Orchestrating a brighter world

NEC

InGuard

Installation Guide

Version 1.0

For InGuard 1.7.0

Contents

Revision History

Version	Author	Date	Changes
1.0	R Horsley	Dec 2019	Initial release of InGuard 1.7.0

What is Toll Fraud?

Toll Fraud is a term used to describe the occurrence un-authorised calls on a PBX. Misuse can of course originate in-house, for example private calls initiated by an employee, or forwarding of a DDI to an extension and then on to an external destination. However, the rise in Dial Through Fraud (DTF) and VoIP security threats reported recently shows us that the worst misuse is likely to be generated remotely by hackers who exploit any available remote access to the customers PBX to generate expensive unauthorised calls.

It is important to note that any customer thus affected is still liable for all such call charges and these can sometimes run can extremely expensive. DTF can be perpetrated via a number of access methods, examples include IP-PBX systems reprogrammed remotely, SIP Trunks, SIP Extensions, DISA (Direct Inward Service Access) or Voicemail. The hacker has the aim of obtaining access codes and passwords/PINs that will enable unauthorised calls to be made via a customer's switch. Often, the hackers then sell on these details to an organised fraudster for profit.

InGuard

InGuard is an active call monitoring application that can be used to help prevent toll fraud from happening. It works by monitoring SMDR output provided by the PBX and applies user configured rules to look for call trends that could be deemed fraudulent. When potential fraudulent activity takes place the guard can send email notifications to users informing them of the suspicion. As the application runs on the PBX it has the ability to prevent further fraudulent activity from taking place by modifying its configuration. If the same extension is making a high number of calls then it can be moved to a restricted toll restriction class to prevent it from making further calls. Likewise if the Guard sees many outbound calls to the same number, it can block this number from being dialled.

There are two stages to the blocking actions for outbound calls, the alerts are first set to warn the user about the possible fraudulent activity. Secondly an automatic blocking action can be carried out, this could be to put and extension a restrictive toll restriction class or block a number from being dialled.

Say for example an alert is configured that provides a warning if 50 outbound calls are made in a 60 minute period and blocks if 100 calls are made in the same time period. When the 50 call limit is reached by an extension, an email will be sent informing the configured users. If the user replies to the email then the extension will be moved to a restrictive toll restriction class to prevent it from being able to dial out. When the 100 call limit is reached, if the user had not replied to the first email then the extension would be automatically blocked from dialling out. When this happens, an email is generated saying that the number has been blocked. The user can reply to the email to un-block the action. A similar concept exists to block an actual number from being dialled rather than an extension making a high number of calls. This would mean if any extension made calls to the same number, the number could be added to a restrict table. Further details of the rules and what they do is available in the End User Guide.

For Inbound calls InGuard will monitor the system for suspicious call patterns and send an email to warn the user. As such there are no blocking actions that can be carried out for incoming calls, the Guard just informs the user about the suspicious behaviour.

InGuard has a built in health check feature that can look at the configuration of the PBX and show if any areas may leave the PBX vulnerable to attack in different ways. This can prompt an installer to make sure adequate precautions are taken when enabling features on the system.

InGuard requires access to an email server that is enabled for SMTP and POP3, these are used for email integration to the application, SSL/TLS and unencrypted connections can be used. The application is accessed using a Web Browser, Internet Explorer version 11, Edge and Firefox 37 can be used to configure the Guard.

This manual explains how to install and configure InGuard application.

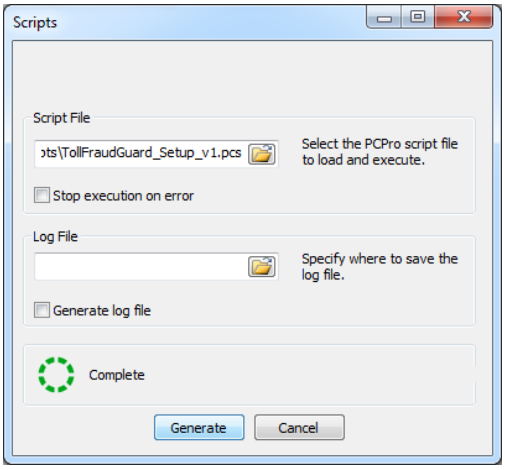
PBX Requirements

InGuard runs on the CPU of the PBX using its Lua engine. A version of system software that contains the Lua engine will need to be running on the PBX, the versions of system software are as follows:

PBX	System Software Version
SV9100 CP10 / CP20	8.00.50 or above
SL2100	1.50.00 or above

PBX Configuration

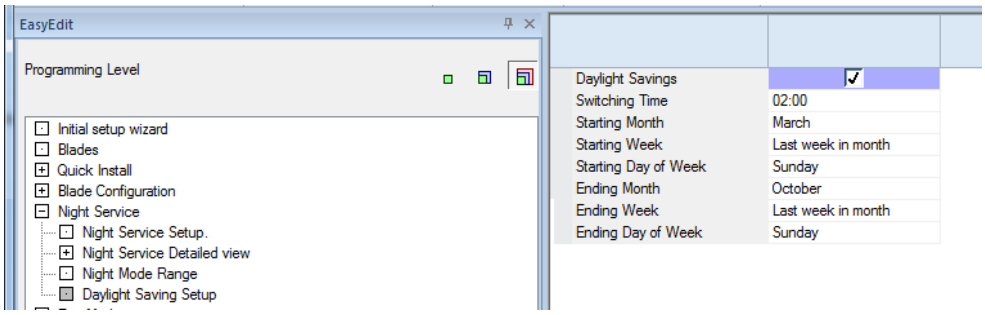
InGuard uses SMDR output from the PBX to gather details about calls that are made. SMDR output has to be enabled in a particular format that the application will recognise. There is a PC Pro script that can be run to configure the SMDR into the right format and enable the output for all extensions and trunks. The Script is called “TollFraudGuard_Setup_V1.pcs”. In effect the script will enable SMDR Output over TCP Port 4001 for all extensions and trunks.



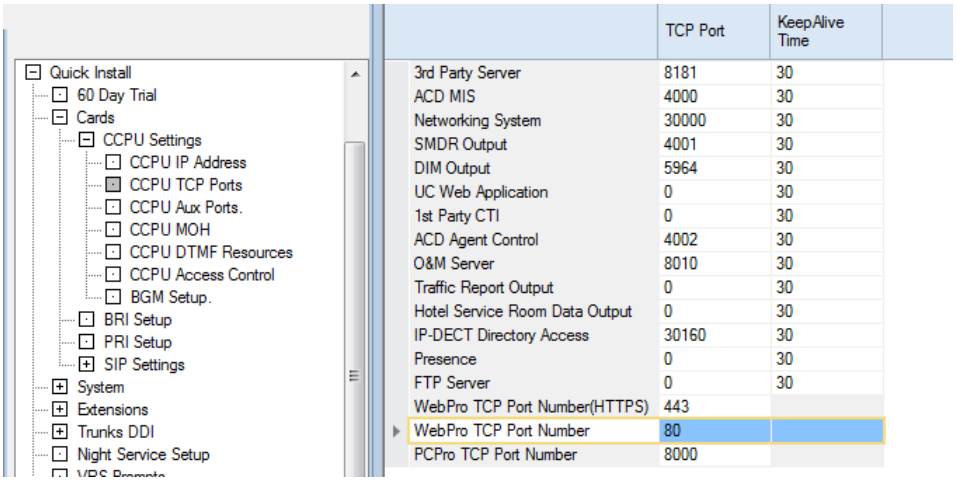
If LCR is being used on the PBX then InGuard cannot always guarantee to perform a blocking action for a number that is being dialled. This is down to the way that LCR carrier codes are included in the SMDR output. It is therefore recommended that F-Route is used instead of LCR.

If InGuard tries to block calls to a specific number and it sees subsequent calls to the number then there is an option to prevent any calls apart from emergency ones from being made on the PBX.

In order for InGuard to be aware of the correct time, the Daylight Saving feature has to be enabled, this is in PC Pro > Easy Edit > Night Service > Daylight Saving Setup or PRG command 10-24.



On the SV9100 CP20, the HTTP TCP port on the needs to be enabled to use any of the InApps. The setting that allows best interoperability with web browsers is TCP Port 80. This can be set in PC Pro > Easy Edit > Quick Install > Cards > CCPU Settings > CCPU TCP Ports or PRG Command 90-54-01.



Licensing

The InGuard Application requires a license in order to run, the license is a normal system license that is installed on the PBX. The application can run when the 60 day license is active on the system.

PBX	Part Number	4 Digit Feature Code(s)
SV9100	BE117757	3512, 0041
SL2100	BE116763	3512, 0041

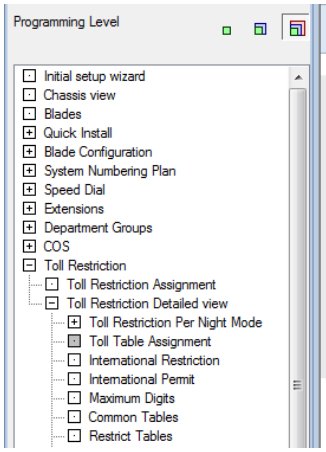
The 3512 code can only be displayed in PC Pro, so if you want to check to see what licenses are installed then look in PC Pro. TelPRO and WebPRO do not show license code 3512.

