Information sheet

\Orchestrating a brighter world

NEC

Toll Fraud Defence

# InGuard

## Pro-active application against toll fraud attacks - 'on duty' 24/7/365

**InGuard is an effective, low cost solution to help protect a business against the rise of toll fraud attacks.**

Toll Fraud is a fraudulent attempt by a hacker to gain unlawful remote access to a phone system. Attacks are often highly organised from an automated server and once accessed, fraudulent calls are connected and over a period of time, can run up call charges of potentially thousands.

Typically, these occur out of office hours and are usually discovered after the event when it's too late and businesses are left to cover the costs.

The vast majority of businesses are considered vulnerable to these attacks and most networks and phone systems have only basic toll restriction features. Although no solution can provide 100% protection, this application is strongly recommended.

### InGuard Uses & Business Benefits

NEC
System Configuration Check
Default System Password
System Password Strength
Working Toll Restriction Class Password Strength
DISA Password Strength

- **Peace of mind** with an effective toll fraud defence
- **'On duty' 24/7/365** & reacts instantly to a toll fraud attack
- **Tailored specifically** to the needs of your business & call patterns
- **Zero maintenance solution** which 'sits in the background' – until any alerts are triggered
- **Easy to use:** alerts are easily switched off if telephone useage is legitimate
- Also acts as a **strong deterent** to internal telephone abuse

### At a Glance

- Effective toll fraud defence for SV9100, SV8100, SL1000 & SL1000 users
- Highly cost-effective
- Low maintenance

**As one of NEC's InApps solutions, features include:**

NEC InAPP BUILT-IN SOLUTION

- Built-in / embedded application
- Browser-based & available 24 / 7
- Extremely cost-effective
- No extra PC / Server required - data is stored on the CPU
- Save on hardware costs

## InGuard Overview

**InGuard is an embedded application that runs on the CPU of the PBX.**

- The application helps to prevent toll fraud by monitoring call records that are output by the PBX
- It has the ability to alter the system programming to prevent extensions from dialling out & certain numbers from being dialled
- 'Rules' are then created & when they are breached, further calls can be blocked
- Custom rules can be created for departments that make lots of calls or known safe dialled numbers

## How InGuard Works

**All call activity is monitored 24/7 and any suspicious call activity is detected instantly.**

This results is one of two automatic alerts:

- An **'alert only'** email sent to designated recipients
- In more severe cases an **'alert and block'** which prevents any further call activity instantly
- The emails provide **call information** explaining why a call or calls were considered to be suspicious

Once checked, if the call activity is legitimate the restriction can be removed simply by replying to the email and your business communications continue as normal.

## Bespoke Settings for a Business

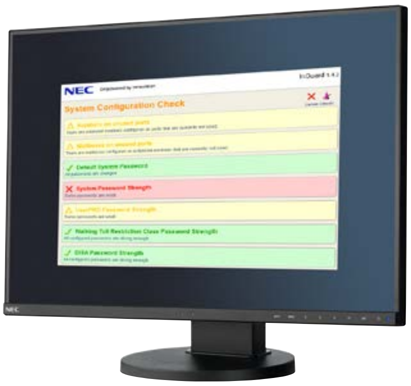
**The simple set-up of Toll Fraud is based around your businesses specific call patterns, i.e. office hours, public holidays, length of a call, excessive calls rates, etc.**

- From these parameters a set of rules are created - and if a rule is broken, an alert is sent
- Not only does this detect a suspected toll fraud attack, it can also help **prevent internal abuse** of the system
- Amends to rule settings (e.g. changes in office hours) can be made remotely via a browser for easy administration

## Health Check Feature

**This feature helps to make sure the system is setup is a secure way, not leaving it susceptible to toll fraud.**

- The Health Check feature looks at the configuration of the PBX & carries out numerous security checks
- A report is produced indicating any potential areas of vulnerability as below - these can be reviewed by the installer to determine if the system is securely configured:


NEC

System Configuration Check

Default System Password

System Password Strength

DISA Password Strength

- **Green** indicates a feature is well configured & secure
- **Yellow** means the configuration may have potential security considerations & should be reviewed
- **Red** is a security risk & this issue should be remedied

## System Requirements

- **SV9100:** v5.00.50 or higher
- **SV8100:** v9.54 or higher
- **SL1000 / SL1100:** v6.11 or higher

**EMEA (Europe, Middle East, Africa)**
NEC Enterprise Solutions
*www.nec-enterprise.com*

For further information please contact NEC EMEA or: