Orchestrating a brighter world

NEC

InGuard

User Guide

Version 1.0

For InGuard 1.7.0

Contents

Revision History 3
Description 4
Accessing the Application 4
Lines 5
Extensions 7
Time Ranges 8
Rules 9
Blocking Rules 10
Warning Rules 11
Creating Rules 14
Example Rule – Target Number Rate 18
Rule Summary 21
Filtering Rules 22
Rule List 23
Link to InReports 26
System Health Check 27
Backup and Restore 41
Actions 41
InGuard – Software Licence Agreement 42
Revision History 47

Revision History

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

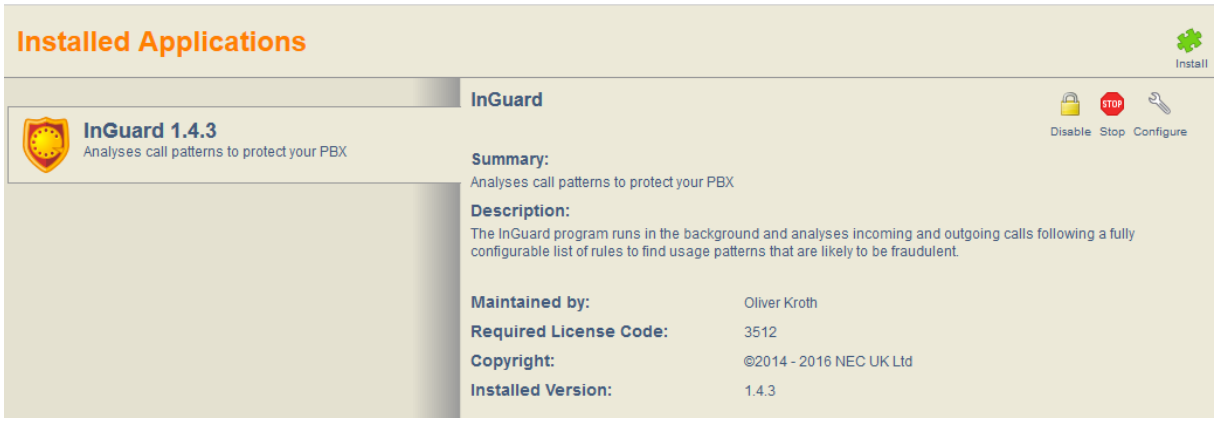
Description

This manual explains how to use the InGuard application. There is a separate installation guide that explains how to install and setup InGuard. Before using the software you must read the InGuard Software License Agreement.

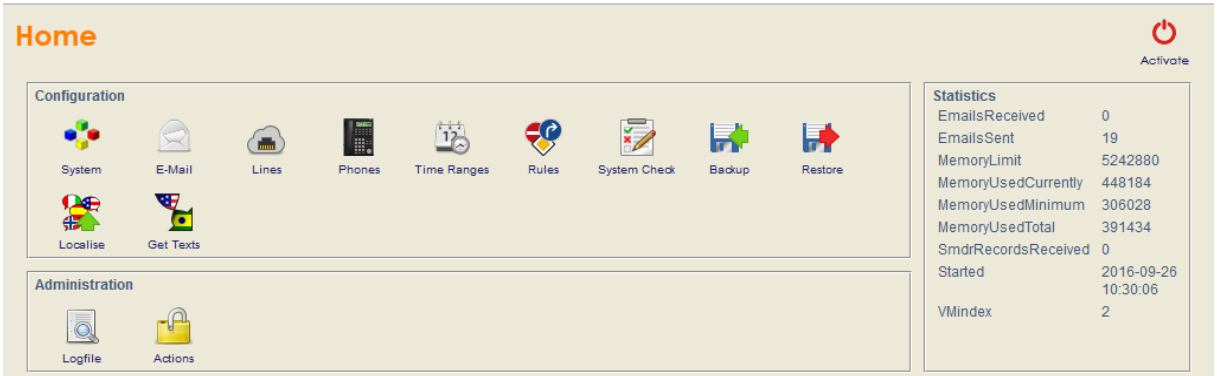
InGuard is configured to send an 'On Duty' email, this is usually sent every 24 hour but can be as frequent as every hour. This can be configured in the email page in the guard. It's important to make sure the On Duty email is being received at the expected time and if it's not then you should investigate to see why it wasn't received.

Accessing the Application

The application can be accessed via the Lua Application Manager Web Page. This will follow the format http://IP Address of the PBX/html/apps/manager.cgi .

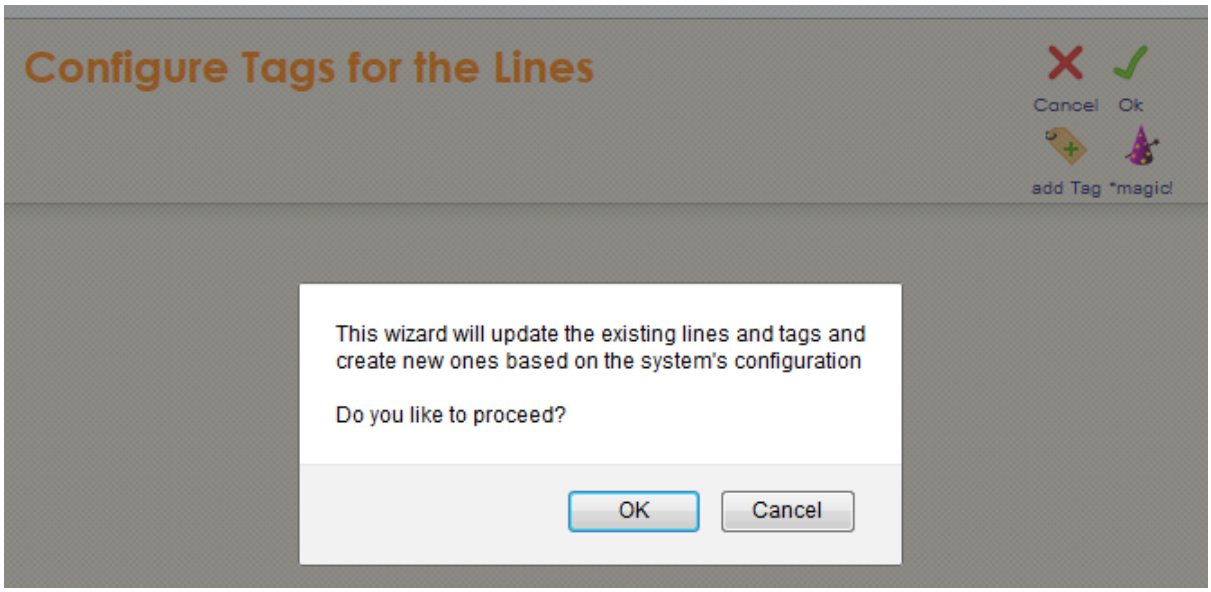


From here you can click the configure button to start using InGuard.

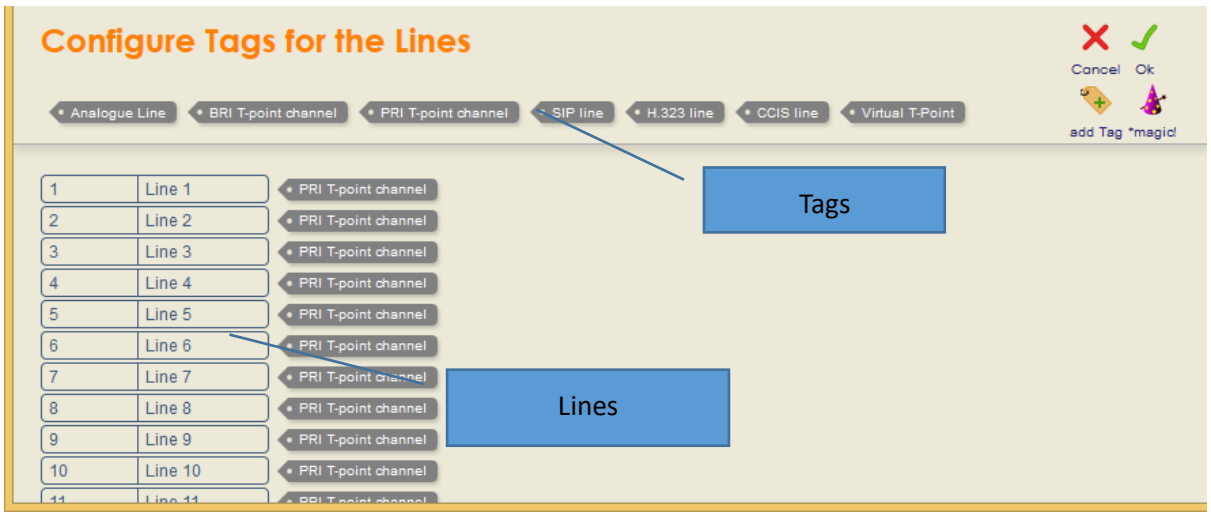


Lines

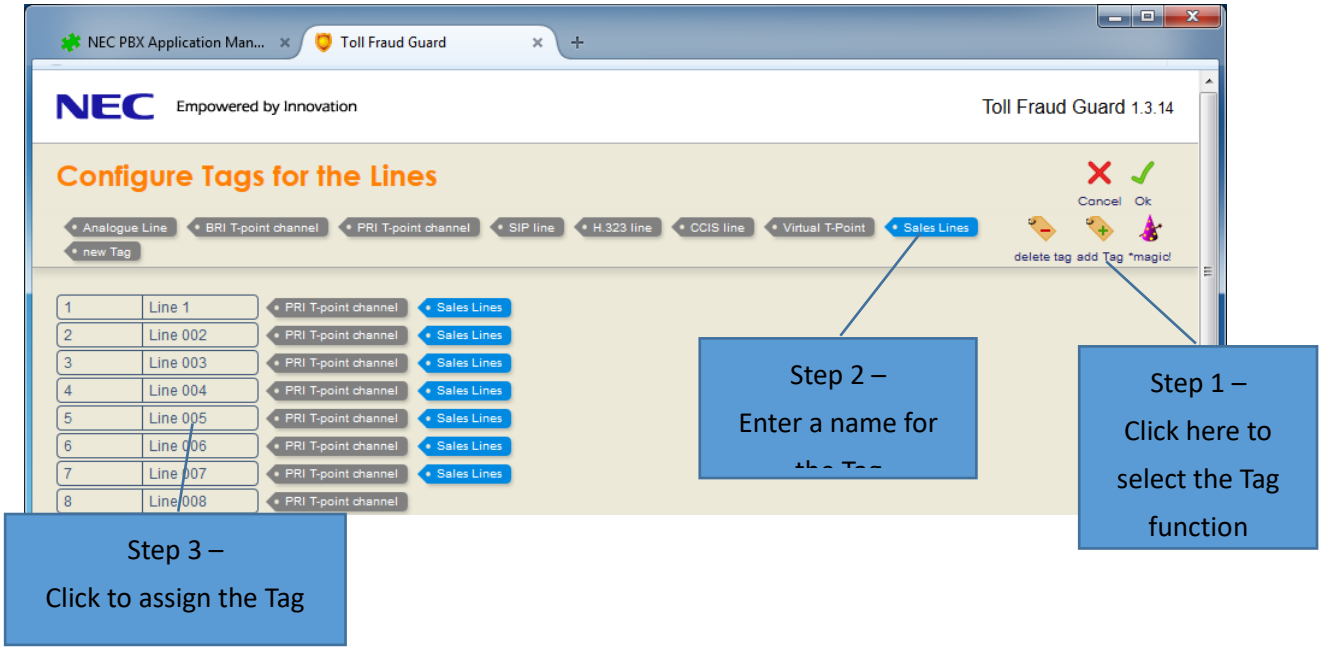
InGuard needs to know what lines (trunks) are connected to the system so it can actively monitor them, from the home page click the Lines button. By default, rules are applied system wide to all lines. It is also possible to create custom groups of lines, these can then be excluded from rules as required. For example some lines may be used for interconnection and don't have access to the PSTN and as a result you don't want InGuard to monitor them. This can be achieved be 'Tagging' line. On a default installation, no lines will be configured, click the Magic button and the Guard will look at the PBX's configuration and display and lines connected to the system.



A warning box will appear, click OK to continue. The lines that have been detected will be displayed in a column on the left hand side and any tags are displayed at the top. There is several default Tags available, you can click on them and they indicate which lines they are associated with.



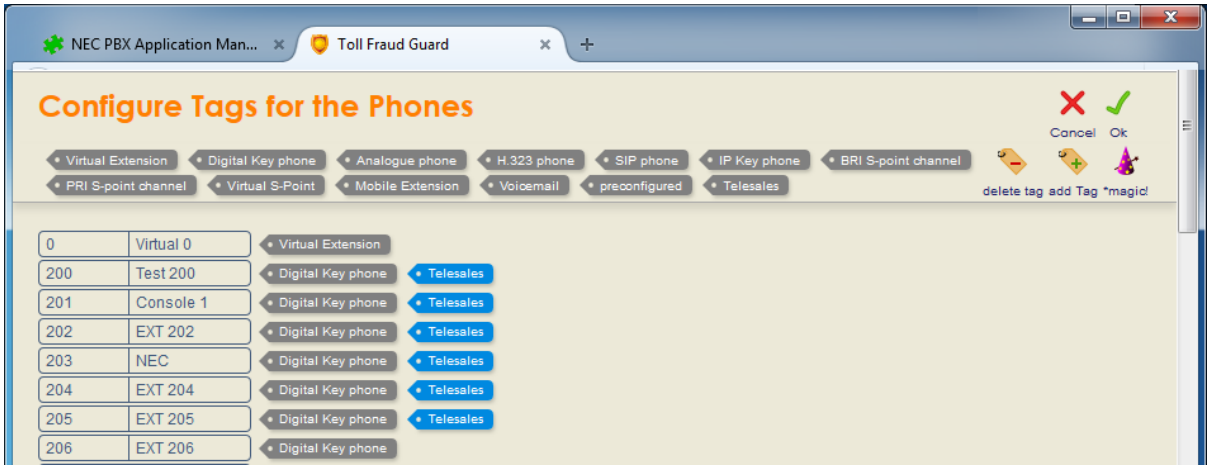
To make a user defined group of lines, click ‘add tag’ (Step1 below), name the tag (Step 2 below) and select which trunks are associated with it (Step 3 below.)