Toll Restriction on the PBX

Toll Restriction should be enabled as normal on the PBX, on top of that for InGuard to be effective, some areas of Toll Restriction have to be set aside for it to use. In terms of actions that InGuard can carry out, firstly it can move extensions to a predetermined Toll Restriction Class. This Toll Restriction Calls should be completely restricted from making any outbound calls apart from calls to emergency telephone numbers. The second action the guard can carry out is to block certain numbers from being dialled by putting it in a Restrict Table. A dedicated Toll Restriction Table should be elected as one that the InGuard application will use.

Configure a Restricted Toll Restriction Class

In PC Pro you will need to switch to Easy Edit Mode and be in programming level 3. In there you will find the Toll Restriction area, alternatively this can be configured in PRG commands 21-xx. Open the page in Easy Edit > Toll Restriction > Toll Detailed View > Toll Table Assignment. Elect a Toll Restriction class that will be used as the restricted area to put extensions into so that they cannot dial out. In the example below Toll Restriction Class 15 has been used.



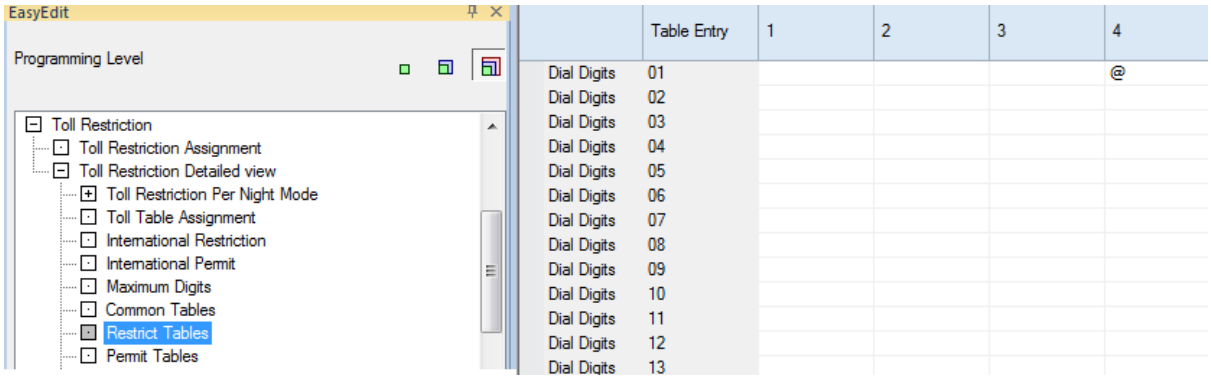
Toll Restriction Class	International Call Restriction Table	International Call Permit Code Table	Maximum Digit Table Assignment	Common Permit Code Table	Common Restriction Table	Permit Code Table	Restriction Table
<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
01	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
02	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
03	Unassigned	Unassigned	1	Assigned (see 21-06-04)	Unassigned	3	3
04	Unassigned	Unassigned	2	Assigned (see 21-06-04)	Unassigned	3	3
05	Unassigned	Unassigned	3	Assigned (see 21-06-04)	Unassigned	3	3
06	Unassigned	Unassigned	4	Assigned (see 21-06-04)	Unassigned	3	3
07	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
08	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
09	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
10	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
11	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
12	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
13	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
14	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
15	Unassigned	Unassigned	4	Assigned (see 21-06-04)	Unassigned	4	4

Set the following data for the elected Toll Restriction Class.

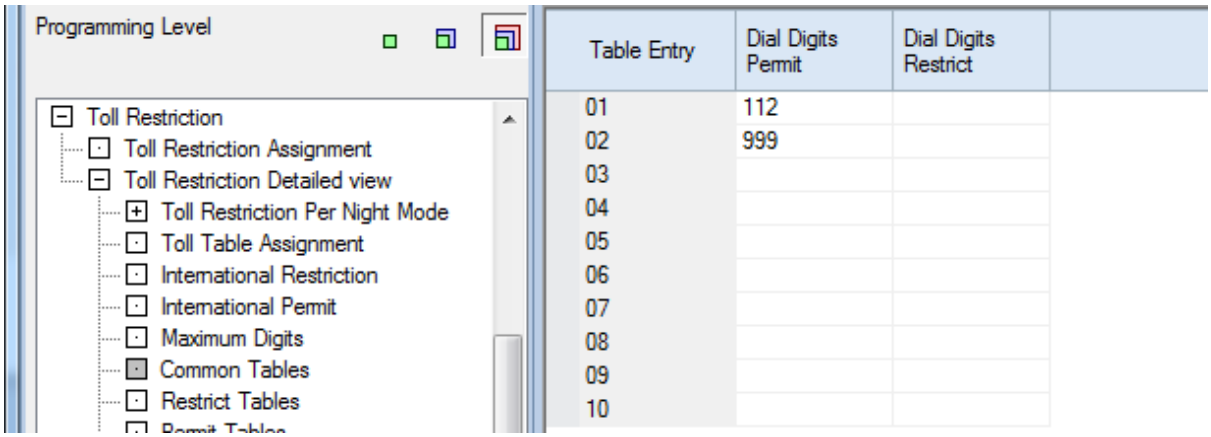
Setting	Value
International Call Restriction Table	Unassigned
International Call Permit Table	Unassigned
Maximum Digit Table Assignment	4
Common Permit Code Table	Assigned (see 21-06-04)
Common Restriction Table	Unassigned
Permit Code Table	4
Restriction Table	4
Speed Dial Common Restriction	Enabled
Speed Group Dial Restriction	Enabled
Internal Call Restriction	Disabled
PBX Call Restriction	Disabled
TIE Call Restriction	Enabled

This effectively means that the Toll Restriction Class will be permitted to dial any number assigned in the Common Permit Code Table or Permit Table 4. Any numbers entered in Restriction Table 4 cannot be dialled.

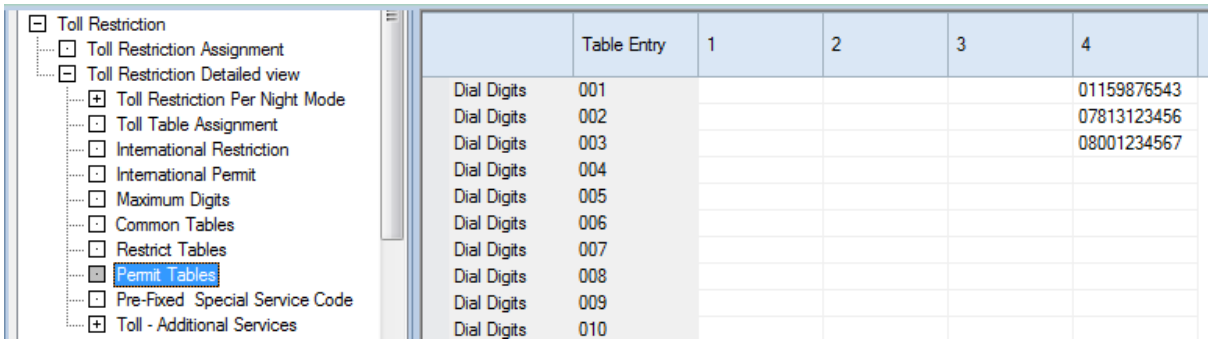
In Toll Restriction > Toll Restriction Detailed View > Restrict Table, enter @ against table 4. This is effectively treated as a wild card meaning no digits can be dialled. The only override for this rule would be any numbers entered in the Common Permit Table or the Permit Table.



In Toll Restriction > Toll Restriction Detailed View > Common Tables, enter any emergency numbers that may need to be dialled in the Dial Digits Permit column. This will allow an extension that has been put into the Toll Restriction Class that InGuard will use will always be able to make emergency calls. Numbers up to 4 digits in length can be entered in this table.



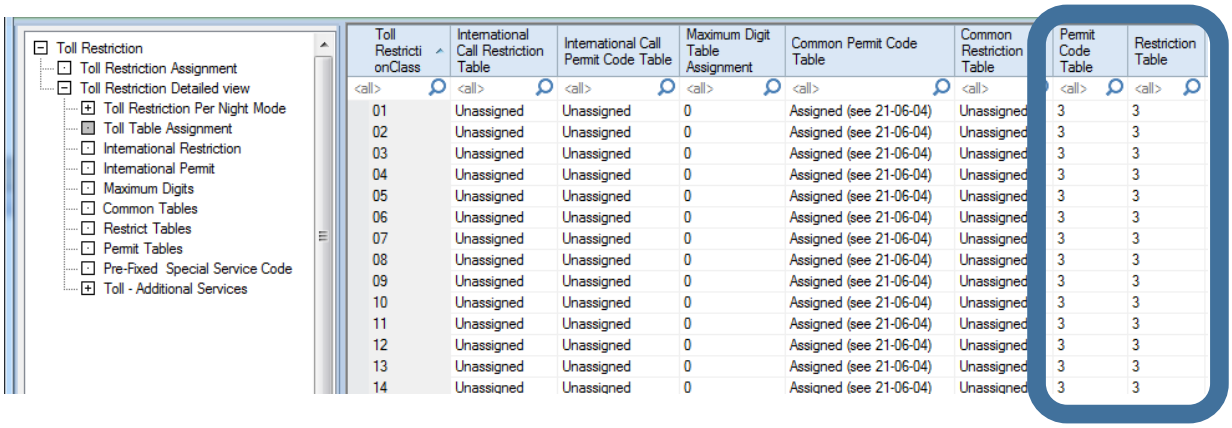
The permit table can be used to enter any other specific numbers that should be allowed to be dialled in the restricted toll restriction class. You may for example want to be able to contact a security company or the maintainer of telephone system.



Once these changes have been applied to the PBX then they should be tested to confirm they are working as expected. To do this, manually assign an extension to the Toll Restriction Class that the Guard will use and try to make some outbound calls to different destination numbers. If you use different Day and Night modes on the PBX then its good practice to check Toll Restriction in each different mode that is used. Once you have confirmed the Toll Restriction is working correctly then move the extension back to its previous toll restriction class.

Configure an Area to Restrict Dialled Numbers

Open the page in Easy Edit > Toll Restriction > Toll Detailed View > Toll Table Assignment. Assign a Restriction Table to all used Toll Restriction Classes apart from the one assigned to the Restrictive Toll Restriction Class. This will prevent any numbers in the restriction table from being dialled, the example below shows Restriction Table 3 being used for Classes 1-14.



Toll Restriction Class	International Call Restriction Table	International Call Permit Code Table	Maximum Digit Table Assignment	Common Permit Code Table	Common Restriction Table	Permit Code Table	Restriction Table
<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
01	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
02	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
03	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
04	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
05	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
06	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
07	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
08	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
09	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
10	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
11	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
12	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
13	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3
14	Unassigned	Unassigned	0	Assigned (see 21-06-04)	Unassigned	3	3

The settings these Toll Restriction Classes should be as follows:

Setting	Value
International Call Restriction Table	Unassigned
International Call Permit Table	Unassigned
Maximum Digit Table Assignment	0
Common Permit Code Table	Assigned (see 21-06-04)
Common Restriction Table	Unassigned
Permit Code Table	3
Restriction Table	3
Speed Dial Common Restriction	Enabled
Speed Group Dial Restriction	Enabled
Internal Call Restriction	Disabled
PBX Call Restriction	Disabled
TIE Call Restriction	Enabled

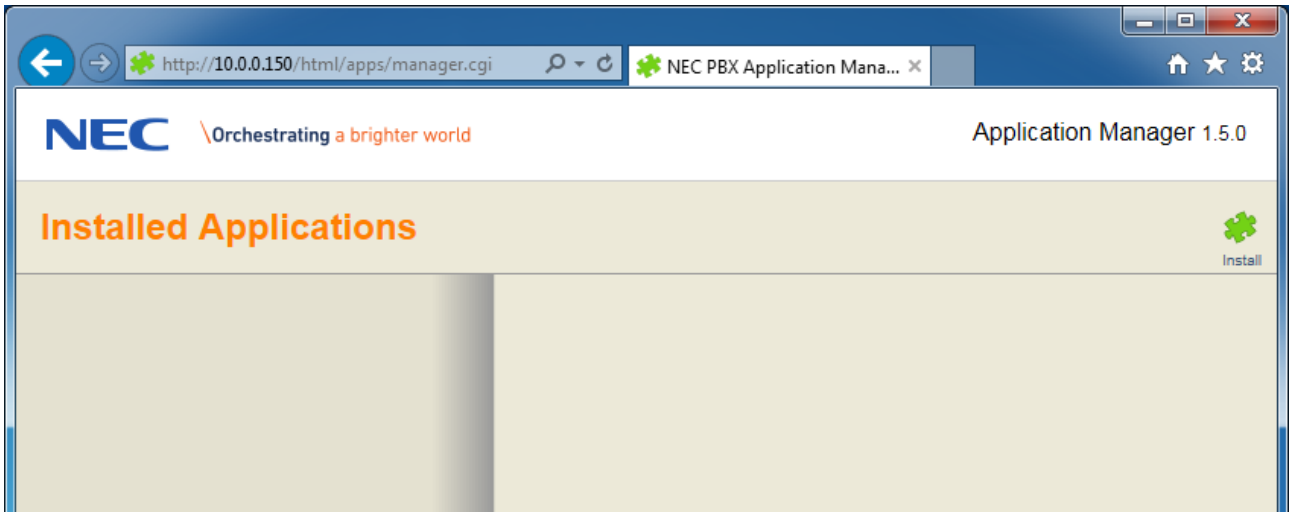
Numbers that should be restricted from dialling will need to be entered in Restrict Table 3, the Guard application will be configured to also put numbers that it blocks into this table. Permitted numbers will need to be entered into Permit Table 3. The common permit code table and common restriction tables can be used to permit and restrict other numbers at a higher level.

Before continuing with the installation of the Guard you should thoroughly test the Toll Restriction programming and make sure it's working as expected. Remember to perform testing in each used day / night mode.

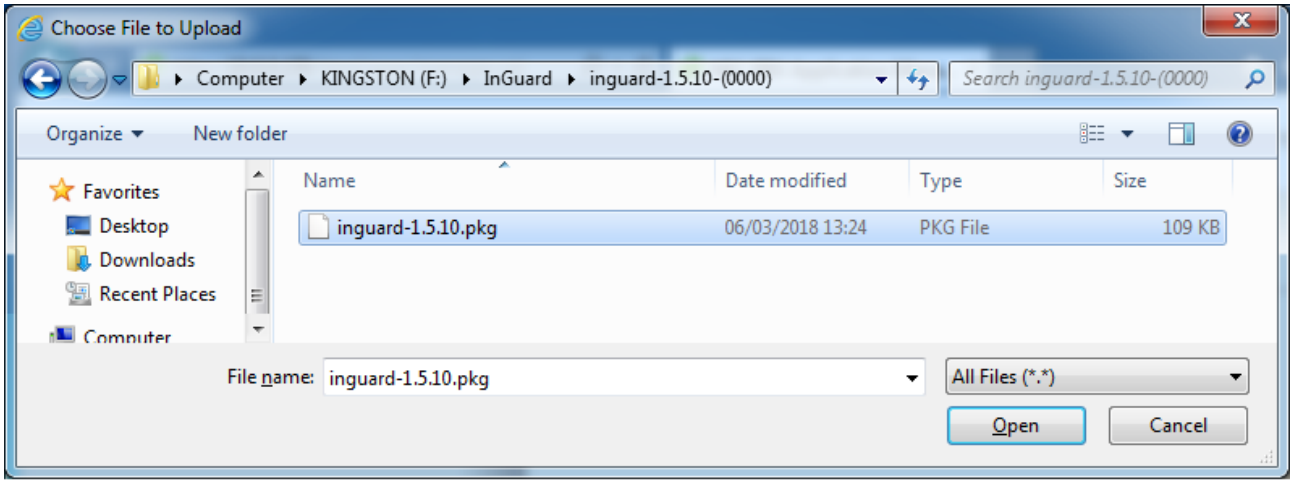
Installing InGuard

Before installing or using the software you must read the InGuard Software License Agreement.

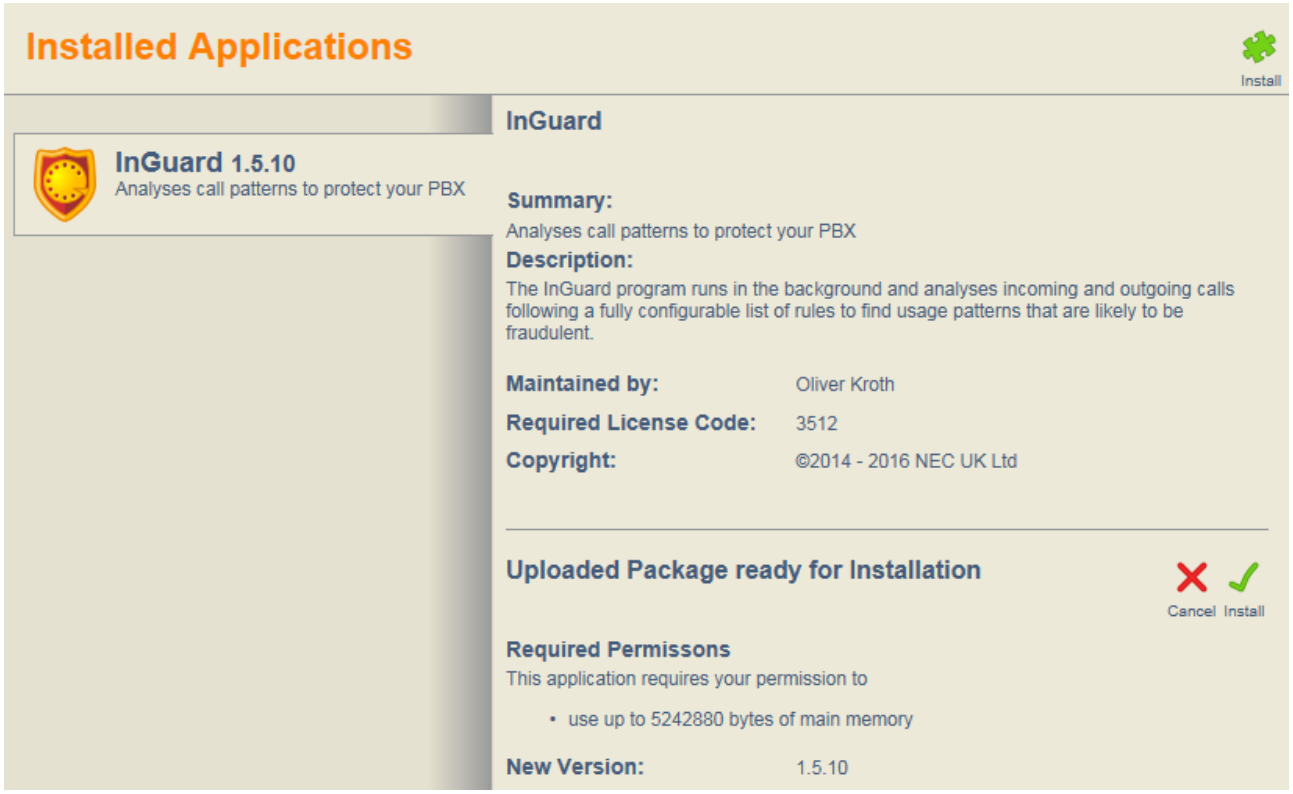
InGuard is installed using the Application Manager page, from the home page click the Install button in the upper right hand side of the page. This is available from:
http://IP Address of the PBX/html/apps/manager.cgi
You need to enter an installer level username and password from command 90-02 to access the application manager.



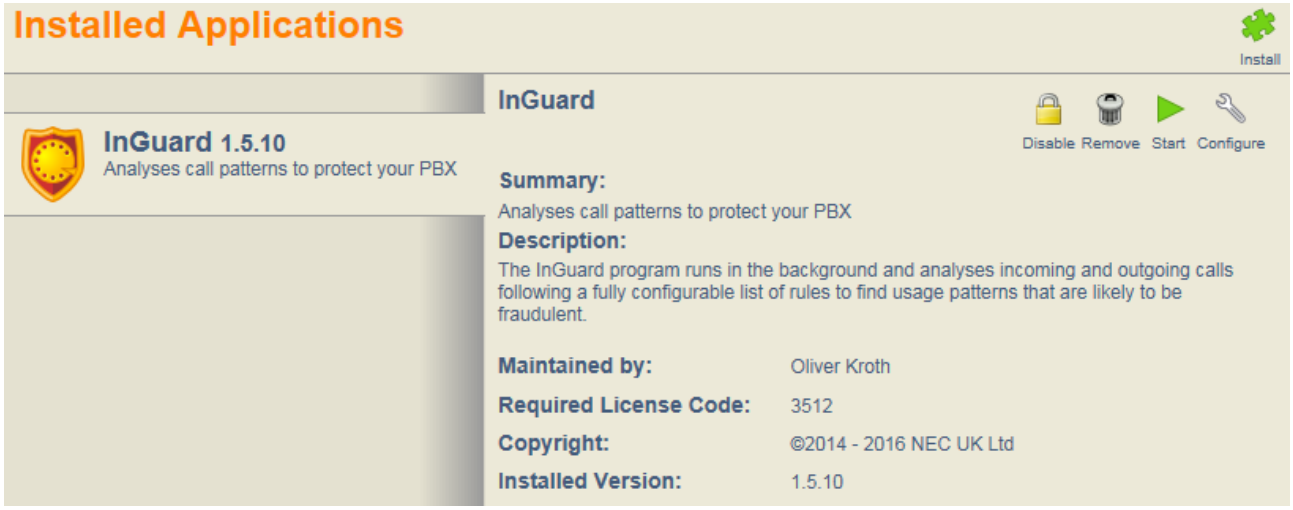
Browse to the InGuard installation file and click OK.



Click the Install button in the lower right hand corner to install the application.



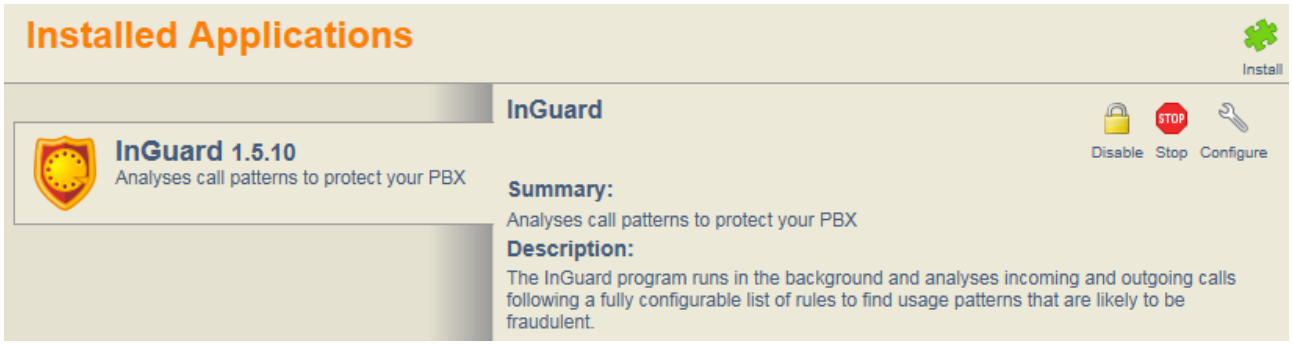
Once the application is installed, the options to Start, Disable, Remove and Configure are available.



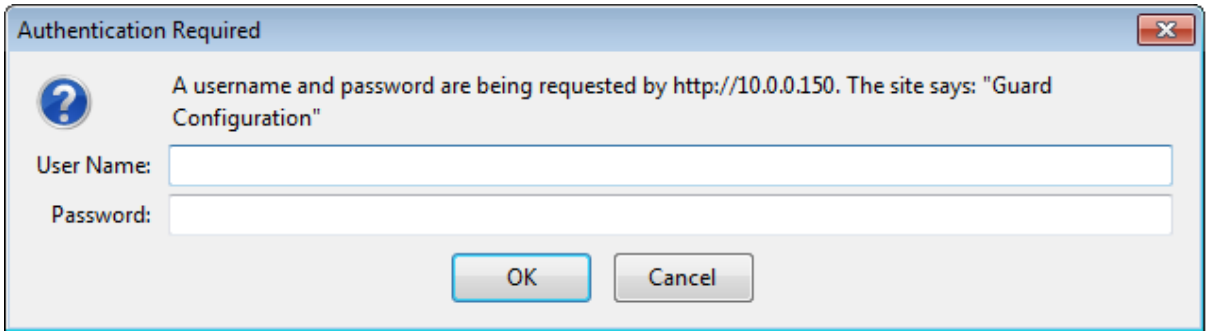
Once the Guard is installed then click the start button to run the application, once started the Start button will be replaced with a stop button. When InGuard is configured and starts, it will start gathering data and apply and rules that are configured. Each time the Guard is stopped and started, it will start gathering data from scratch, the guard doesn't hold historic call information. When the PBX is restarted InGuard will automatically start unless it has been disabled.

Configuring the InGuard

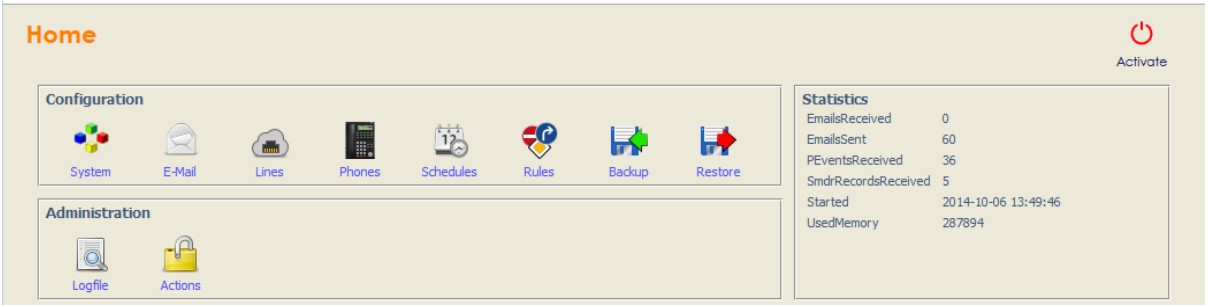
Click the Configure button on the right hand side to begin setting up the guard application.



You will be prompted to enter a username and password to access the configuration. Enter an installer level username and password for the PBX to logon.



Once you have logged in, you will see the configuration home screen. From here you can configure all the different options that are available in the guard.

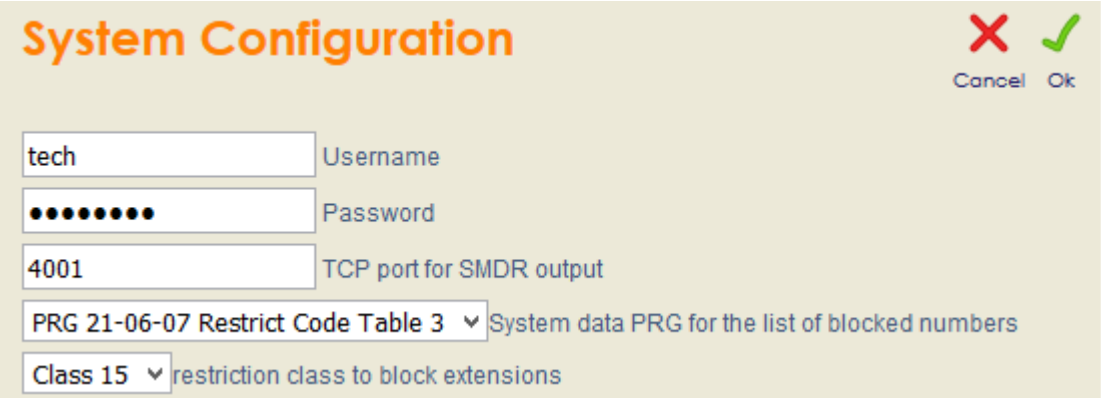


System

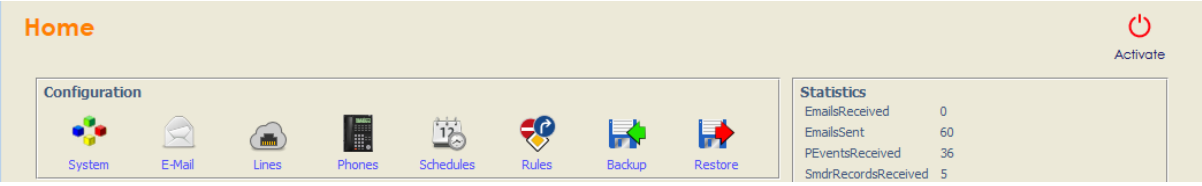
The system menu is used to define information used by InGuard to integrate to the PBX.

Setting	Value
Username	The username for the PBX is automatically detecting during the installation of the application. A new username can be entered if required.
Password	The password for the PBX is automatically detecting during the installation of the application. A new password can be entered if required.
TCP port for SMDR Output	Enter the TCP Port for the SMDR output, the Script sets this to 4001 by default.
System Data PRG for the list of blocked numbers	This is the area where the guard will enter numbers that are blocked from dialling. This should have already been created and defined in the PBX's Toll Restriction configuration.
Restriction Class to Block Extensions	This is the Toll Restriction Class that has been created for the Guard to use.

Enter the system configuration parameters and click OK to save the changes.



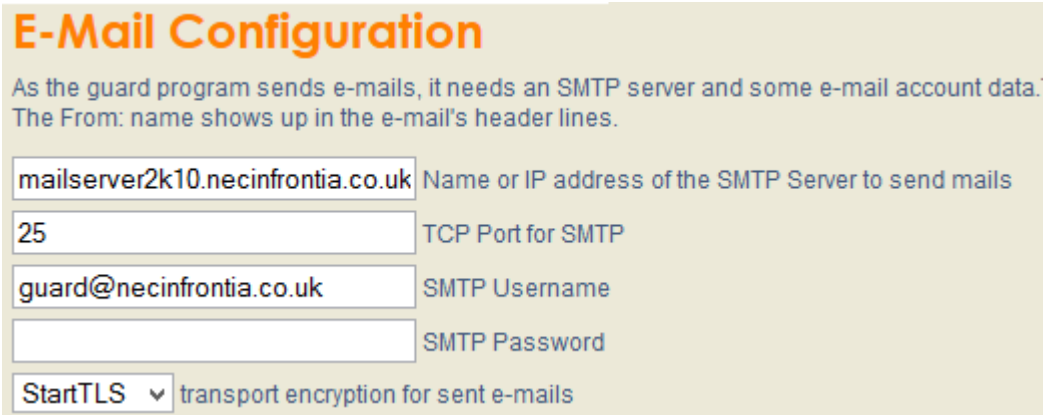
To apply and changes, click the Activate button in the home page.



Email Configuration

InGuard uses emails to inform users when Toll Fraud rules have been broken. Emails that InGuard sends are sent using SMTP, typically the administrator of the mail server will assign an email address that will be used by InGuard. The username will be the username of the SMTP user account. If the mail server is using Authentication mode then an SMTP Password will need to be entered. If Authentication mode isn't being used then do not enter a password.

InGuard should work with any SMTP mailserver and has been specifically tested with Exchange 2010©, Gmail© and Argosoft©.



Note! The SMTP Username is used in the SMTP protocol as the sender, this is usually entered in a format containing the domain name.

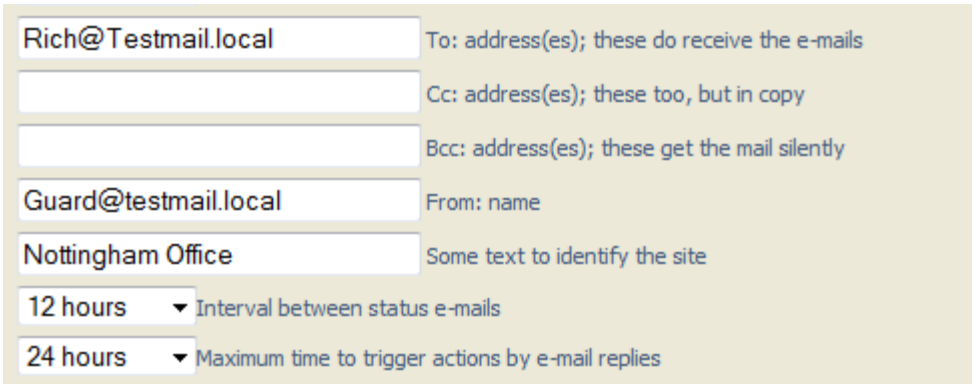
If the mailserver is entered as a hostname, then DNS must be entered in PRG command 10-12-13.

Setting	Value
Name or IP Address of the SMTP Server to send mails	Enter the IP address or hostname of the mail server.
TCP Port for SMTP	Enter the TCP port for SMTP mail server.
SMTP Username	Enter the username for the SMTP account.
SMTP Password	If required enter a password.
Transport Encryption for sent emails	Select the encryption type that will be used for sending emails.

The next part of the configuration is used for the POP3 functionality, this is used by InGuard to look for replies to email messages. The administrator of the mail server will typically need to create an account that is enabled for POP3. The guard will logon to the configured POP3 account with the supplied username and password to check for new emails.

Setting	Value
Name or IP Address of the POP3 Server to collect mails	Enter the IP address of the POP3 mailserver.
TCP Port for POP3	Enter the TCP port for SMTP
POP3 Username	Enter a username
POP3 Password	Enter a password
Transport Encryption for received emails	Select the encryption type that will be used for receiving emails.
Period to look for new emails	Select the how often the Guard will look for replies to emails.

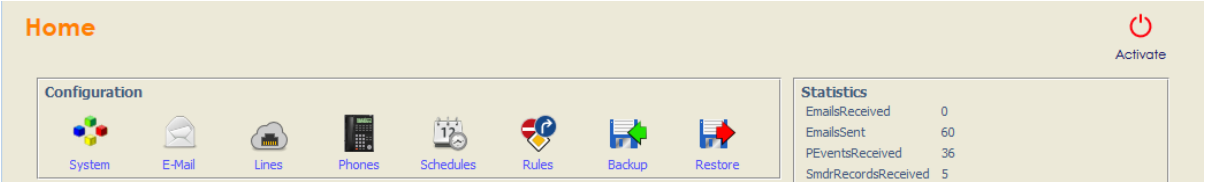
The final part of the email configuration defines the rest of the mail settings and some miscellaneous items.



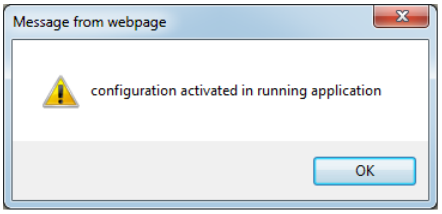
Configure the settings as required.

Setting	Value
To: Address	Enter the email addresses that will receive the emails. Use a comma , to separate multiple email addresses.
Cc: Address	Carbon Copy Email addresses can be entered here.
Bcc: Address	Blind Carbon Copy Email addresses can be entered here.
From:	This will be who the email is sent from.
Some Text to Identify the site	Enter a name to Identify the site, this text is included in the email subject and main body.
Internal between status emails	The Guard will send an 'On Duty' email at set intervals to inform the user that it is still running. Set the interval in the drop down menu. The 'On Duty' email can be disabled by selecting 'Do NOT Send'
Maximum time to trigger actions by email replies	When an email is generated it will be valid for a period of time, set the duration that the email will be valid for in here.

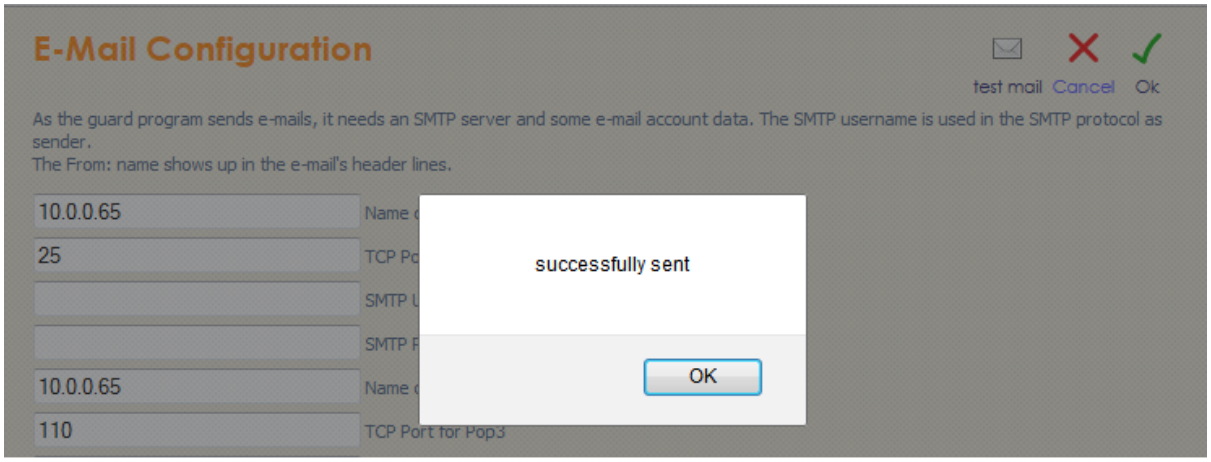
When all the settings are entered, the SMTP settings can be validated by clicking the Test Mail icon. Before clicking the test mail button, you first have to click the OK button and then click the Activate button in the configuration home page.



