

### **Preventing Toll Fraud**

Preventing Toll Fraud Introduction: Toll fraud and unauthorized PBX access should be a major concern for anyone with a PBX in their office. Toll Fraud can end up costing you (or more often) your clients many thousands of dollars, yet the simple steps necessary to secure an AltiGen system are often overlooked.

Securing the AltiGen Voicemail system:

While ensuring the Operating System is secure from unauthorized access is a good start, it is by no means the only step necessary to preventing toll fraud. The most commonly exploited vulnerability for any PBX system, is a poorly secured Voicemail system. AltiGen systems have many Voicemail features designed to enhance mobility and ease of use for the remote or travelling worker. Unfortunately these features can be exploited if the system administrator is not cognizant of the risks and proper security measures. Most toll fraud attempts against AltiGen systems involve outside callers logging in to a mailbox on the AltiGen system, and then placing toll calls out over the system's trunks, either directly or by setting up a call forward.

- 1) Change the AltiAdmin password and make sure only authorized users have the new password.
- 2) Check the call restrictions for each extension. In AltiAdmin, go to Extension Configuration -> Restriction Tab -> Other Call Restrictions. Ensure that only users who really need these permissions have them.
- 3) If possible, do not allow voicemail access from the main auto attendant, instead setup a special AA with it's own DID/DNIS number for users to call to access their Voicemail while out of the office. This will prevent a hacker from gaining entry to the VM system from the main published phone number.
- 4) Utilize notifications options to warn a manager or administrator if unusual call activity has been detected. This setting is enabled by checking the box 'when unusual call activity has been detected' under the Notification tab of the Extension Configuration. This will initiate a notification call to warn the configured extension when calls made from voice mail are unusually long (by default, more than 120 minutes) or when the number of calls made from voice mail is unusually high (by default, more than 20 calls in one voice mail session).
- 5) Make sure all extensions have a secure password. Delete extensions or at least change their VM password when an employee leaves the company. Periodically change the default password used when setting up new extensions.

Generally, an extension is considered secure if its password meets the following conditions:

- Contains 4-8 digits.
- Is different from the extension.
- Is different from the default system password.
- Does not consist of consecutive numbers.
- Does not consist of a repetition of the same digit.

Note: By default, a VM box will become locked for 1 day after 8 bad login attempts. You can change the lock duration from the Call Restriction tab of System Configuration. You can view extension security status and reset locked extensions using the Admin and Extension Security Checker utility under the Start, Programs,

AltiWare (or MAX Communications Server), Utilities.

#### Securing the Server and Operating system:

The easiest way to prevent unauthorized access to your AltiGen PBX is to make sure all local administrator accounts have a secure password, which is known by as few individuals as possible. You should never leave the Administrator password blank or as the default. It is common for AltiGen servers to be joined to a domain, so it is also important to be aware of your client's network security policies, and to be prepared to make recommendations for improvement if they are lacking. Here are a few helpful links on creating strong passwords and best practices for domain security:

Creating Strong Passwords

Windows 2003 Security Guide

Windows XP Security Guide

What should I do if the system has already been compromised?

The very first step would be to follow the instructions in this document to close any security holes and prevent any future toll abuse. Next contact the telco and inform them of the toll fraud, use the CDR search to help identify the unauthorized calls. Ask the carrier who will be responsible for the charges, unfortunately the end user is generally responsible for any toll calls on their lines, whether or not the use of the lines was authorized or not.

<https://know.altigen.com/questions/896/>