When a line has been assigned to a tag then it’s displayed on the right hand side, to remove a tag from a line just double click on it. Any of the tags including the default one can be deleted by selecting them and clicking on the delete tag button.

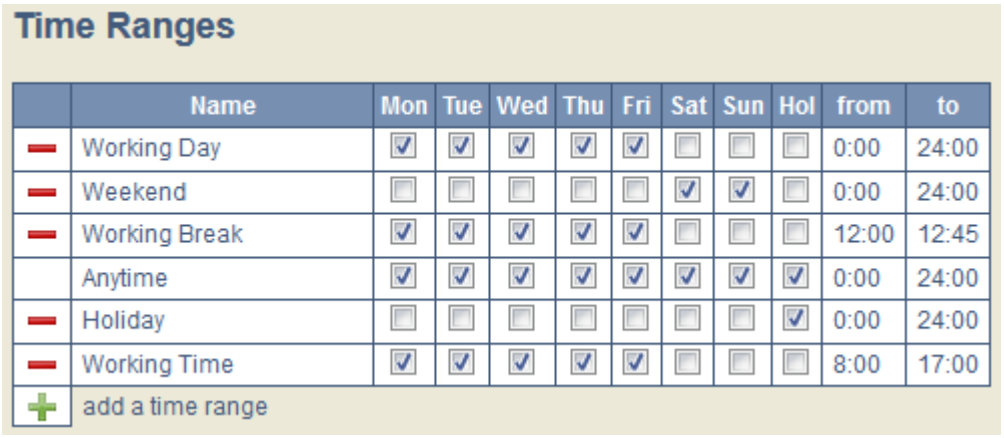
Extensions

Extensions are configured in a similar way to lines, from the home page click the Phones button and then click Magic. The extensions along with the default tags are listed and custom tags can be added as required. The purpose of adding extension based tags is to allow for different expected call rates for different groups of extensions.



Time Ranges

Time Ranges are used alongside rules to allow the guard to cope with different expected call rates at different point across the week. For example, it may be normal for 10 international calls to be made per hour during normal Working Time. At the weekend the expected call rate could be far lower.

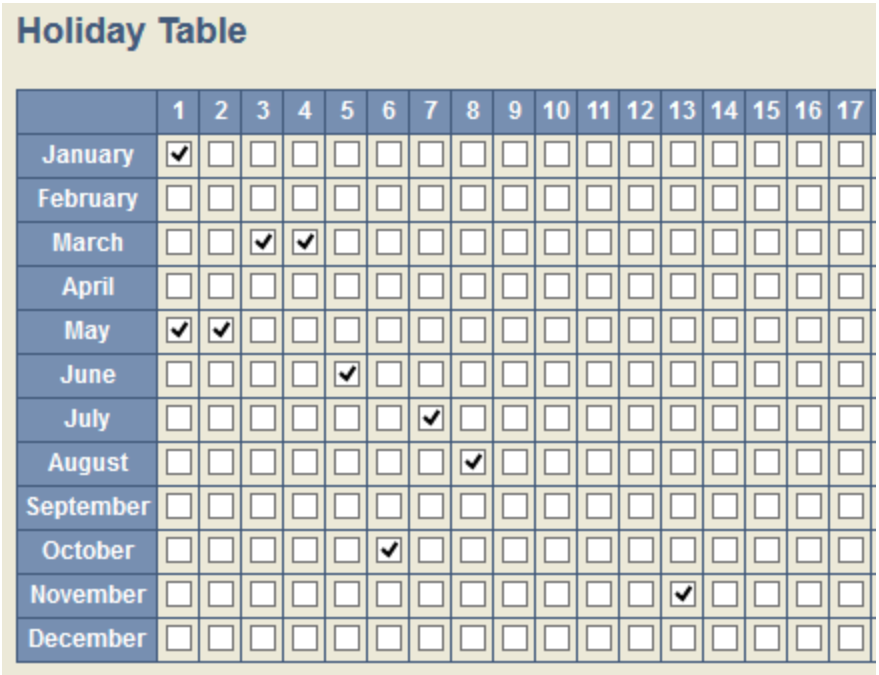


Time Ranges

	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Hol	from	to
−	Working Day	☑	☑	☑	☑	☑	☐	☐	☐	0:00	24:00
−	Weekend	☐	☐	☐	☐	☐	☑	☑	☐	0:00	24:00
−	Working Break	☑	☑	☑	☑	☑	☐	☐	☐	12:00	12:45
	Anytime	☑	☑	☑	☑	☑	☑	☑	☑	0:00	24:00
−	Holiday	☐	☐	☐	☐	☐	☐	☐	☑	0:00	24:00
−	Working Time	☑	☑	☑	☑	☑	☐	☐	☐	8:00	17:00
+	add a time range										

The existing Time Ranges can be modified by clicking in the appropriate area and entering values as required. They can also be deleted by clicking the red – sign and new ones added by clicking the + sign. Any entries that do not have the red minus sign next to them are already assigned to a rule.

It's also possible to create a time range that is applied to specific day of the year. This is particularly useful when there is a public holiday and you would expect a lower call rate on that day. If the site has been upgraded from an older version of InGuard then the Holiday time range will need to be added as shown above.



Holiday Table

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
January	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
February	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
March	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
April	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
May	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
June	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
July	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
August	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
September	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
October	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
November	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐
December	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

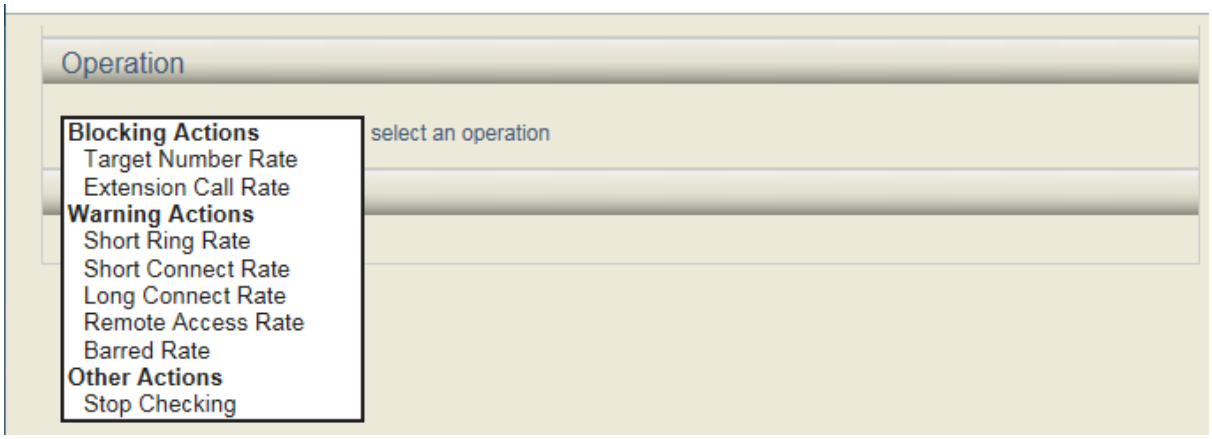
Rules

Once InGuard is configured then different rules can be applied to trigger notifications. Rules by default are system wide for all telephone numbers, all trunks, all extensions and DDI numbers. They are also created against a time range allowing different thresholds to trigger rules based on the time of day and day of the week.

The rules that can be created are categorised based on the action that they perform;

- Blocking Actions – When configured these rules have the ability to either restrict an extension from dialling out or to bar a number from being able to be dialled.
- Warning Actions – When configured these rules will report the suspicious behaviour to the configured email addresses.
- Other Actions – This allows certain calls to be ignored by the Guard.

When creating the rules you select the required rule from the drop down menu.



Blocking Rules

The available blocking rules are the Target Number Rate and Extension Call Rate, using different 'Time Ranges' it's possible to cope with different expected call rate during office hours and out of office hours.

Target Number Rate	
Target Number Rate rules look for repeated outbound calls from any extension to the same number, this is a common symptom of Toll Fraud. The guard looks only at the first 8 digits that are dialled and not the complete number, this way the Guard can catch dialling patterns for similar numbers.	
Configuration:	
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of calls to the same number that will trigger the warning email
Block	The number of calls to the same number that will trigger the automatic blocking action.
Action(s):	
When the warning email is triggered the user can reply to the email to block the number from being dialled.	
When the Block action is triggered, the number is automatically blocked by adding it to the Restrict Table in the PBX and an email is sent to the user. The user may reply to the email to un-block the number.	
The alerts can also be responded to using the 'Actions' page, you could do this for example if you didn't have access to email.	

The Target number rate can also block calls to all numbers when the restrict table is full. When this is activated, **all** numbers (except for explicitly allowed numbers) are blocked from dialling, this is done by putting numbers 0-9 in the restrict table. The intention of this feature is to provide effective protection when the restrict table becomes full and as a result InGuard wouldn't be able to take action. If this mode is ever activated then the installer or maintainer of the PBX should investigate why so many numbers are entered in the restrict table and see if the number in there could be entered in a more efficient way.
When a blocking action is attempted and the restrict table is full, InGuard will send an email stating that the restrict table is full. An email will be sent saying all calls have been blocked, the user will be able to reply to the email to reverse the action and restore the previous entries into the restrict table.

InGuard can also make sure that any changes it makes are 100% effective, it does this by monitoring to see if calls further calls are made to destination numbers that it has barred. If further calls are made then InGuard will report that the Toll Restriction action may have been ineffective. There is an option to reply to the email to block all numbers apart from emergency numbers. By replying to the email InGuard will enter all numbers into the assigned restrict table.

Extension Call Rate	
A higher than expected call rate is another common symptom of Toll Fraud. If an extension on a PBX had been compromised then a hacker could make many calls over a period of time. The extension call rate rules allow you to enter the expected call rate for an extension and if that rate is exceed an alert can be triggered. **Voicemail Ports can often have a lower expected call rate so its good practice to create separate rules with lower warn and block limits specified.**	
Configuration:	
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of outbound calls that will trigger the warning email
Block	The number of calls outbound calls that will trigger the blocking action.
Action(s):	
When the warning email is triggered the user can reply to the email to move the extension to the configured Toll Restriction Class.	
When the Block action is triggered, the extension is automatically moved to the configured Toll Restriction Class. The user may reply to the email to undo the action, they will be moved back to their original Toll Restriction Class.	
The alerts can also be responded to using the 'Actions' page, you could do this for example if you didn't have access to email.	

Warning Rules

Warning Rules can be configured to alert the users to suspicious behaviour, they cannot perform any blocking actions. All the warning rules are described here:

Short Connect Rate	
If a hacker has taken control of some extensions on a PBX then they may attempt to make several short outbound calls to see what types of calls they can make. They may wish to establish if they can make International or Premium rate calls in preparation for making a mass of expensive calls. The Short Connect Rate rule can identify this type of behaviour.	
Configuration:	
Max	Enter the maximum length of a call in seconds. Calls less than this duration will be counted as a Short Connect Call.
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of calls to trigger the rule.
Action(s):	
An email is sent informing the user that the rule has been triggered, there is no blocking action available for this rule.	

Long Connect Rate

If a PBX has been compromised then often many long calls will be made that can typically incur lots of expense. Long Connect Rate can be used to identify if there is a suspicious amount of long calls. The Long Connect Rate rule can identify this type of behaviour.	
Configuration:	
Min	Enter the minimum length of a call in seconds. Calls longer than this duration will be counted as a Long Connect Call.
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of calls to trigger the rule
Action(s):	
An email is sent informing the user that the rule has been triggered, there is no blocking action available for this rule.	

Barred Rate

If a call is made to a number that is barred in PBX's, then an SMDR record is output by the system. If there are several of these calls are made, it could indicate that someone is trying to make fraudulent calls.	
Configuration:	
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of calls to trigger the rule
Action(s):	
An email is sent informing the user that the rule has been triggered, there is no blocking action available for this rule.	

Short Ring Rate

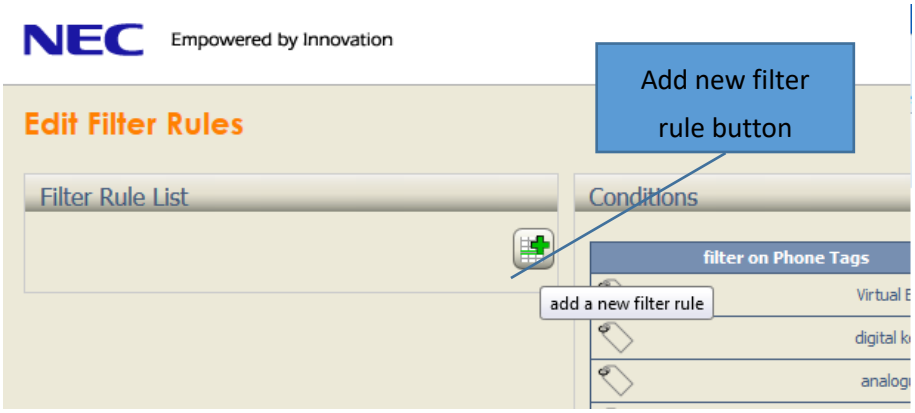
A hacker may try call many different DDI's numbers belonging to a customer. The idea being they will ring each DDI number for a few seconds to see if the call is answered by voicemail. If a call is answered by voicemail then they may try to compromise the voicemail box. The Short Ring Rate rule can detect a number of abandoned calls with a short ring rate over a period of time.	
Configuration:	
Max	Enter the maximum ring duration.
Wndw	Enter the number of minutes over which the rule will check for calls.
Warn	The number of calls to trigger the rule. For the rule to be triggered the calls must be on different DDI numbers.
Action(s):	
An email is sent informing the user that the rule has been triggered, there is no blocking action available for this rule.	

Remote Access Rate	
A hacker may try and dial into the remote access mode on a PBX in an attempt to compromise its security. The Remote Access Rate rule can detect this type of activity and report it.	
Configuration:	
Max	Enter the number length of a failed remote access attempt in seconds. Calls shorter than this duration are counted as a failed attempt.
Wndw	Enter the number of minutes over which the rule will check for dial remote access attempts.
Warn	Enter the number dial in attempts to trigger the alert.
Action(s):	
An email is sent informing the user that the rule has been triggered, there is no blocking action available for this rule.	

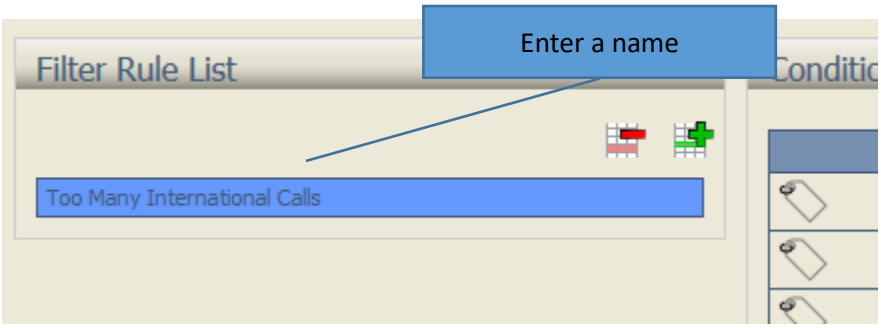
Stop Checking
Stop Checking is a rule that can be defined to prevent the Guard from looking at certain call types.
Configuration:
Only Filtering Conditions are applied to this alarm and no direct actions are associated with this, details on filtering rules are available in Filtering Rules.

Creating Rules

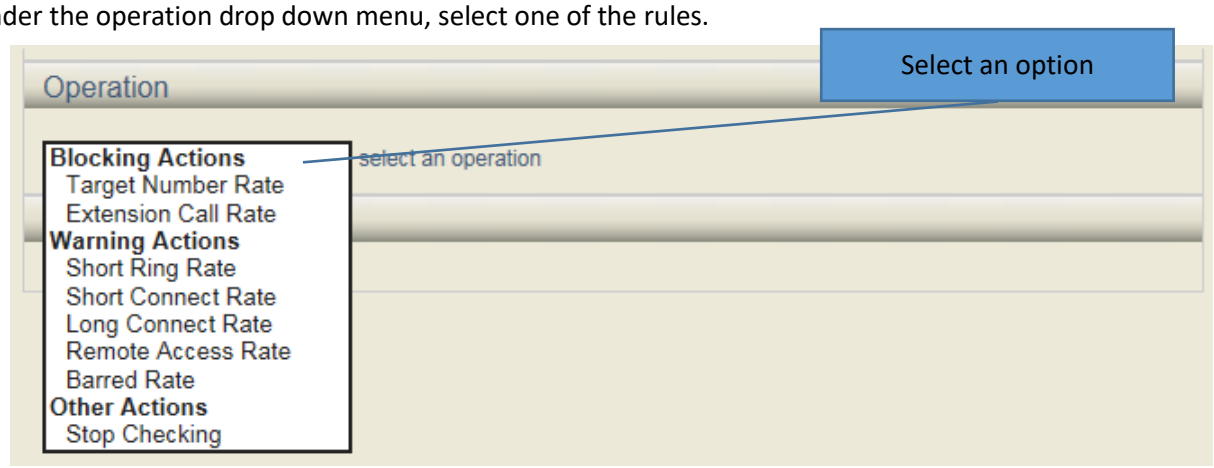
To create a rule, click the Rules button on the home page and click the green ‘add new filter rule’ button.



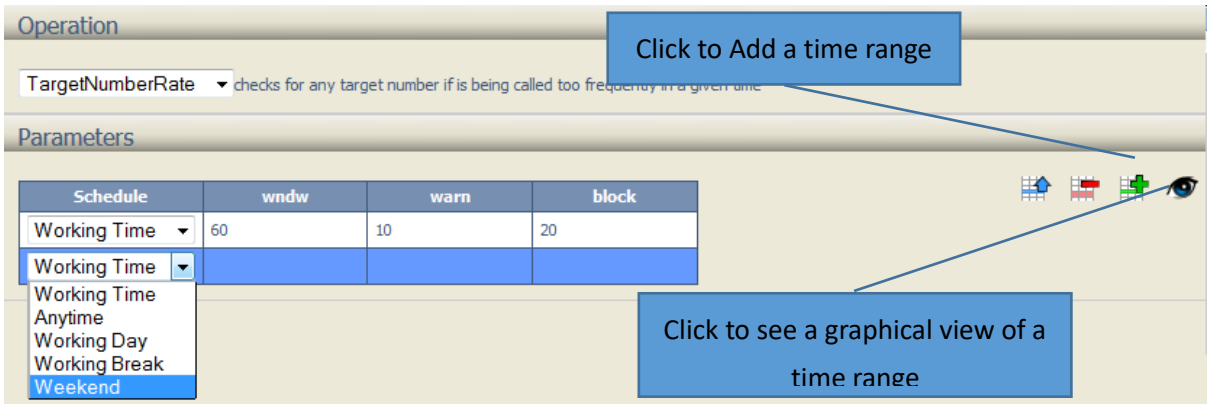
A rule will be created, double click in the box and enter a meaningful name for it. The text entered here will be displayed in any emails that are generated.



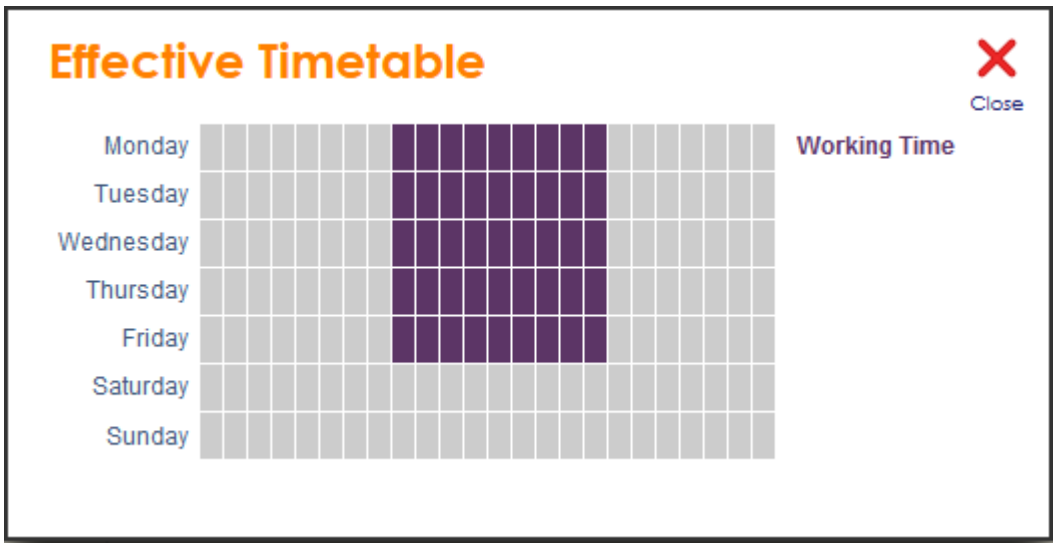
Under the operation drop down menu, select one of the rules.



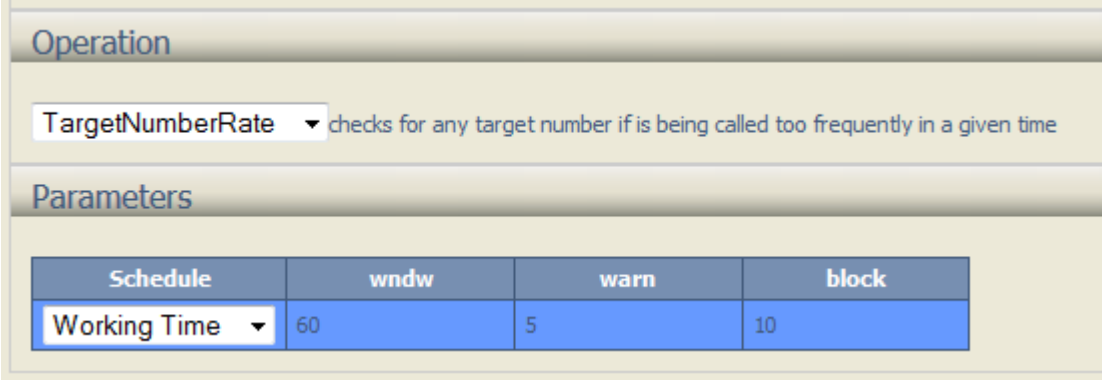
Once a rule has been selected then it has to be applied to a time range, the time range can be selected in the drop down menu. To add multiple time ranges, click the green plus icon and select different time ranges as required.



You can see a graphical view of when the time ranges are effective showing each hour of the day and each day of the week by clicking on the eye icon.



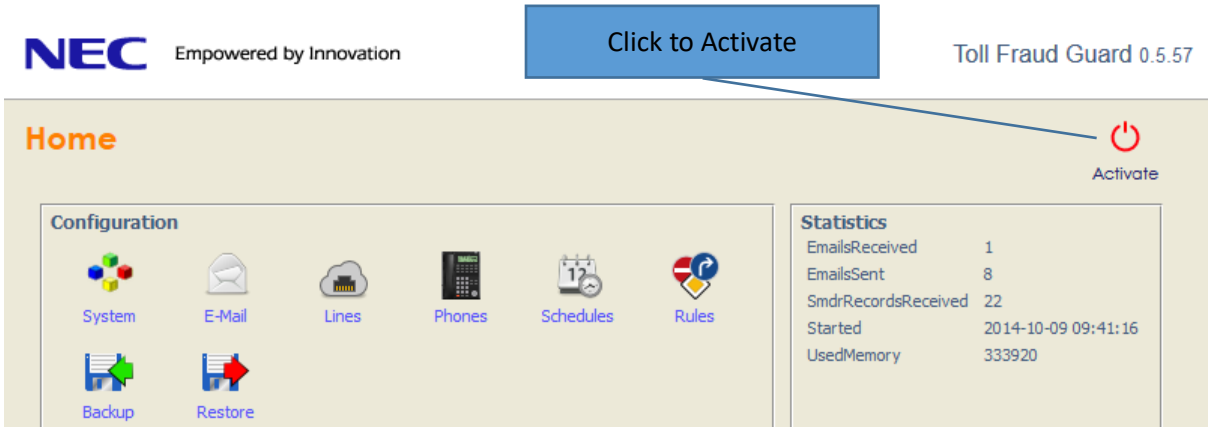
Once time ranges have been added, then the parameters have to be set to trigger the alert. The configurable parameters are different for each of the rules, this example is a TargetNumberRate. TargetNumberRate will monitor for calls by any extension to the same number. The blocking action for this alarm is to stop the number from being dialled by putting it into a restrict table in the PBX.



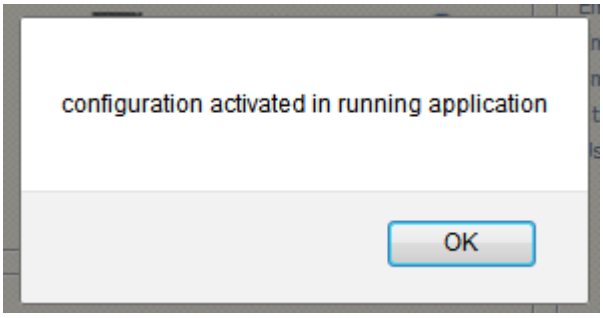
The three parameters that can be set for this:

Setting	Data
Wndw	The Time Period in minutes to monitor calls for this alert. The example above is set to 60 minutes.
Warn	The number of calls during the time period to trigger the warning email. When the warning threshold is reached, an email is triggered to the user telling them about the suspicious behaviour. The user can reply to the email to block the dialled number the triggered the alert.
Block	The number of calls during the time period to trigger the automatic block action. Once the threshold is reached the number will be automatically blocked from dialling. The user will receive an email telling them that the number has been blocked. They can reply to the email to undo the action.

Before the rule will be active, it has to be applied to the InGuard running configuration. To do this, click the OK button in the Rules page to save any changes. From the home page click the Activate button in the upper right hand corner.

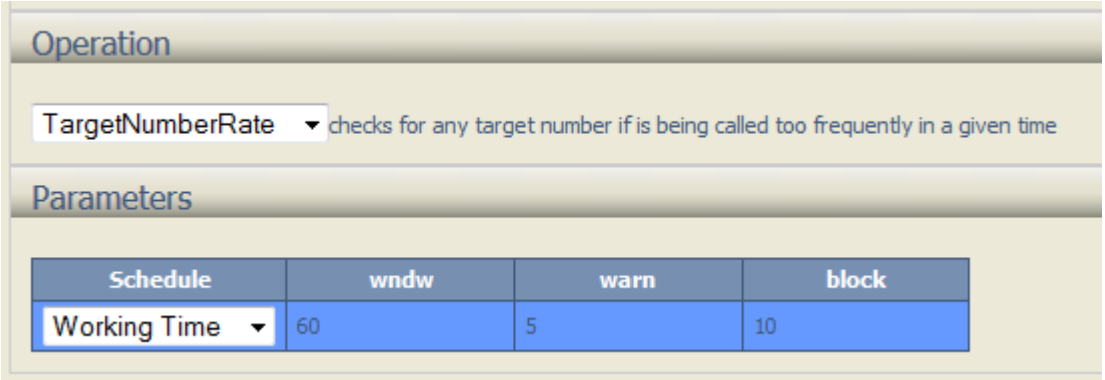


A confirmation message will be displayed when the configuration is activated.

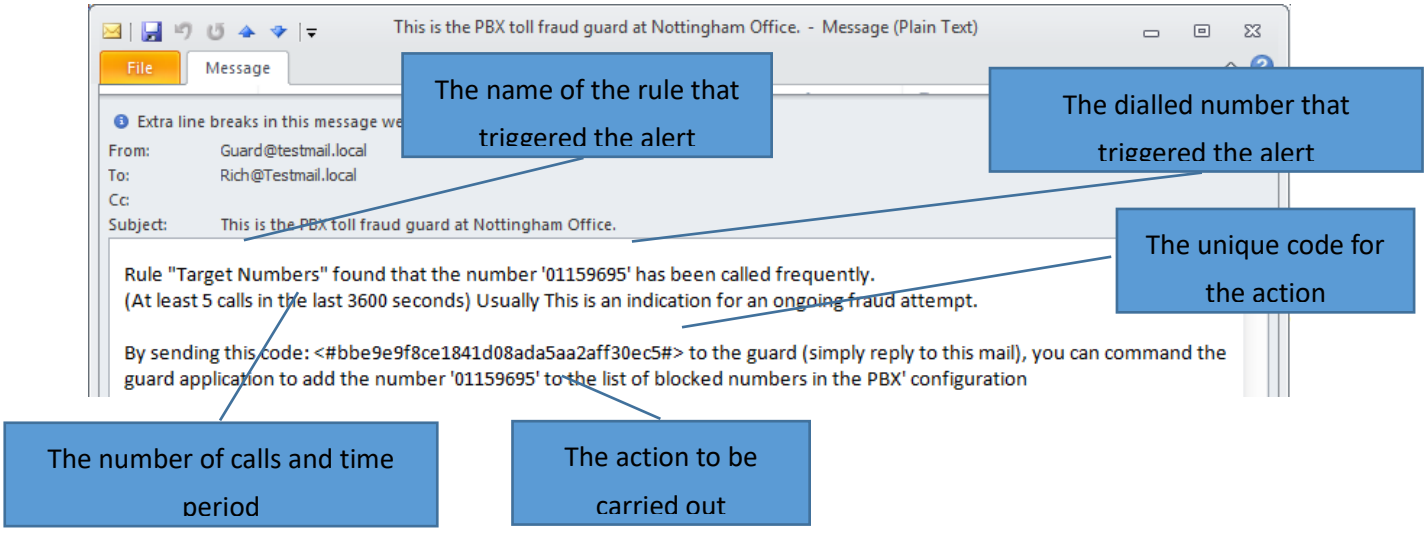


Example Rule – Target Number Rate

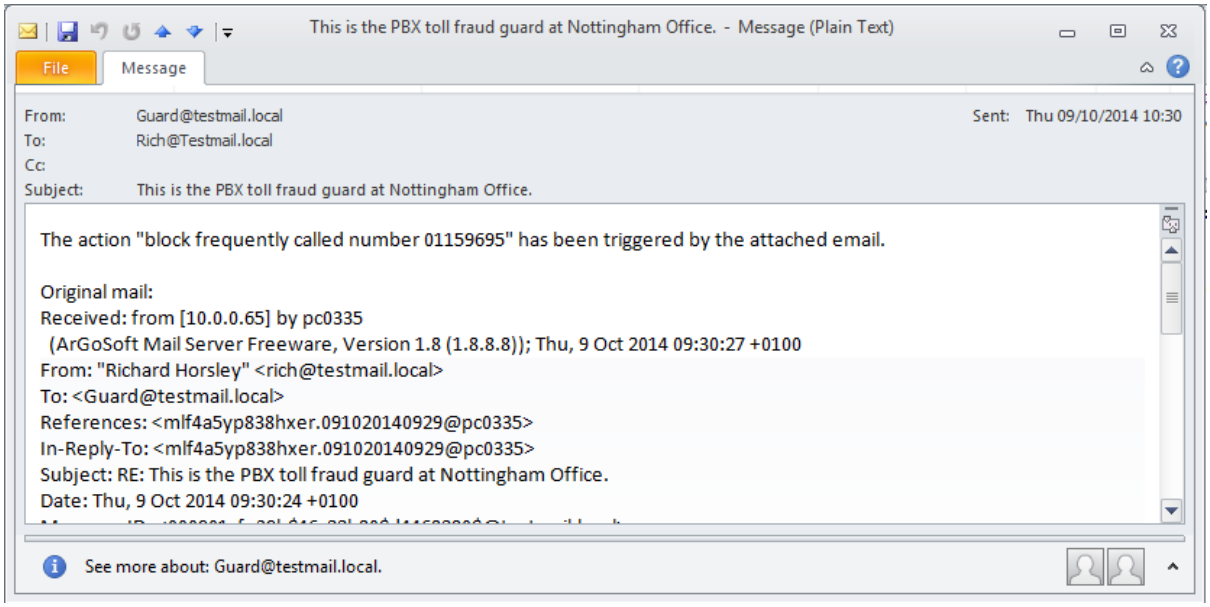
This is an example of how the Target Number Rate rule works. If the rule was configured as shown in the screenshot below, then during the 'Working Time' time range if 5 calls were made to the same number during a 60 minute period, then the warning action would be triggered, this would generate an email.



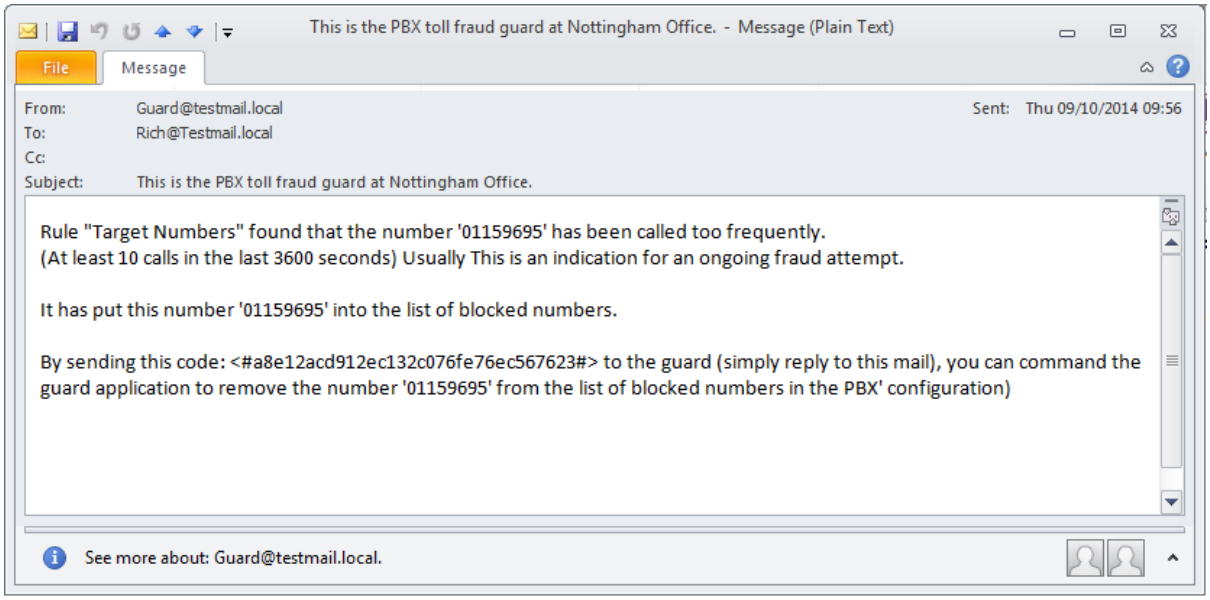
The email will provide a summary of what triggered the alert and what actions can be taken. For the Target number alert, the action is to reply to the email to block the number form being dialled again.



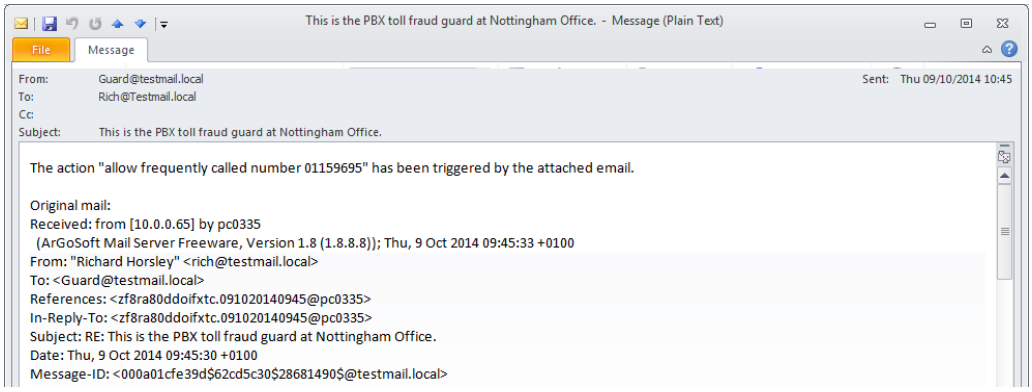
When you have replied to an email to carry out a blocking action, the guard will carry out the action and send a confirmation email.



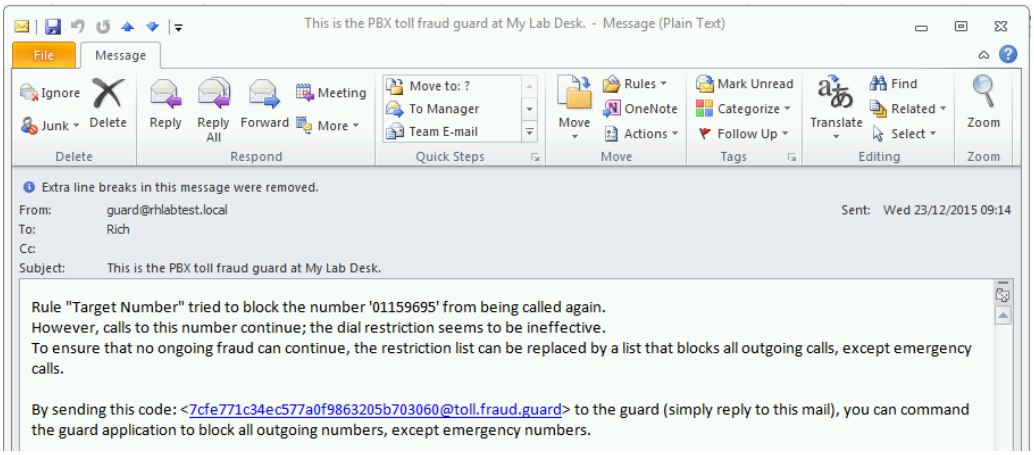
If the user hadn't responded to the warning email, when the block threshold is reached at 10 calls the email is slightly different, it will confirm that the number has been automatically blocked. The will give the user the option to reply to the email to unblock number.



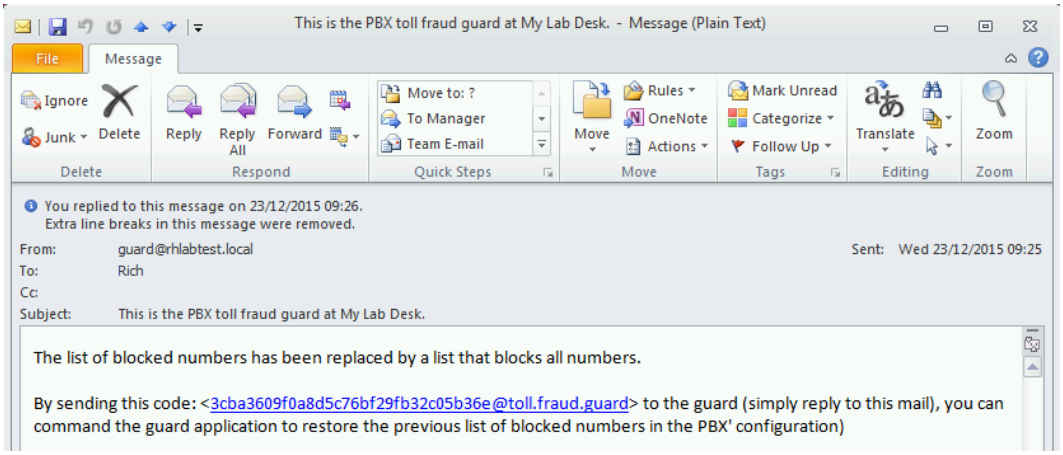
If you reply to the email, the action will be undone and a confirmation will be sent.



Once InGuard has blocked a number from being dialled, it will continue to monitor to see if any further calls are made to this destination. If further calls are made then InGuard will report that the Toll Restriction action may have been ineffective. There is an option to reply to the email to block all numbers apart from emergency numbers. By replying to the email InGuard will enter all numbers into the assigned restrict table.



Once the action has been carried out then a confirmation email will be sent.



To undo the action and restore the previous list of blocked number, reply to the email.

Rule Summary

The different rules that are available apply to specific call types, the table below indicates all the rules and what call type they apply to.

Rule	Outgoing Calls	Incoming Answered Calls	Incoming Abandoned Calls
Stop Checking	✓	✓	✓
Target Number Rate	✓		
Extension Call Rate	✓		
Short Connect Rate	✓		
Long Connect Rate	✓		
Barred Rate	✓		
Remote Access Rate		✓	
Short Ring Rate			✓

Each rule has its own set of values that are used to define when the alert is triggered.

Rule	Min	Max	Wndw	Warn	Block
Target Number Rate			✓	✓	✓
Extension Call Rate			✓	✓	✓
Short Connect Rate		✓	✓	✓	
Long Connect Rate	✓		✓	✓	
Barred Rate			✓	✓	
Short Ring Rate		✓	✓	✓	
Remote Access Rate		✓	✓	✓	
Stop Checking					

Min means the minimum value to trigger an alert, for example you might need to specify the minimum call duration.

Max means the max value to trigger an alert, for example you might need to enter a maximum call duration, or maximum number of calls.

Wndw mean the time period over which to check in minutes, for example a 60 minute period to check for calls may be specified.

Warn is usually the number of calls to trigger a warning email.

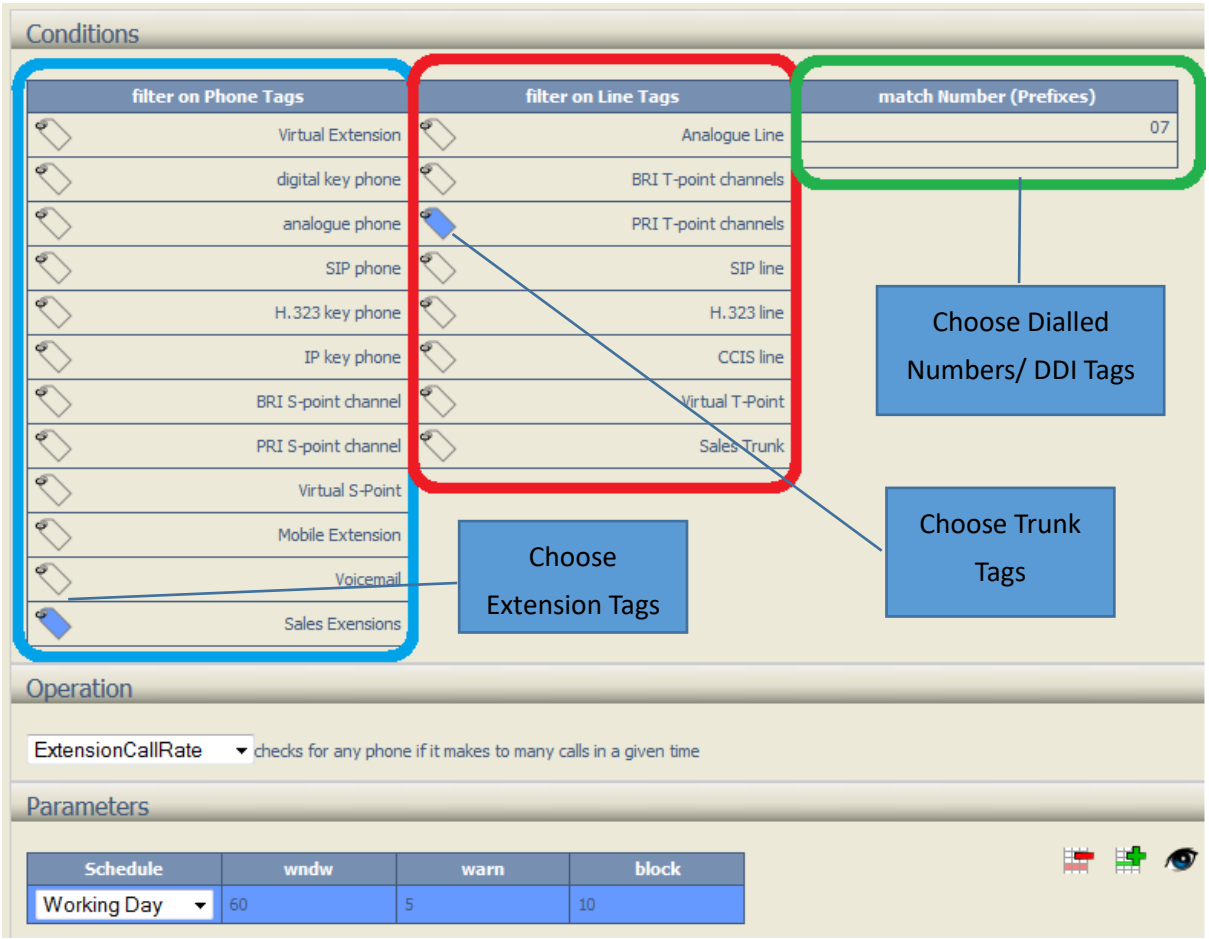
Block is usually the upper limit before an automatic block action is carried out.

Stop Checking is a rule that can be used to create exceptions to other rules, the common use for this is to exclude trunk, extensions, DDI's or dialled numbers from other rules.

Filtering Rules

By default all rules are applied system wide across all devices. They can be optionally filtered down to a defined group of extensions or trunks. Furthermore rules can be filtered against a Dialled Numbers or DDI's. There are several predefined groups available and custom groups can be created. To apply a filter to a rule, create the rule as normal and select the filtering options. When a filter is applied, an alert will only trigger if the call matches a filter. For example if a filter was applied against an extension group then only a call from an extension in that group would trigger the alert.

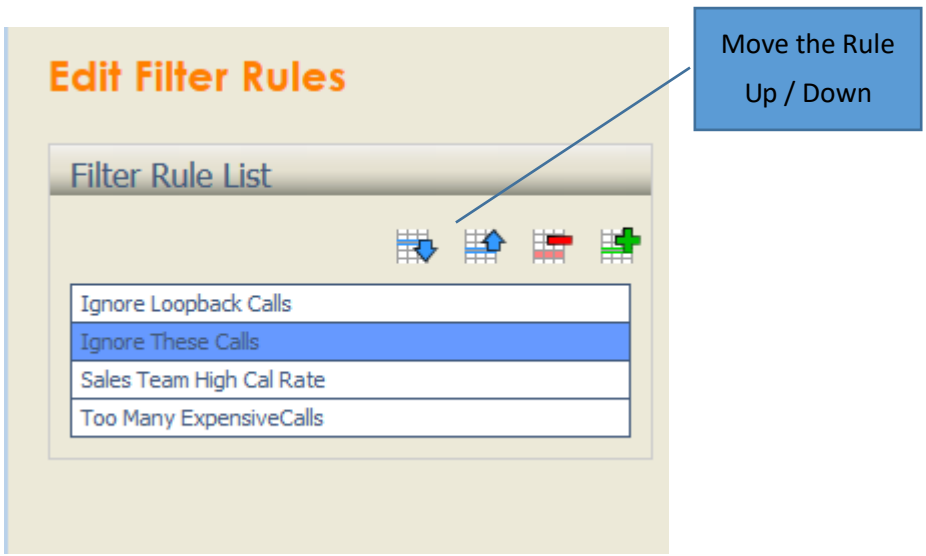
The left hand column listed under conditions displays extension tags. When a tag is applied against the group is shows blue. The middle column allows tagging against trunk types or groups of trunks. The right hand column allows tagging against a Dialled Number or DDI. If the alarm is based on outbound calls the numbers entered here are treated as Dialled Numbers, if the call is incoming then they are treated as DDI.



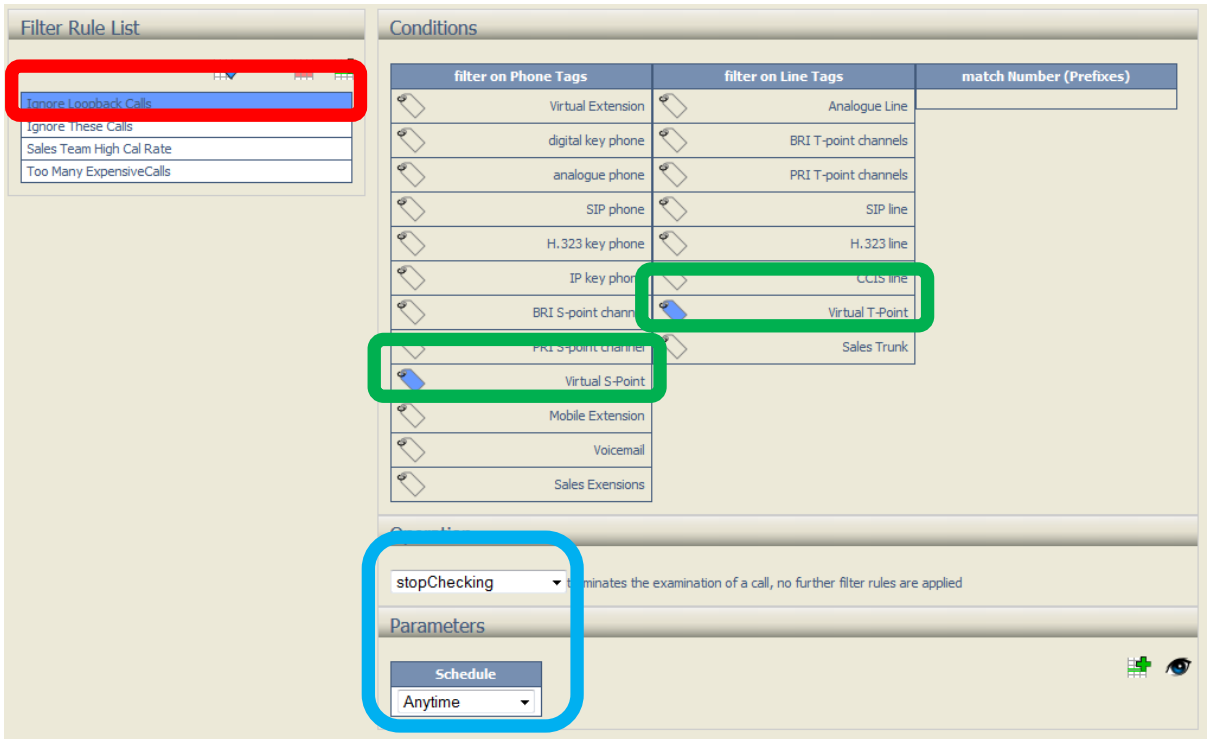
The above screenshot shows an Extension Call Rate rule configured to look at calls over a 60 minute period and trigger a warning at 5 calls and block at 10. The filtering above shows that it will only trigger on calls made by the 'Sales Extensions' group **and** is on a "PRI T-point Trunk" **and** is to a number beginning with 07. Multiple filters of the same type can be applied to a rule, these are applied using an 'or' condition. For example Sales Extensions or Mobile Extension or IP key phone.

Rule List

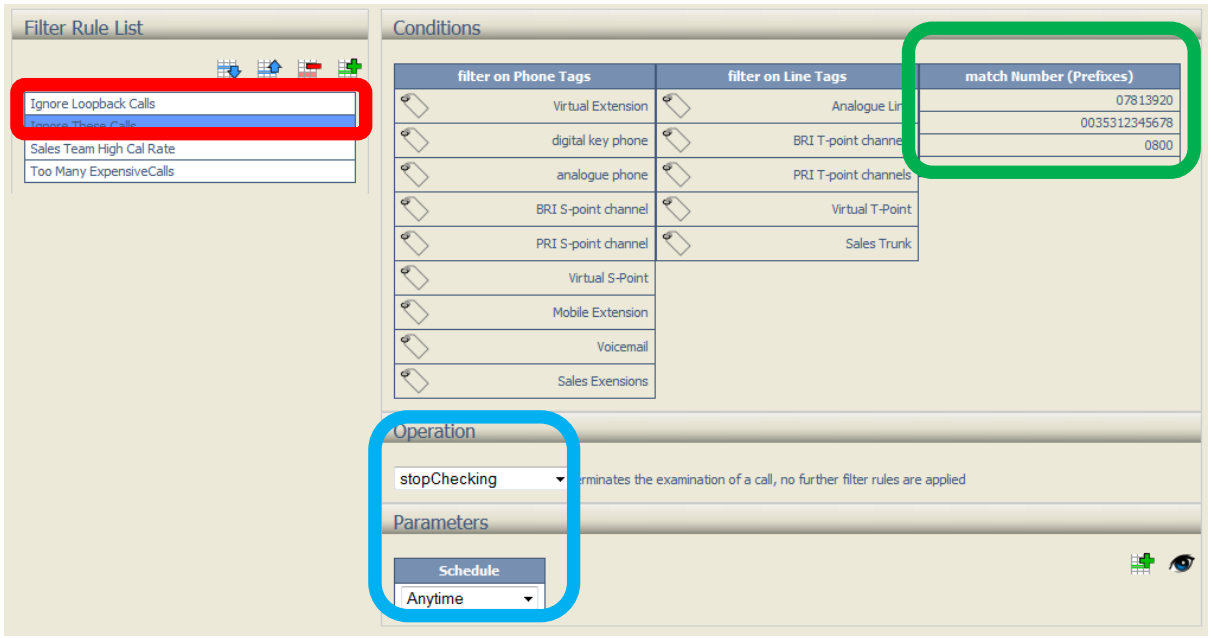
Rules are applied in the order that they are listed in rules configuration page. Below you can see there are four rules that are defined, the order in which they are listed and ultimately applied can be changed using the buttons. Rules are only applied when the time range they are assigned to is active.



Any Stop Checking rules should be applied at the top of the list, in the example below the first rule is called 'Ignore Loopback Calls.' It is a 'Stop Checking Rule' associated with the 'Anytime' time range that is applied to virtual loopback extensions and trunk ports. This rule would ignore any incoming or outgoing calls on a virtual extension or trunk. If a call was on any other extension or trunk then InGuard would look at the next rule in the list.