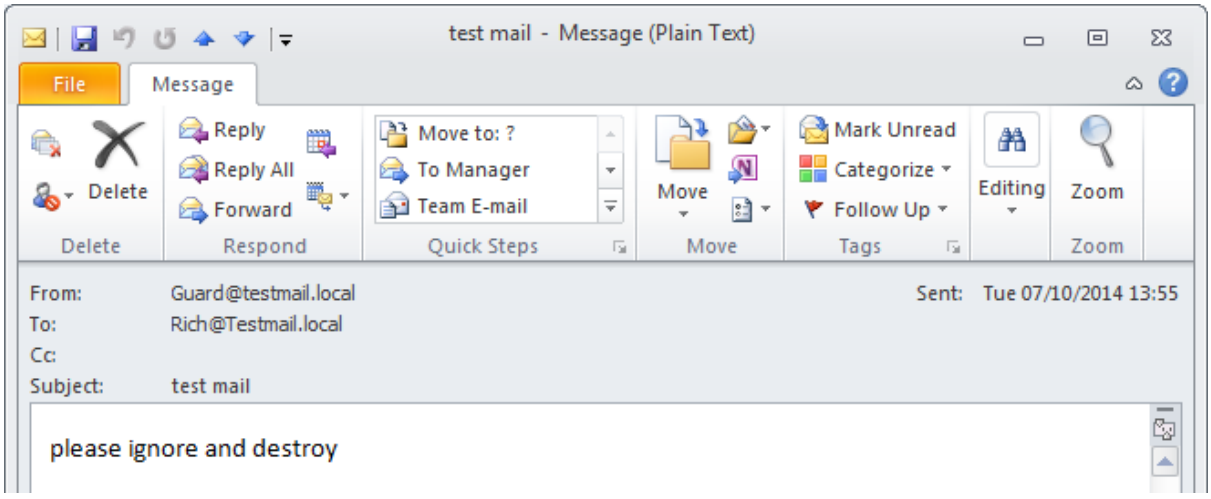
A confirmation message is displayed when the configuration has been successfully activated.



Return to the Email configuration page and click and click the Test Mail button and InGuard will attempt to send an email using the configured details, a message will be displayed saying if the test was successful or not. The test doesn't perform a test on the POP3 settings.



The test email looks like this.

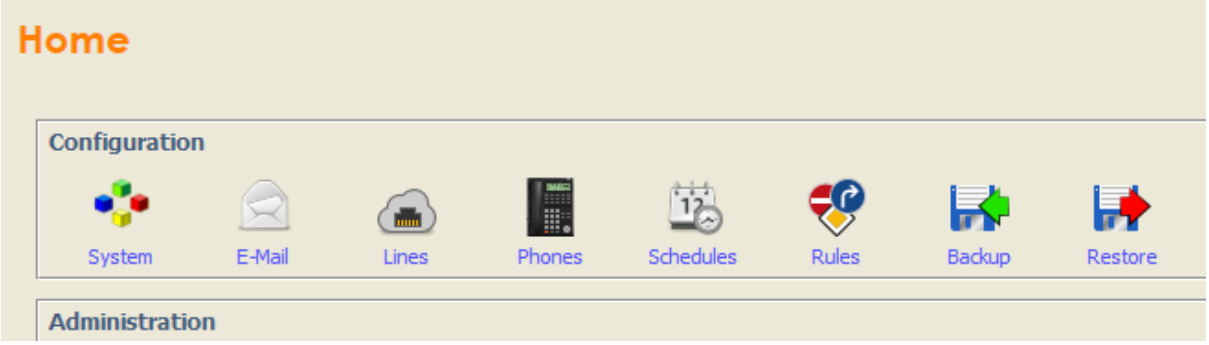


After performing the test, click OK to save the changes and from the home page, click the Activation button to save the changes to the Email configuration.

For Information on using InGuard, refer to the separate User Guide.

Backup and Restore

InGuard's configuration is can be backed up to a file, this is particularly useful if you are intending on making some changes to the configuration and wanted to be able to roll them back.

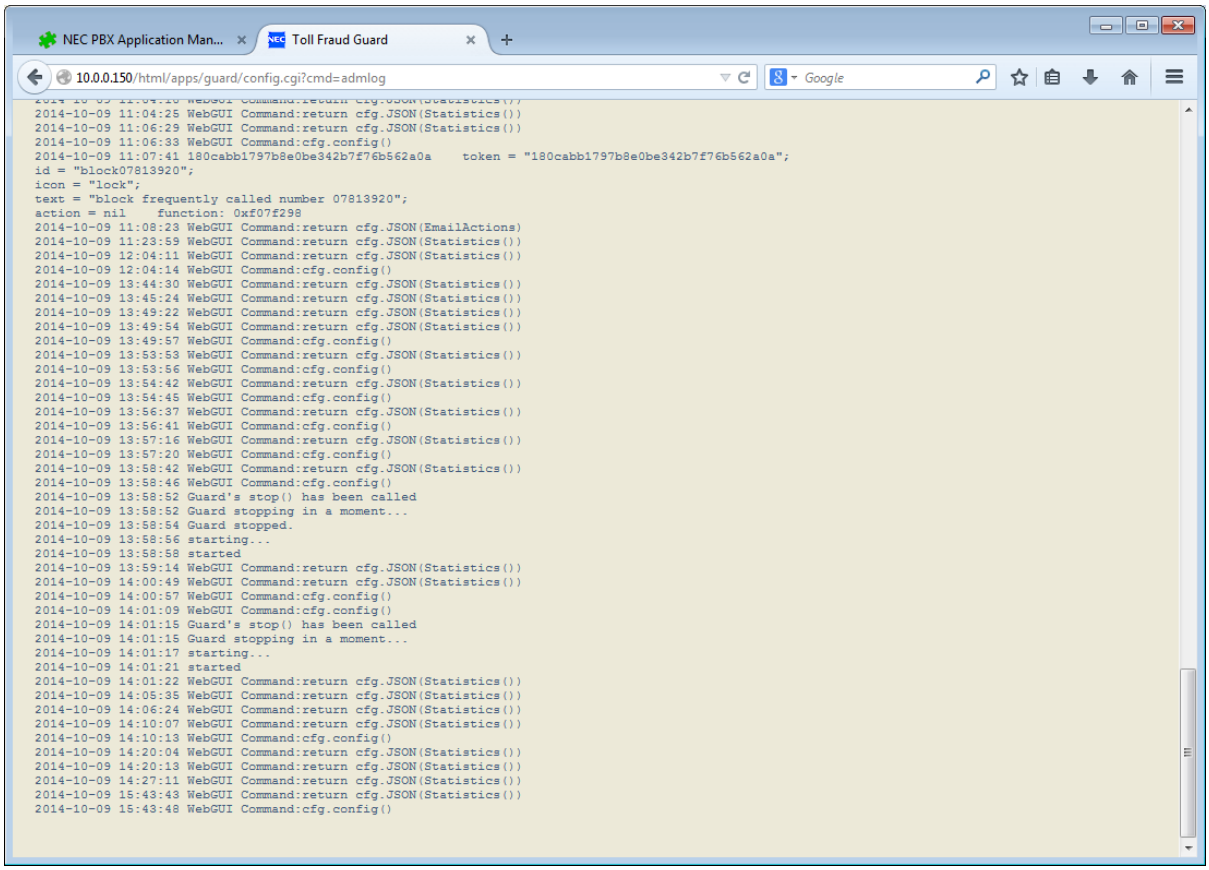


From the home page, click the Backup button and follow the prompts to save the file. The file will be date and time stamped. To carry out a restore from a file, click the Restore button and browse to the backup file.

Log Files

Under Administration menu, there is an option to look at log files.

This keeps a log of when the guard started / stopped and SMDR records that have been processed.

