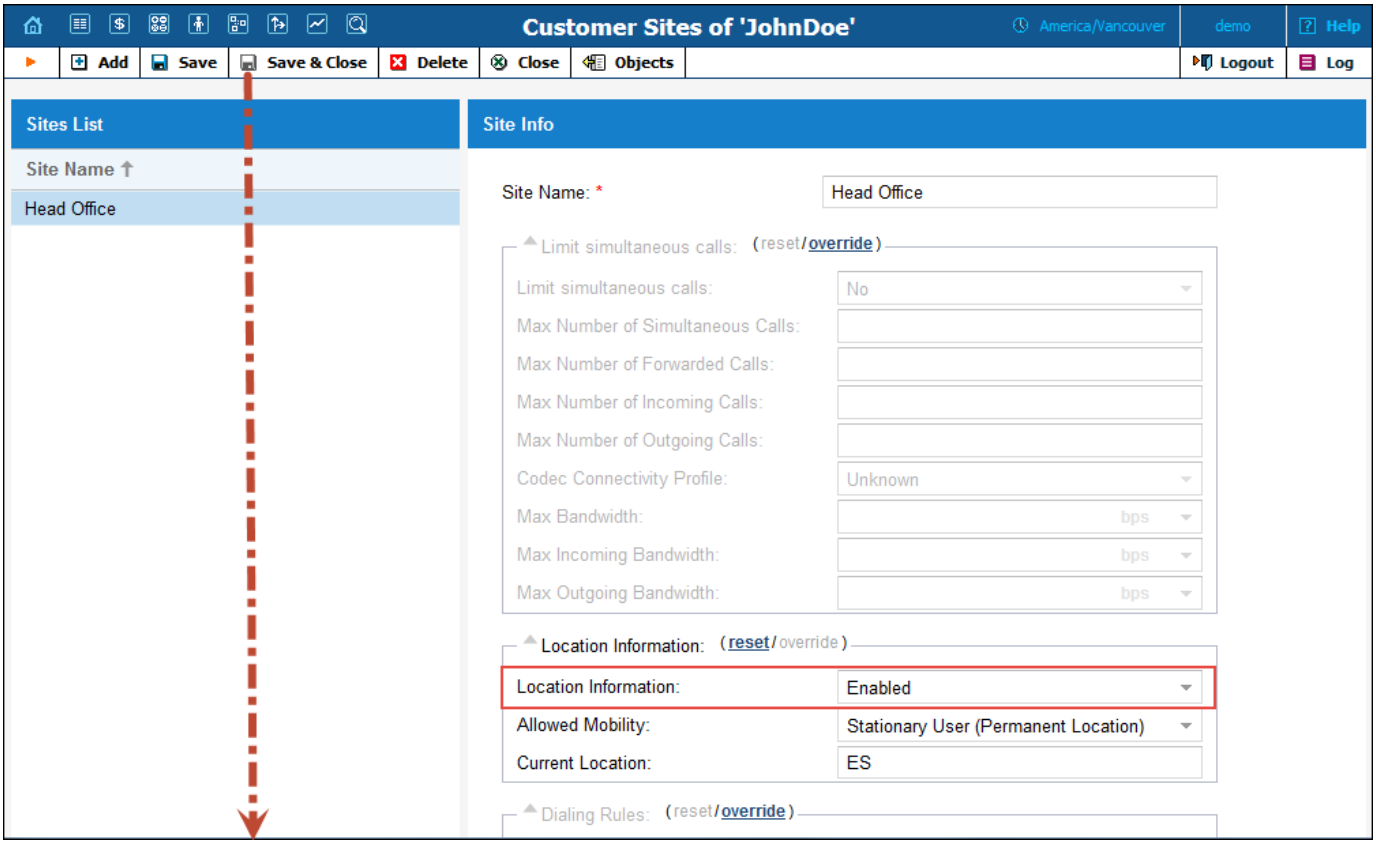


The documentation below is OUTDATED, it describes Maintenance Release 50. Click here for the latest version.