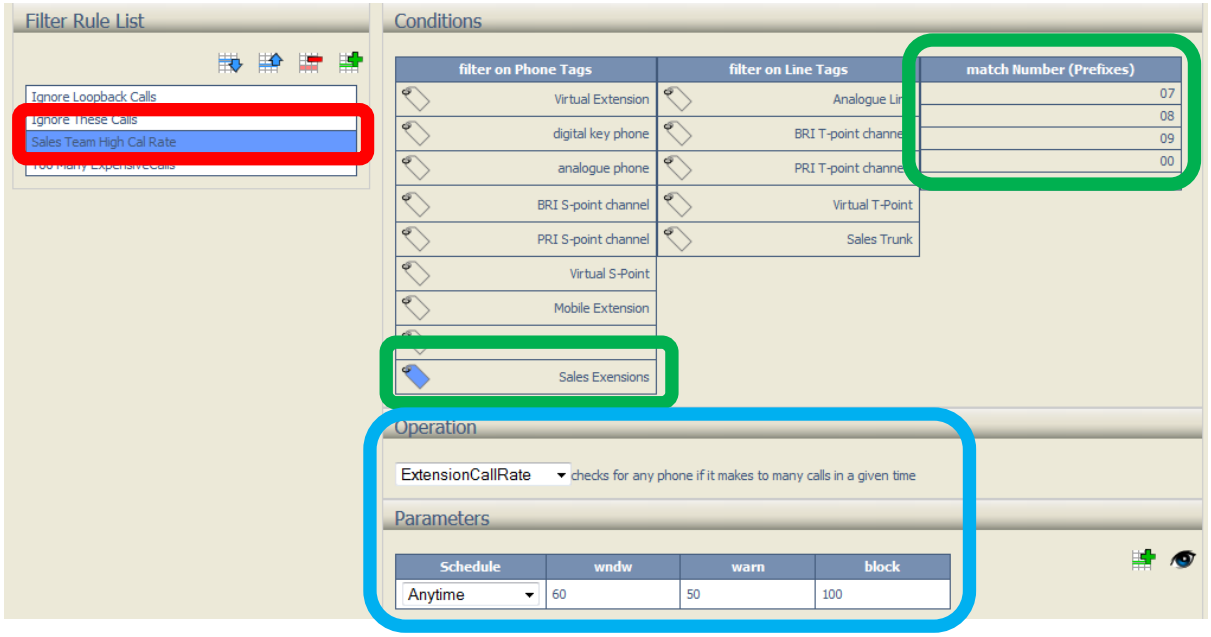


The next rule in the list is called 'Ignore These Calls' and lists a series of 'dialled numbers'. The rule is a 'Stop Checking' configured for the 'Anytime' time range. On outbound calls, this will ignore any calls to the destination numbers that have been entered. If any incoming alarms have been setup, then it will treat these as DDI numbers.

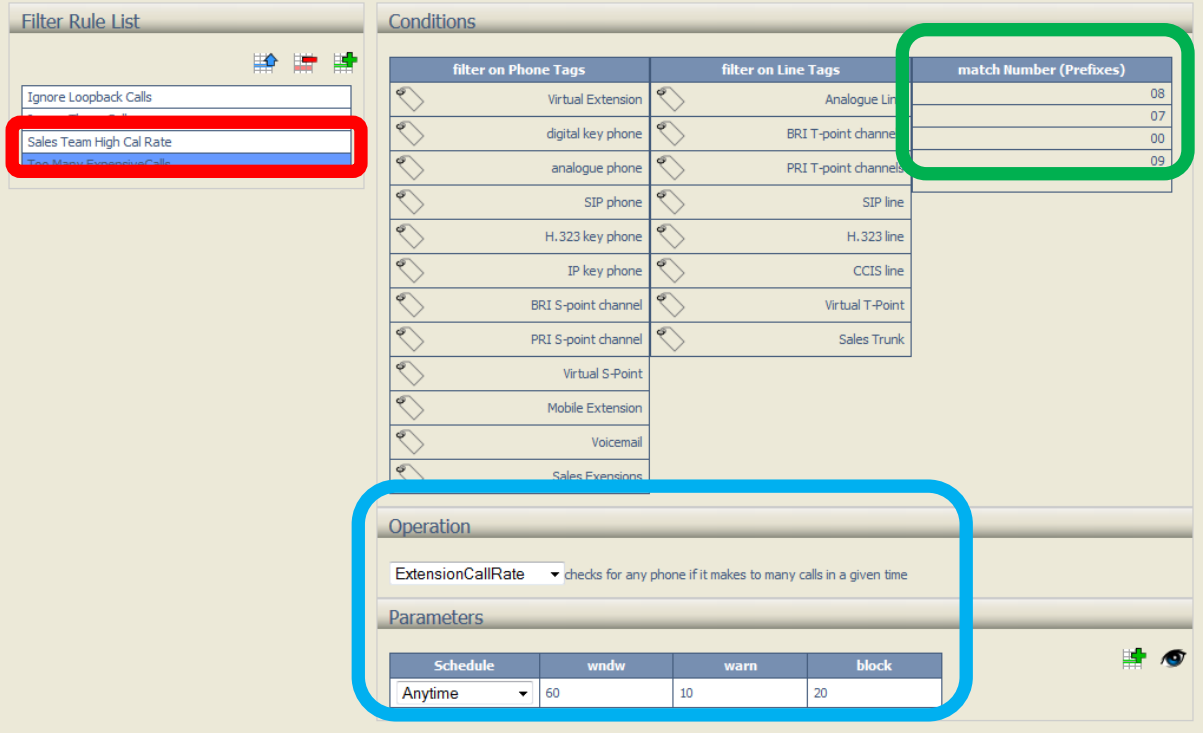


The two rules that are configured so far Stop Checking calls on Virtual Loopbacks and calls to the listed numbers. Any other calls would continue to be checked against the other configured rules.

The next rule is called 'Sales Team High Call Rate' and is applied to the Sales Extensions and any number beginning 07, 08, 09 and 00. The rule is an 'Extension Call Rate' applied to the 'Anytime' time range and will warn if 50 calls are made in 60 minutes and block at 100 calls.



The final rule is called 'Too Many Expensive Calls' and is filtered only against the numbers beginning 07, 08, 09 and 00. The rule is an 'Extension Call Rate' applied to 'Anytime' and will warn if 10 calls are made in 60 minutes and block at 20 calls.

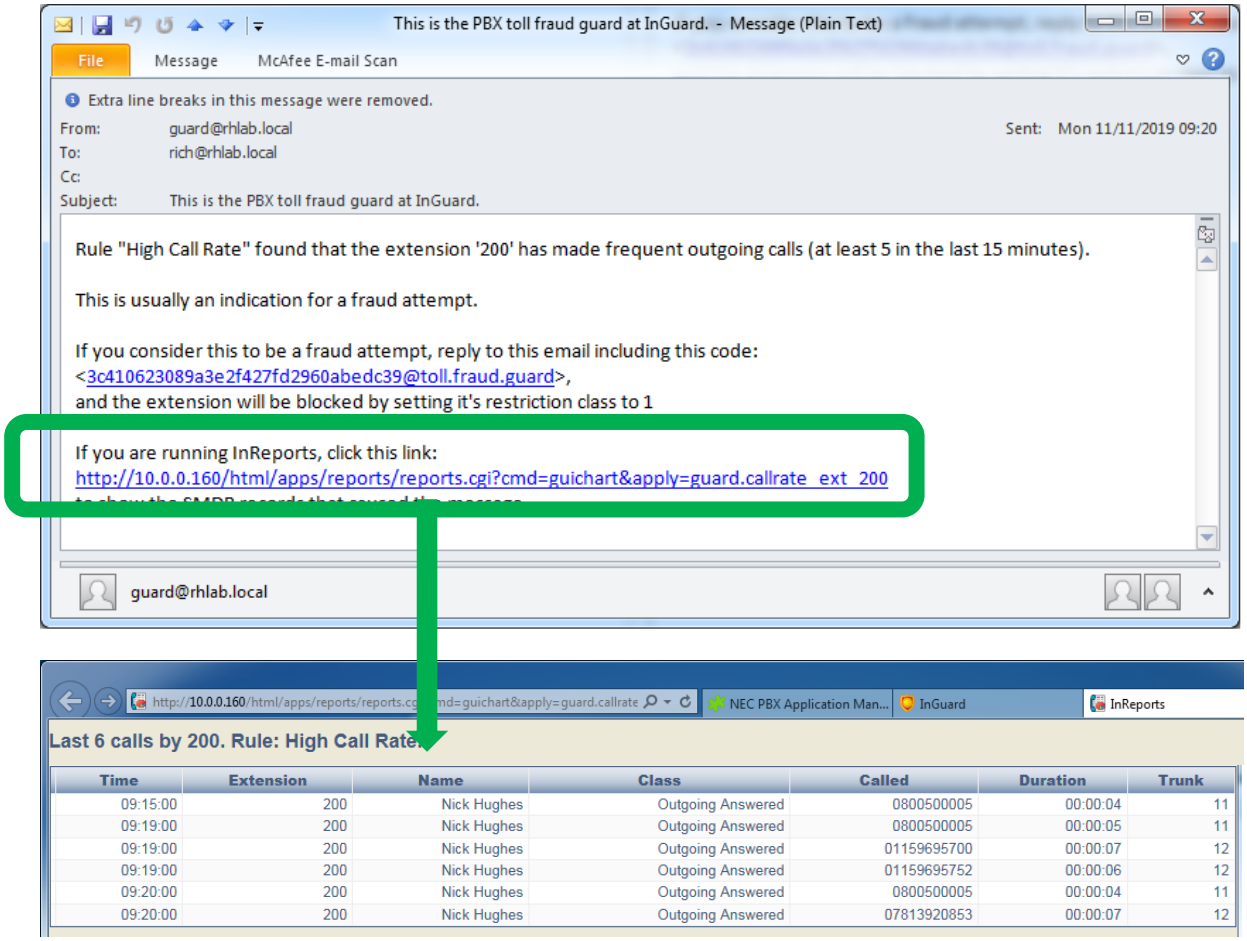


Looking back at the configured rules, the first rule said to stop checking calls if they are on a virtual loopback extension or trunk. If there was a call on a loopback then the guard would not apply any further rules to it. The second rule was applied system wide and would ignore any calls to the numbers listed in the match number column. The third rule was for the sales extensions making a number of calls to range of numbers. Finally the fourth was for any extension on the system making a number of calls to a range of numbers.

Link to InReports

InGuard 1.7.0 and above has a feature the can provide integration into InReports, this allows the user to click a link in the emails sent by InGuard. The link opens InReports and displays the call records that triggered the rule.

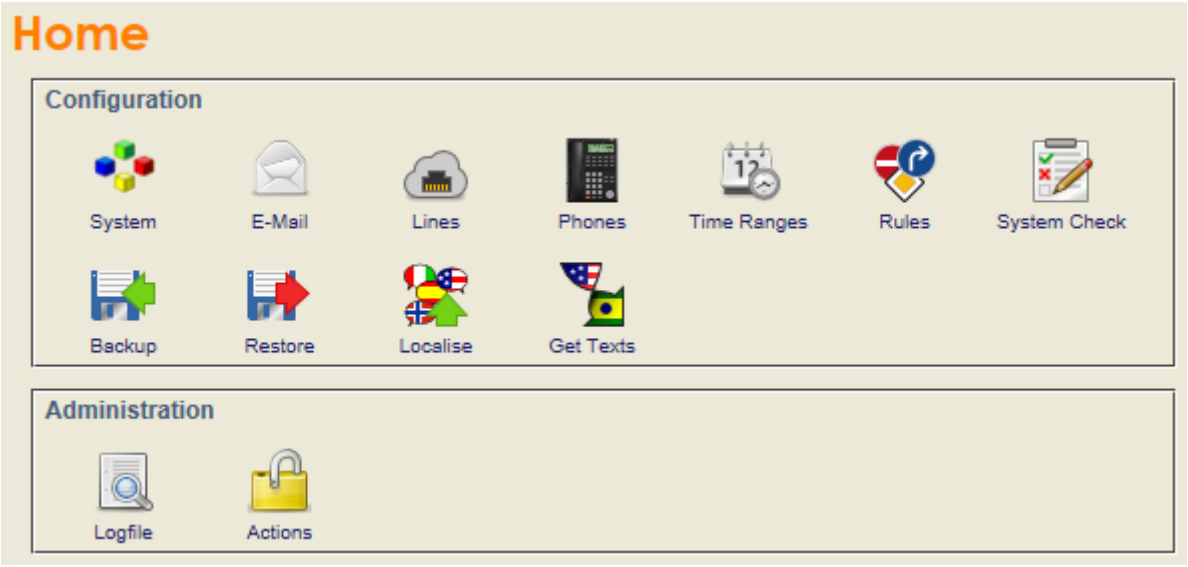
For this to work InReports 1.7.0 or above must also be installed as well as InGuard. Nothing needs to be configured for this to work, any emails that are generated will contain a link to InReports. If the user isn't logged in to InReports, they will be prompted to login first and then the links can be launched.



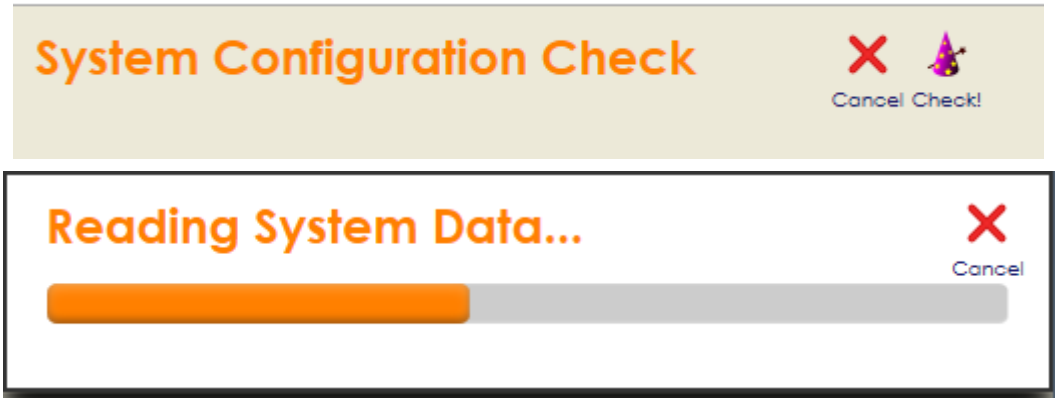
The reports can also be manually launched by clicking the link in the Reports area of Stored Activities.

System Health Check

The system health check is a built in feature that can look at the configuration of the PBX and show if any areas may leave the PBX vulnerable to an attempted hack. This can prompt an installer to make sure adequate precautions are taken when enabling features on the system. To run the System Check, click the icon from the InGuard home page.