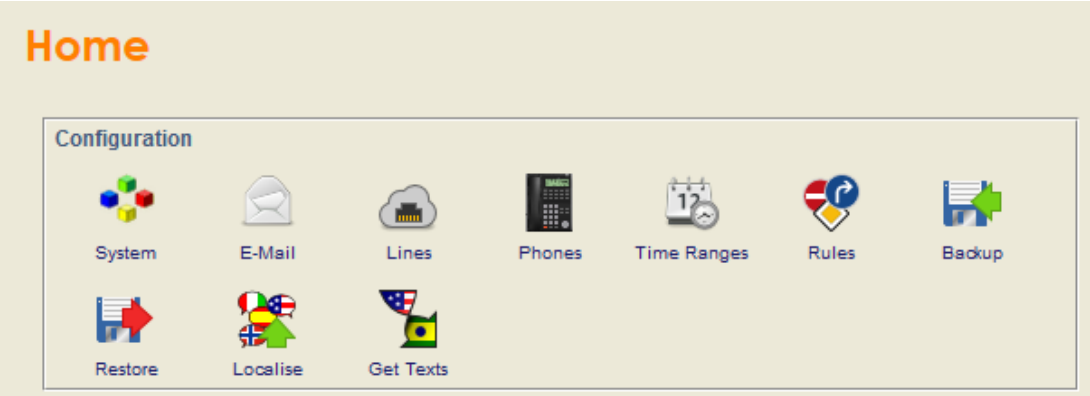


Translating InGuard

The InGuard application can be translated, making the application available to a variety of users. There are three main steps to translating the application:

1. Export the text file from the application.
2. Edit the text file translating the appropriate text. The file that is downloaded is in UTF-8 format, it's important that this file format is maintained else the translated text will not be displayed properly after it's re-imported.
3. Import the translated file.

To begin, click the Get Texts Icon and save the file.



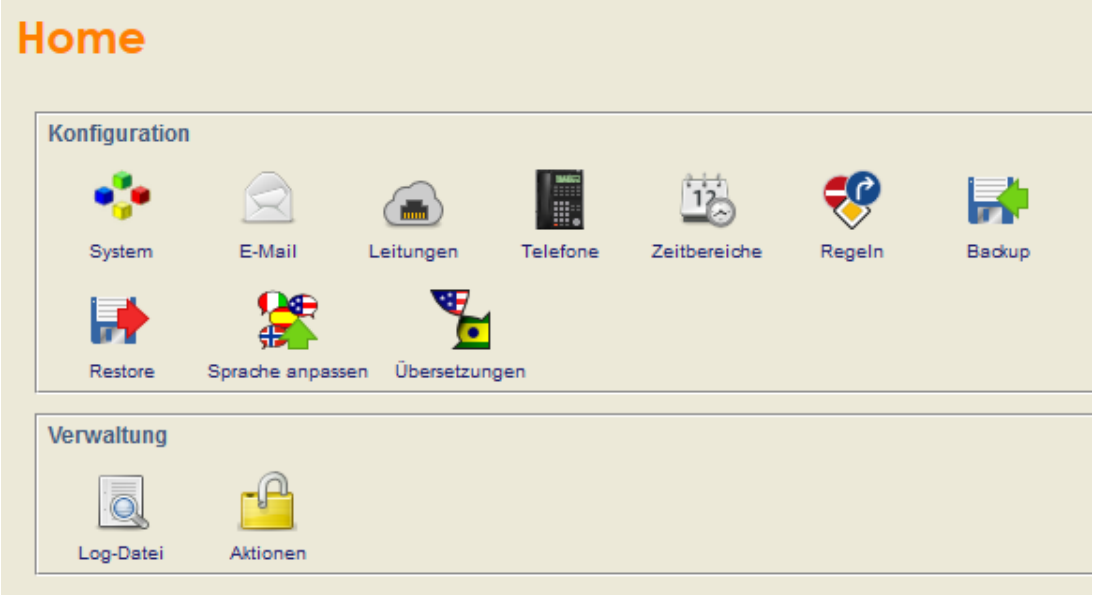
Open the file in a text editor and translate the test that appears between the double square brackets. Two open square brackets [[denote the start of a section for translation and two closed]] brackets the end. Any text between curly braces { } should not be translated. The picture below highlights in red boxes which text should be translated for the opening section.

```
10  -- {cdr.*} will be replaced by appropriate fields from the cdr (call detail record)
11  -- {cfg.*} takes values from the configuration
12  -- {rule.*} references the current applied rule
13  -- {params.*} delivers values from the currently active parameter set
14  --
15  -- DO NOT CHANGE ANYTHING BETWEEN THE {CURLY BRACES}
16  --
17
18  WarnExtensionCallRate =
19  [[
20  Rule "{rule.name}" found that the extension '{cdr.ext}' has made frequent
21  outgoing calls (at least {params.warn} in the last {params.wndw} seconds).
22
23  This is usually an indication for a fraud attempt.
24
25  If you consider this to be a fraud attempt,
26  reply to this email including this code: <#{replycode}#>,
27  and the extension will be blocked by setting it's restriction class to {cfg.DialBlockClass}
28
29  By sending this code: <#{replycode}#> to the guard (simply reply to this mail),
30  you can command the guard application to block the extension '{cdr.ext}', which is
31  done by setting it's restriction class to class #{cfg.DialBlockClass}
32  ]];
```

Here is another example from further down the file:

```
148  Starting =
149  [[
150  The Toll Fraud Guard at {cfg.EmailSiteName} is on guard now.
151  Expect a report every {cfg.EmailReportInterval} seconds
152  ]];
153
154  Stopping =
155  [[
156  The Toll Fraud Guard at {cfg.EmailSiteName} has been shut down.
157  ]];
```

As the words Starting and Stopping fall outside of the square brackets, they should not be translated. Once the file is translated and saved, then click the Localise button in the guard application and browse to the translated file and click OK. The application will refresh and show the translations.

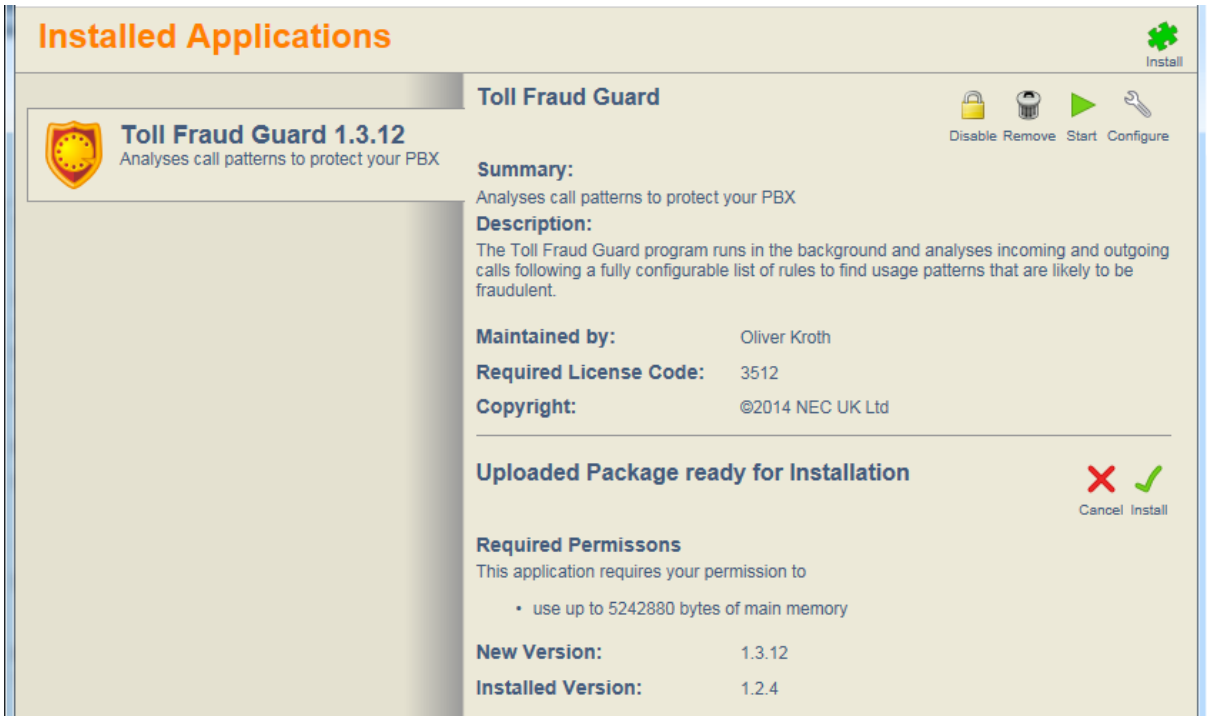


The get texts button can be used to re-export the currently used translation file.

Upgrading InGuard

InGuard can be upgraded to the latest level using the application manager, any existing rules and configuration are persevered during the upgrade. As a precaution it's recommended that you perform a backup of InGuards configuration and note the version number that is installed. Details on how to perform a back can be found in the Backup and Restore section of this manual.

Before commencing the upgrade process, the InGuard application should be stopped using the application manager. Once the stopped, click the install button in the upper right side of the application manager. Browse to the version of the guard that you want to install and click OK. To proceed with the upgrade, click the install button.



Once the installation has finished then start the application again. The new version number will be displayed on the left hand side of the application manager. The application can then be restarted.

InGuard – Software Licence Agreement

PLEASE READ THIS SOFTWARE LICENCE AGREEMENT ("LICENCE") CAREFULLY BEFORE USING THE INGUARD SOFTWARE. BY USING THE TOLL FRAUD GUARD SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENCE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENCE DO NOT USE THE SOFTWARE.

1. The Definitions

1.1. “Licence” means this Software Licence.

1.2. “Customer” means Software User.

1.3. “Software” means all INGUARD Software, the subject of this Licence, including (a) the accompanying documentation and any Updates and (b) any Upgrades purchased by the Customer or provided by NEC at no cost pursuant to §5.2 below.