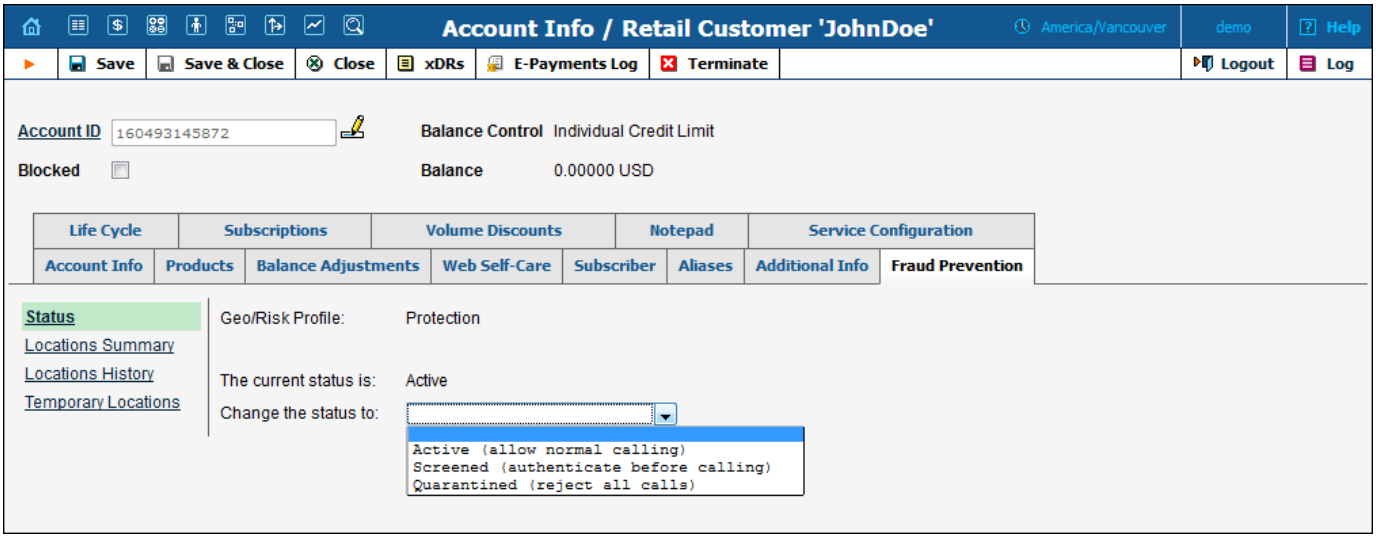




2. Select a customer.
3. On the toolbar, click the **Sites** button.
4. Click the **Add** icon to add a new customer site.
5. Specify the name of the new site in the **Site Name** field.
6. Click **Submit**.
7. Fill in the following fields:
   - **Location Information** – Select the **Enabled** option, which will allow you to define a customer's permanent location for Geo-IP fraud prevention.
   - **Allowed Mobility** – Choose **Stationary User (Permanent location)** since the employees of this company always make calls from the same location.
   - **Current Location** – Type the country where the customer is located. Note that the country specified in this field should be in a *country code top-level domain* format (e.g. *FR* for France, *DE* for Germany, etc). In our example it is *ES*, since the customer is located in Spain.
8. Click the **Save** icon to save changes.