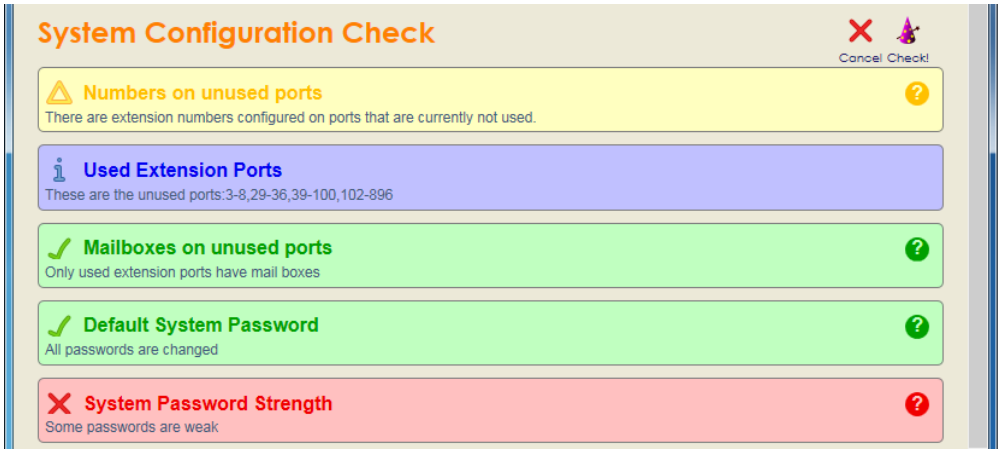


Click the Check button to perform the check.



Once the data has been read from the system then the report is displayed, each of the items will be displayed green, yellow or red depending on the result of the test. Green indicates that the PBX is configured well, yellow is more of an advisory condition that means this may be safe dependant on the feature. Anything in red is a warning and attention should be given to this.

Each item has an icon on the right hand side that provides more information about the check.



The manual goes on to explain in detail what each check does and the reason it is done. After making changes to the system data in the PBX, you can re-run the check.

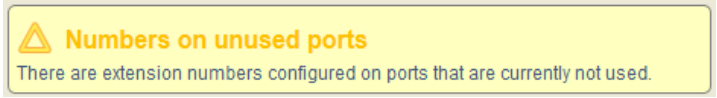
Numbers on Unused Ports

Purpose of the check	To determine if there are any unused extension ports that have extension numbers assigned to them.
Reason for the Check	Its good practice to remove any extension numbers from unused ports on the PBX. This stops potential hackers from trying to obtain an extension by an unauthorised method.

Possible Outcomes

If all unused extension ports don't have extension numbers assigned to them then a green tick is displayed.

If there are unused extension ports that have extension numbers assigned to them then the yellow triangle is displayed. As a corrective action you should remove extension numbers from unused ports. These can be found in Easy Edit / Extensions / Extension / Extension Properties / Extension Basic Setup or PRG command 11-02.



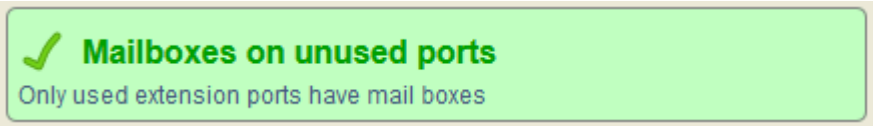
The next option down displays any used extension ports, meaning only these ports should have extensions assigned to them. If you have extension numbers configured on unused ports then this is a quick way to identify them.

Mailboxes on unused Ports

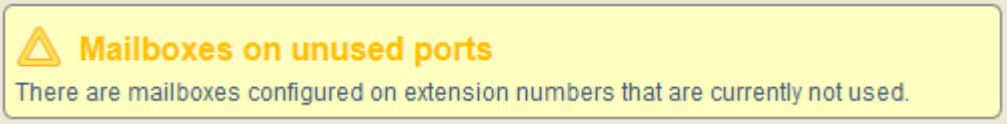
Purpose of the check	To make sure that mailboxes only exist for extensions that are used.
Reason for the Check	Voicemail can often be a target for hackers so it's considered a good safety measure to only have mailboxes enabled for extensions that are used. This greatly reduces the opportunity for a hacker to seize control of an un-used mailbox.

Possible Outcomes

If mailboxes only exist for used extension ports on the PBX then a green tick is displayed.



If there are mailboxes assigned to extensions that are not used then the yellow triangle is displayed. As a corrective action mailboxes should be removed from any un-used extension ports, this can be done it Easy Edit / Voicemail / InMail / InMail Mailboxes / InMail Mailbox Options or PRG command 47-02.

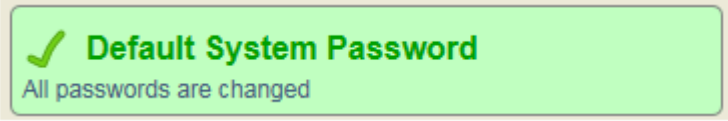


Default System Password

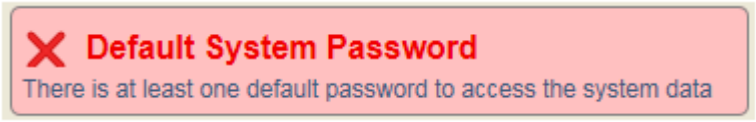
Purpose of the check	To make sure that the default usernames and passwords have been changed.
Reason for the Check	Like any default passwords it's possible that a hacker will know this information or will be able to find it out. Changing the default passwords is a simple precaution that can be used to prevent un-authorised users from gaining easy access to the PBX.

Possible Outcomes

If all of the default usernames and passwords that can connect to the system have been changed then a green tick is displayed.



If some of the default username and password haven't been changed then a red X is displayed, this can be corrected in PRG 90-02.

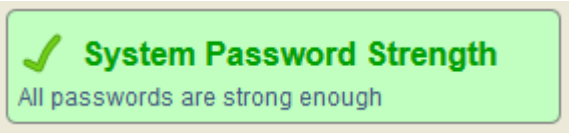


System Password Strength

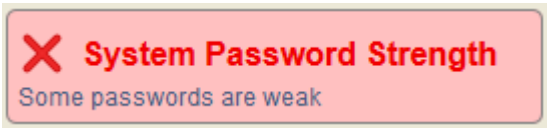
Purpose of the check	To make sure that the passwords used to connect to the PBX are suitably strong.
Reason for the Check	If a hacker is going to try and attempt to connect to a PBX, they might try with a simple password. By using a strong password this reduces the chances of success that they may have.

Possible Outcomes

If the system passwords are considered strong then a green tick is displayed.



If the passwords are not considered strong then the red X is displayed, this can be corrected in PRG command 90-02. Passwords shouldn't have numbers that are too close to each other, such as: 2468642, 12345678. Instead make up a password based on numbers that are far apart from each other such as 91628362.

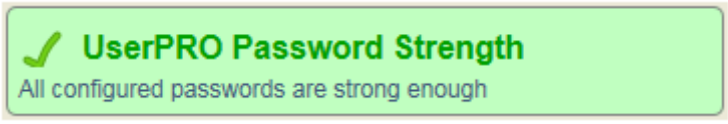


UserPRO Password Strength

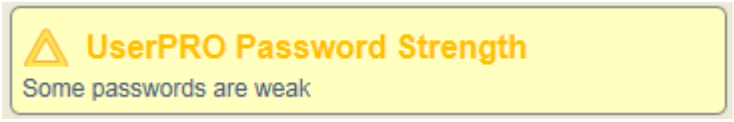
Purpose of the check	To make sure that any UserPRO passwords that are used are suitably strong.
Reason for the Check	If a hacker is going to try and attempt to access UserPRO, they might try with a simple password. By using a strong password this reduces the chances of success that they may have.

Possible Outcomes

If the UserPRO passwords are considered strong then a green tick is displayed.



If the passwords are not considered strong then a yellow triangle is displayed. To correct this you can change the UserPRO passwords in Easy Edit / Advanced Items / User Pro / Extension Password. Strong numeric password shouldn't have numbers that are too close to each other for example 2468. Passwords would be considered strong if the numbers are not too close to each other such as 2846.



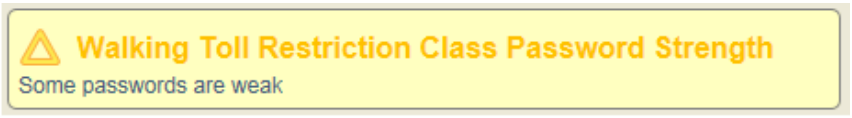
Walking Toll Restriction Class Password Strength

Purpose of the check	To make sure that if Walking Toll Restriction passwords are used that they are suitably strong.
Reason for the Check	If Walking Toll Restriction passwords are used then they should be suitably strong to prevent un-authorised use of the facility.

Possible Outcomes

If Walking Toll Restriction is used then the passwords are checked to make sure they are strong, if they are then the green tick is displayed. If Walking Toll Restriction isn't used then a green tick is also displayed.

If there is some Walking Toll Restriction passwords entered and they are not considered strong then a yellow triangle is displayed. To correct this you can change the passwords in Easy Edit / Toll Restriction / Toll Restriction Detailed View / Toll – Additional Services / Walking Toll Restriction Passwords or PRG command 21-14. Strong numeric password shouldn't have numbers that are too close to each other for example 123456 would be considered weak. Passwords would be considered strong if the numbers are not too close to each other such as 928461.

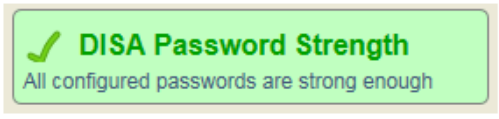


DISA Password Strength

Purpose of the check	To make sure that if DISA passwords are used that they are suitably strong.
Reason for the Check	If DISA passwords are used then they should be suitably strong to prevent un-authorised use of the facility.

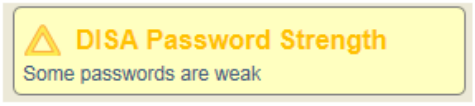
Possible Outcomes

If DISA is used then the passwords are checked to make sure they are strong, if they are then the green tick is displayed. If DISA isn't used then a green tick is also displayed.



If there is some DISA passwords entered and they are not considered strong then a yellow triangle is

displayed. To correct this you can change the passwords in Easy Edit / Auto Attendant / DISA / DISA Password or PRG command 25-08. Strong numeric password shouldn't have numbers that are too close to each other for example 123456 would be considered weak. Passwords would be considered strong if the numbers are not too close to each other such as 928461.

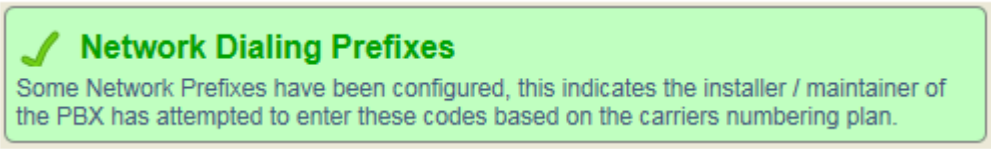


Network Dialling Prefixes

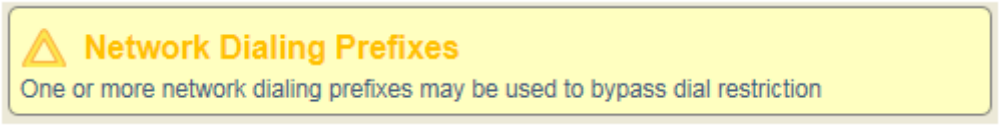
Purpose of the check	To make sure that the PBX has some Network Dialling Prefixes entered.
Reason for the Check	In the UK for example, some dialled numbers can be prefixed with network based service codes such as 1280, 141 and 1470 that can be dialled to access certain features on the public telephone network. If for example all international calls are barred by preventing the PBX from dialling '00' but an extension dials 141 followed by 00 this would be allowed. To get around this issue, 141 and any other prefix number have to be added to the toll restriction setup on the PBX as Pre-Fixed Special Service Codes. It is therefore important that an installer enters the correct codes for the carrier. These codes can of course vary between different carriers and different countries. The health check feature doesn't know the correct service codes that should be entered, it just checks to make sure that entries exist in the tables on the PBX. This indicates the installer has attempted to enter the correct codes.

Possible Outcomes

If some numbers have been entered in the table then a green tick is shown. This only means that numbers have been entered and does mean the correct numbers are entered.



If no numbers are entered in the table then a yellow warning is displayed. To correct the problem, there must be entries in Easy Edit / Toll Restriction / Toll Restriction Detailed View / Pre-fixed Special Service Codes and /Toll Additional Services / Pre-Fixed Specified Access Code or PRG commands 21-06-09 / 21-06-10.

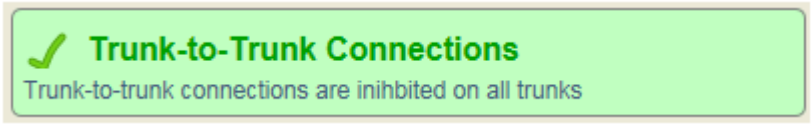


Trunk to Trunk Connections

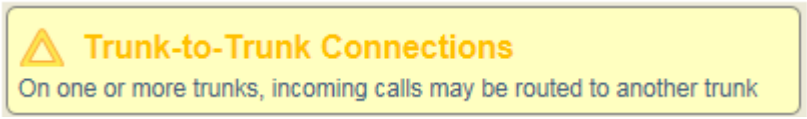
Purpose of the check	To indicate if any trunks are enabled for trunk to trunk transfer.
Reason for the Check	If trunks are enabled for trunk to trunk transfer then this can potentially allow calls to arrive at the system and be routed out again. The check will indicate that the feature is enabled and it then becomes the responsibility of the installer to make sure that the appropriate level of Toll Restriction is configured on the PBX. Toll Restriction may for example prevent calls from being allowed out of the PBX outside of normal working hours.

Possible Outcomes

If no trunks are enabled for trunk to trunk transfer then a green tick is displayed.