1.4. “Update” means minor Software release the primary purpose of which is to remove incompatibilities, apply corrections, enhance the stability or remedy technical faults in the Software.

1.5. “Upgrade” means major Software release the primary purpose of which is to add new functionality or enhance the performance of the Software.

2. The Licence

2.1. NEC grants the Customer a limited, non-exclusive, non-transferable, non-sub licensable Licence to use the Software, subject to the following conditions:

2.1.1. The Software may only be used on the System upon which it is first installed. Consent must be obtained beforehand if the Software is to be used on a different System.

2.1.2. The Software may not be copied except for internal back-up purposes.

2.1.3. The Software may not be modified, de-compiled, disassembled, reverse engineered, merged or de-coded in any manner whatsoever.

2.1.4. The Software shall be maintained in safe custody. Any unauthorised use, reproduction, distribution or publication of the Software must be prevented. If the Software comes into the possession of a third party NEC must be notified immediately.

2.1.5. This Licence is personal to the Customer. The Software or a copy thereof shall not be loaned, rented, leased, licensed, assigned or otherwise transferred. The Customer acknowledges NEC’s proprietary rights to the Software. No title or ownership to the Software is transferred. The Software shall not be used in any manner that would derogate from NEC’s proprietary rights in the Software. The Software is protected by applicable copyright laws and international treaty provisions.

2.1.6. The Software, including documentation relating thereto, contains confidential information. Such information shall not be disclosed to any third party, other employees or authorised agents of the Customer, without NEC’s prior written consent.

2.1.7. The use of the Software shall be supervised and controlled in accordance with the terms of this Licence. The Customer shall ensure that its employees, subcontractors or agents who have authorised access to the Software are made aware of the terms of this Licence and comply therewith. The Customer shall maintain safe custody of the Software.

2.1.8. The Customer shall permit NEC during NEC normal business hours to audit use of the Software and verify its compliance with the above conditions.

3. Copyright

3.1. The Customer acknowledges that the Software and documentation are protected by European and International copyright laws. The Customer shall not, during or at any time after the expiry or termination of this Licence, permit any act that infringes that copyright. The Customer expressly agrees that it shall not copy the Software except for back-up purposes pursuant to §2.1.2, or distribute, modify, publicly display or publicly perform the Software.

3.2. Ownership: This is a Licence to use the Software. It is NOT an agreement for the sale of the Software. All worldwide ownership of and all rights, title and interest in and to Software, and all copies and portions thereof, including without limitation, all copyrights, patent rights, trademark rights, trade secret rights, inventions and other proprietary rights therein and thereto, are and shall remain exclusively in NEC and its licensors. The Customer's rights to use the Software are specified in this Licence, and NEC retains all rights not expressly granted to the Customer in this Licence.

4. Limited Warranty

4.1. Subject to §4.2 through 4.7, NEC warrants that for ninety (90) days from the purchase date of the Software, it will perform according to its specifications.

4.2. NEC shall repair or replace Software subject to a valid warranty claim made within the warranty period, either on-site or off-site, at NEC's discretion and during normal business hours. If the Customer asks NEC to provide services outside its normal business hours, it shall be charged for such services at NEC's standard after-hours rates. If it is not possible to repair or replace the Software, the Software licence fee shall be refunded. The remedies described in this §4.2 shall be NEC's sole obligation and the Customer's sole remedy in the event Software fails to perform according to its specifications during the warranty period. For support purposes, the Customer shall permit remote access to the Software, during normal business hours, upon request for support. The Customer recognises that NEC's ability to support the Software is dependent upon the Customer providing this remote access.

4.3. Because there is such a diverse range of telecommunications environments, NEC cannot warrant that the Software will be compatible in every operating environment. It is the Customer's responsibility to ascertain whether its own operating environment is compatible with the Software.

Any Software modifications which NEC may agree to make to achieve compatibility shall be at its prevailing rates and charges. NEC does not warrant that the Software will meet the Customer's requirements or that its operation will be uninterrupted or error-free. NEC does not warrant that the Software is free of errors or defects. The existence of such Software errors or defects shall not constitute a breach of this warranty. Notwithstanding the foregoing NEC shall provide the Customer with Software corrections for known errors that also affect NEC's other licensees. NEC excludes, and expressly disclaims, all express and implied warranties of merchantability or fitness for any particular purpose. NEC shall not be responsible for external factors affecting the performance of the Software, including without limitation, telecommunications and network breakdowns, power surges or interruptions and other "Acts of God".

4.4. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL NEC BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES ARISING OUT OF OR RELATED TO YOUR USE OR INSTABILITY TO USE THE NEC SOFTWARE, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF NEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.5. The Toll Fraud Guard is an active call monitoring application that can be used to help prevent toll fraud. It is intended to work by monitoring SMDR output provided by the PBX System and looks for calls that could be deemed fraudulent. When such activity takes place the guard can send email notifications to users informing them of the suspicion in order that they can act quickly on this information. As the application runs on the PBX System it also has the ability to prevent further fraudulent activity from taking place by modifying the PBX System configuration. The Toll Fraud Guard application has been designed to assist in making systems reasonably secure from unauthorised usage and intrusions. However, the Toll Fraud Guard cannot make a PBX system totally invulnerable to fraud or hacking due to other factors involved with the PBX System such as and not limited to system and network programming which has potential to change. NEC disclaims any express or implied warranty that the Toll Fraud Guard will render a PBX System technically immune from or prevent fraudulent intrusions into and/or unauthorised use of those PBX Systems to which the Toll Fraud Guard has been applied. The Customer is hereby warned that fraudulent use of the, including but not limited to DISA, auto-attendant, voice mail, is possible. NEC makes no express or implied warranty against such fraud or hacking, and will not be responsible for consequential, incidental or special costs, including telephone line charges resulting from such activity.

4.6. Some jurisdictions do not allow the exclusion of certain implied warranties or conditions, so the above exclusions may not apply to the Customer. This Licence does not exclude any implied warranties or conditions that may not under applicable law be excluded. In no event shall NEC total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of seventy five pounds (£75). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

Toll Fraud Guard – Software Licence Agreement

4.7. This Licence does not impose any obligations upon NEC to provide support and Software Assurance ("SA") services outside of the warranty period. Should the Customer require such services, they shall be obtained by arrangement with NEC Technical Services.

5. Other Services

5.1. If NEC provides services outside the coverage of its limited warranty or after it has expired, the Customer shall pay for such services at NEC's standard rates and charges, plus travel and accommodation if applicable.

5.2. To fix an error in the Customer's Software, it may be necessary to install an Upgrade containing both version enhancements and bug fixes. During the warranty period, NEC shall provide such Software Upgrade at no cost. After the warranty period, NEC shall provide such Upgrade at its standard price. In addition to the price of such Upgrade, the Customer shall pay us for any services that NEC provides pursuant to §5.1.

6. Termination/Cancellation

6.1. NEC may Terminate/Cancel this Licence if the Customer breaches any condition thereof. If the breach is capable of remedy, NEC shall give the Customer thirty (30) days written notice within which to do so. Otherwise, Termination/Cancellation shall take effect immediately upon the Customer's receipt of NEC's notice.

6.2. The Customer may Terminate/Cancel this Agreement upon forty five (45) days prior written notice to NEC. Upon the date of Termination/Cancellation, the Customer's Licence to use the Software shall be deemed revoked, the customer will no longer be bound by the terms of this Agreement. Payment for the Software remains unaffected by this clause; this clause does not grant any free period of usage.

7. Term of Licence

7.1. This Licence commences upon the Customer's acceptance hereof. It shall continue, in perpetuity, subject to termination by NEC in the event that the Customer breaches any term herein, or by the Customer with written notice as stipulated in §6.2.

7.2. Upon termination/cancellation the Customer or its representatives shall immediately stop using the Software and documentation and shall return, or destroy all copies of the Software and documentation in a manner directed by NEC.

8. Other Clauses

8.1. If NEC foregoes or delays enforcing an obligation or remedy under this Licence, such forbearance or delay shall not result in a waiver or variation of such obligation or remedy. No failure by NEC to insist upon strict performance of any term or condition in this Licence shall constitute a waiver or
variation of such term or condition. Such failure shall not prevent NEC from claiming default or seeking a remedy under this Licence.

8.2. This is the entire agreement between NEC and the Customer. Upon agreeing to the terms of this Licence the Customer agrees that this Licence supersedes prior licensing agreements, both written and verbal for NEC Software.

8.3. This Agreement shall be governed by and construed in all aspects in accordance with the Laws of the jurisdiction in which NEC as the supplier of the Software is geographically based and each party submits to the non-exclusive jurisdiction of the courts in that geographic location.

8.4. The Customer acknowledges that a breach of this Agreement may cause irreparable and continuing damage to NEC for which money damages may be insufficient, and NEC shall be entitled to injunctive relief and/or a decree for specific performance and such other relief as may be proper (including money damages if appropriate). In the event of litigation between NEC and the Customer concerning Software or any other item which is subject to this Agreement, the prevailing party in the litigation will be entitled to recover legal fees and expenses from the other party.

8.5. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms.

8.6. Acknowledgement. **BY INSTALLING SOFTWARE, THE CUSTOMER ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.**

NEC Enterprise Solutions reserves the right to change the specifications, functions, or features at any time without notice.