Account Provisioning

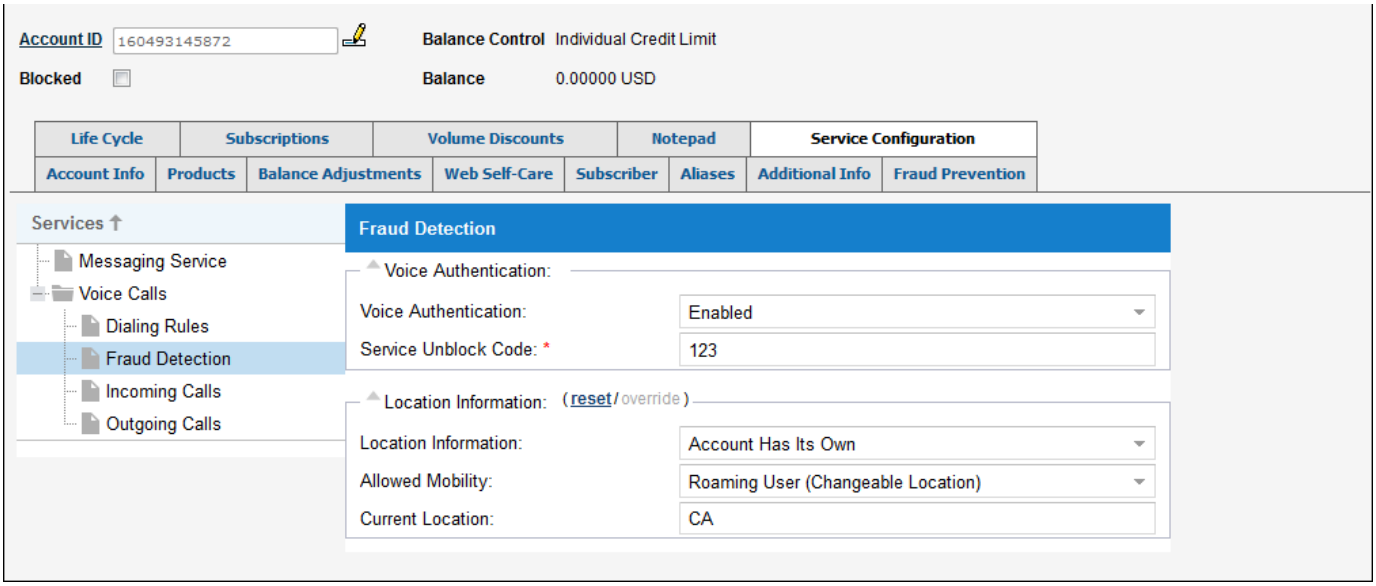
Check an account's fraud protection information and current status. Change the status if necessary.



1. Open the **Account Info** page.
2. Click on the **Fraud Prevention** tab. Here you can view the Geo / Risk Profile name and current status for this account.
3. In the **Change the status to** field you can change the status of this account.
4. If you have modified the **Change the status to** field, click the **Save** icon to save changes.

Override Fraud Protection Settings for an Account (optional)

Perform fraud protection configuration for an individual user. Let's assume that this account is used by this company's sales manager, whose office is situated in Toronto, Canada, although he travels around the world from time to time.



1. Open the **Account Info** page.
2. Select the **Service Configuration** tab.
3. Select the **Fraud Detection** section under the **Voice Calls** service type.
4. Fill in the following fields:
   - **Voice Authentication** – If the call has been made from a "suspicious" location, this feature will enable or disable a customer's authentication when a legitimate customer attempts to make a call.
   - **Service Unblock Code** – This is the account's unique code that is usually provided upon sign-up and can be used later to confirm that a legitimate customer is attempting to make a call *if* the call was made from a "suspicious" location.
   - **Location Information** – Choose **Account Has Its Own** to define a different location for this specific account.
   - **Allowed Mobility** – Only available when **Geo-IP Fraud Detection** is set to **Enabled** and a profile is selected in the **Geo / Risk Profile** option for the account's product. Select **Roaming user (Changeable Location)** since the user of this account frequently travels; in this case, a location change would be considered acceptable.
   - **Current Location** – Type the country where the user of this account is located. Note that the country specified in this field should be in a *country code top-level domain* format (e.g. *FR* for France, *DE* for Germany, etc). In our example it is *CA*, since the user of this account is located in Canada.

5. Click the **Save** button to save the changes.

Fine-Tune Fraud Protection Settings for Private Networks

Internal subnets such as 10.x.x.x, 172.16.x.x, 192.168.1.x do not belong to any specific country. However, there is an option called **GeoIPOverride** that makes it possible:
a) to mark the internal subnets as **Internal Network**s. The Billing Engine considers the Internal Network to be a separate country, so any fraud protection settings described previously can be applied to these internal subnets.
b) to assign the internal subnets to a specific country.
This can be adjusted on the Configuration Server.

1. Go to PortaSwitch® Configuration on the Configuration Server.

NOTE: You can only apply changes for the configuration if it is inactive.

2. Select **BillingEngine** on the Configuration Tree and then choose **VoiceCallsRoaming** among the Groups.

country.

NOTE: Each record must be written in a separate row.

5. Press the **Check / Apply** button.

The configuration shown in the screenshot means that IP addresses from 10.x.x.x, 172.16.x.x, 192.168.1.x subnets are marked as Internal Networks. The customer may now move them to "No Restriction," "Suspicious" or "High-risk" lists on the PortaBilling web interface. The 192.168.222/24 subnet is now considered to be from the Netherlands. Further adjustments for this country must also be done on the PortaBilling® web-interface.