If any trunks are enabled for trunk to trunk transfer then the installer must consider if they are setup in a way that doesn't present a security threats to the PBX. Trunk to trunk transfer can be disabled in Trunks / General / Trunk Basic Data Setup or PRG command 14-01.

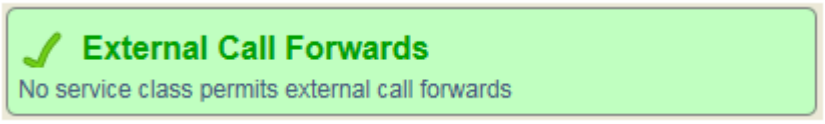


External Call Forwards

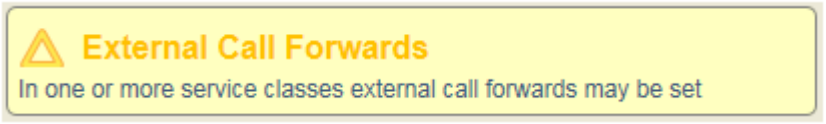
Purpose of the check	To indicate if External Call Forwards are enabled on the PBX.
Reason for the Check	External call forwards can be enabled to allow calls to be routed out of the PBX. The check will indicate that the feature is enabled and it then becomes the responsibility of the installer to make sure that the appropriate level of Toll Restriction is configured on the PBX. Toll Restriction may for example prevent calls from being allowed out of the PBX outside of normal working hours.

Possible Outcomes

If External Call Forwards is disabled in all class of services then a green tick is displayed.



If External Call Forward is enabled in any class of service then the yellow triangle is displayed and the installer must consider if they are setup in a way that doesn't present a security threats to the PBX. External Call Forward can be disabled in Easy Edit / COS /COS or PRG command 20-11.

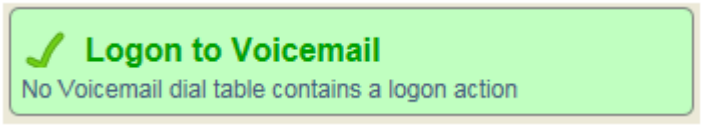


Logon to Voicemail

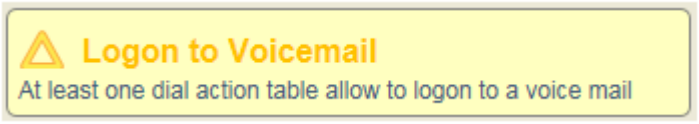
Purpose of the check	To make sure that the Voicemail Dial Action Tables don't have the 'Logon Action' enabled.
Reason for the Check	The Logon action allows someone who has been answered by a voicemail box to enter an extension number and the logon to the mailbox for that extension. A hacker may do this in an attempt to comprise the voicemail. The check will indicate that the feature is enabled and it then becomes the responsibility of the installer to make sure that the appropriate level of Toll Restriction is configured on the PBX. Toll Restriction may for example prevent calls from being allowed out of the PBX outside of normal working hours. Furthermore, explicit Toll Restriction rules may be applied to the voicemail ports.

Possible Outcomes

If no mailboxes have the Logon action set then the green tick is displayed.



If any mailboxes have the logon action enabled then the installer must consider if they are setup in a way that doesn't present a security threats to the PBX. The feature can be disabled in Easy Edit / Voicemail / InMail / InMail Routing / InMail Dial action Tables DAT or PRG command 47-13.



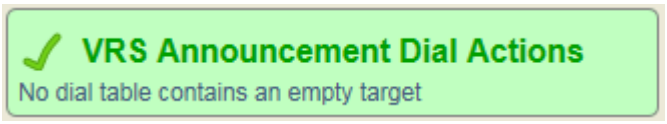
VRS Announcement Dial Actions

Purpose of the check	To make sure the outside callers that are answered by the VRS can only dial known digits.
Reason for the Check	If a 'Next Attendant Message' and a 'Destination Number' isn't specified then when a call is answered by the VRS, the digit can be dialled potentially allowing a user to access system features and possibly compromise them.

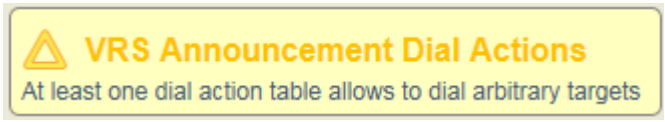
Possible Outcomes

If each used VRS Message contains either another target or a VRS message then a green tick is displayed. An example of correctly programmed VRS message is below, you can see this is for message 1 and options 1, 2 & 3 and pointed to 200, 202 and 203. The remaining options all point back to message 1.

Attendant Message	Received Digit	Next Attendant Message	Destination Number
Attendant Message: 001			
001	1	0	200
001	2	0	202
001	3	0	203
001	4	1	
001	5	1	
001	6	1	
001	7	1	
001	8	1	
001	9	1	
001	0	1	
001	*	1	
001	#	1	



If there are used VRS Message that don't either point to another attendant message or a destination then the check will fail, to correct this each these in Easy Edit / Auto Attendant / Auto Attendant / Auto Attendant Single Digit Operations.

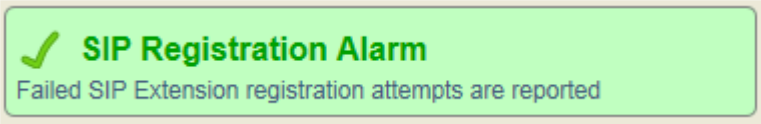


SIP Registration Alarm

Purpose of the check	To see if the SIP Registration Alarm is enabled.
Reason for the Check	The SIP registration alarm will trigger an alarm on the PBX when any SIP extension attempts to register to the system and fails to do so. This can be a sign of an attempted hack.

Possible Outcomes

If the SIP registration Alarm is enabled then a green tick is displayed.



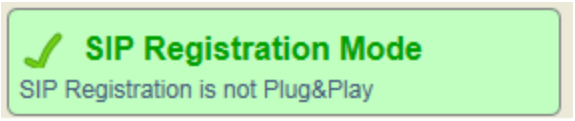
If the SIP registration alarm isn't enabled then the yellow triangle is displayed. The alarm can be enabled in Easy Edit / Advanced Items / Maintenance / Alarms / System Alarm setup and enabled alarm 61 or PRG command 90-10.

SIP Registration Mode

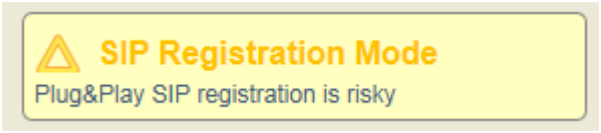
Purpose of the check	To see if 'Plug and Play' SIP registration is enabled.
Reason for the Check	Plug and Play can present an easy way for a user to connect a handset to the system that could be available for use.

Possible Outcomes

If Manual Mode or Automatic is set then the green tick is displayed.



If Plug and Play mode is set then the yellow triangle is displayed. The Register Mode can be set in Easy Edit / Advanced Items / VoIP / Extensions / DT700 800 Setup / Register Mode or PRG command 10-46-01.



IP NAT and Encryption

Purpose of the check	To see if a safe combination of NAT and Encryption is enabled.
Reason for the Check	If NAT is enabled then it's important to use Encryption this is because typically NAT'd traffic will go over the public internet and would be susceptible to someone being able to see the traffic.

Possible Outcomes

If NAT isn't enabled then a green tick is displayed. If NAT is enabled and Encryption is enabled then a green tick is also displayed.

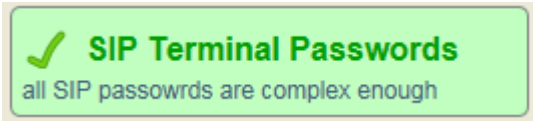
If NAT is enabled and Encryption isn't then the yellow triangle is displayed and you should consider enabling encryption.

SIP Terminal Passwords

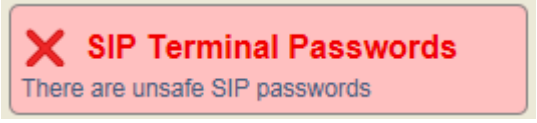
Purpose of the check	To make sure that any passwords for SIP extensions that are enabled on the PBX are suitably strong. This check is only performed when the SIP registration mode is set to Automatic or Manual.
Reason for the Check	A hacker may attempt to register a SIP extension by trying simple passwords for a device, using a complex password greatly reduces the possibility of someone guessing a password.

Possible Outcomes

If all passwords are complex then a green tick is displayed.



If there are some passwords that are considered not complex then a red x is displayed. The passwords can be changed in Easy Edit / Advanced Items / VoIP / Extensions / SIP Extensions / SIP Terminal Settings / Authentication Password or PRG Command 15-05-16.

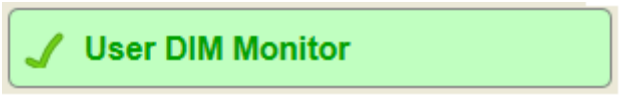


User DIM Monitor

Purpose of the check	To check if the User DIM Monitor is enabled, if it is then make sure it as a suitably strong password.
Reason for the Check	The DIM monitor can be used to aid a maintainer when they are diagnosing problem on the PBX. It's possible that a hacker could exploit the PBX if they had access to the DIM.

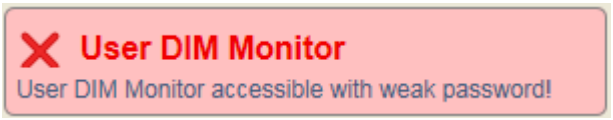
Possible Outcomes

If DIM access has been disabled in PRG command 90-31 then a green tick is displayed indicating that the DIM Monitor is disabled.



If DIM access is enabled and has complex password then the yellow triangle is displayed.

If the DIM access is enabled with a weak password then the red X is displayed.



Restriction Classes used by the Guard

Purpose of the check	To make sure that used Toll Restriction classes on the PBX are assigned to the restrict table that the Guard is configured to use.
Reason for the Check	To make sure the installer has installed the Guard in a way for it to be effective for all extensions.

Possible Outcomes

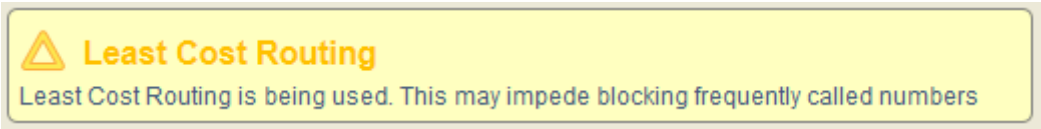
The health check will look at the restrict table the Guard is configured to use and make sure that it's assigned to any used Toll Restriction Classes. All Toll Restriction classes are check apart from the one that is used by the Guard for blocking extensions. If this is correctly configured then a green tick is displayed.

If there are Toll Restriction classes used on the system that are not assigned to the restrict table used by the guard then a red X is displayed.

Least Cost Routing	
Purpose of the check	To see if LCR is enabled on the PBX.
Reason for the Check	To make sure the Guard can effectively apply blocking actions to dialled numbers that are triggered by rules.

Possible Outcomes

If LCR isn't enabled on the PBX then no message is displayed, if LCR is enabled then a yellow warning message is displayed.



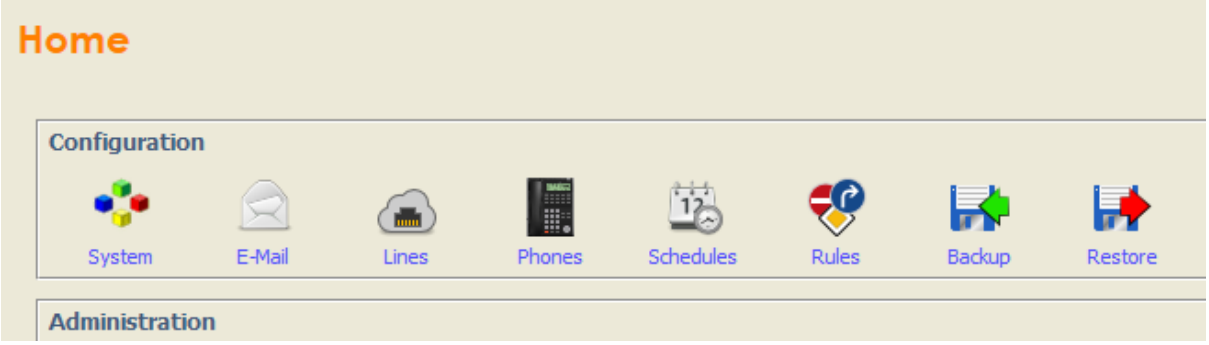
Dial Restriction Override	
Purpose of the check	To see if Toll Restriction Override is enabled on the PBX.
Reason for the Check	If this is enabled then it would allow someone to override Toll Restriction and dial ANY number.

Possible Outcomes

If Toll Restriction Override is enabled in any Class of Service then the red warning is displayed. If the feature isn't enabled then nothing is displayed.

Backup and Restore

InGuard's configuration 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 InGuard 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.

Actions

When warning email are sent out giving the option to block an number from being dialled or for an extension to be moved to a restrictive class of service, the action can be carried out from the Stored Activities menu. Clicking the Padlock icon will carry out the action and clicking the Trash icon will effectively delete the request meaning it can no longer be actioned.

InGuard – Software Licence Agreement

PLEASE READ THIS SOFTWARE LICENCE AGREEMENT ("LICENCE") CAREFULLY BEFORE USING THE InGUARD SOFTWARE. BY USING THE InGUARD 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 NEC 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.**

Revision History

Version	Author	Date	Updates
1.0	R Horsley	Nov 2019	Release of InGuard 1.7.0

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

NEC Enterprise Solutions has prepared this document for use by its employees and customers. The information contained within this manual is the property of NEC Enterprise Solutions and shall not be reproduced without prior written approval of NEC Enterprise Solutions.

NEC Nederland
B.V.
Olympia 4
1213 NT Hilversum
The Netherlands
www.nec-enterprise.com