



User Guide

Contents

Features	6
How Does Scammer Jammer Work?	6
Important Stuff	6
Requirements	7
Additional Parts	7
For Use in the United State Only.	7
Telephone Service Provider.	7
Caller ID Service	8
Call Waiting Service	9
Telephones	9
Voice Mail or Dedicated Answering Machine	10
Network Access	11
Firewall Settings	11
Installation	12
Install Scammer Jammer	12
Using the Navigation Switch	14
Set Primary Scammer Jammer Settings.	18
Find the Serial Number	19
Install Sjsconfig	20
Creating a New Scammer Jammer Account	23
Adding a Scammer Jammer Device to an Account	27
Place a Test Call	28
Review the Log in sjsconfig	29
Using an Answering Machine with Scammer Jammer	30
Testing Voice Mail / the Answering Machine	32
Using Scammer Jammer	34
Call Indicator	34
Call Log	35
Creating or Changing a Rule using the Call Log.	35
Using sjsconfig	37
Logging in to the Scammer Jammer Server.	37
Forgotten Login or Password	38
Main Window	39
Call History Log Window	40
Log Detail Window	42
411 Information Window.	42
Make Rule.	44
Make Scammer	45
Make Genuine.	46
Goto 800Notes.com	47
Report to FTC.	49
Rules List Window	50
Rule Definition Window.	50
Default Action	52
Standard Rule Subscriptions	53

Subscribing to a Standard Rule.	53
Unsubscribing from a Standard Rule	54
Standard Rule Definitions.	55
Recommended Subscriptions	57
SJ Device Settings	58
Selecting a Device to Change	58
Common Settings	59
Except Action	59
Scammer Detection Tuning	60
Deleting old Call Log Data.	61
Extended CNAM Lookup.	61
SJ Device Settings Buttons.	62
Account Settings	62
Delete Account	63
Advanced Topics	64
Advanced Installation	64
Using Scammer Jammer with Multiple Telephones.	64
Multi-Telephone Wiring for VoIP.	65
Multi-Telephone Wiring for Land Lines	67
Using Scammer Jammer with a MODEM or Fax Machine	70
Using Scammer Jammer with a Burglar Alarm	70
Modes - Alter the Processing of Actions.	73
Changing the Mode.	73
Timed Connect ALL.	74
Cancel Timed Connect ALL.	74
Old Mode Names	74
Caller ID Name Based Rules	76
Partial Match Rules	77
Using Partial Match Rules for a Company.	78
Using Partial Match Rules to Forward Local Spoofing	78
Using Partial Match Rules to Block an Entire Area Code	78
Using Name Override and Partial Match Rules	79
Which Rule will be used?	79
Using the Default Action when Defining a Rule.	80
Nuisance Calls - 3rd Party Scammer Testing	81
Rule Sources and Source Order.	83
What Happens when a call is Blocked?	85
Scammer Jammer Strategies	86
Connect Known and Unknown Callers, Block All Others	86
Connect Known, Forward Unknown, Block All Others.	87
Connect Known Callers, Block All Others.	87
Bypassing Scammer Jammer by Redialing	89
Blocking Local Exchange Spoofed Calls	90
Forwarding rather than Blocking Scammers	91
When Voice Mail nor an External Answering Machine is Feasible	92
Using a Built-In Answering Machine.	92
Using a PBX with Integrated Voice Mail.	92

Using a PBX and Forwarding to Integrated Voice Mail	93
Master Scammer Jammer Units	94
Subscribing to Emailed Status Reports	97
Store / Restore of Scammer Jammer Settings	99
Request SJ Settings be Stored	101
Request SJ Settings be Restored	103
Viewing Settings	104
Editing Settings	105
Saving Settings	106
Save Copy of Settings	106
Deleting Settings	107
Copying Settings to the Clipboard	107
Advanced Settings	108
Installing the Native Mac Version of sjsconfig	109
Notes for Using Native Mac Version of sjsconfig	114
When to Use Static IP Addressing	116
Appendices	118
Telephone Compatibility List	118
Telephone Carrier Compatibility List	120
Recommended Answering Machines	121
Menu Tree	122
Settings Menu	125
Warning and Error Messages	133
Call Indicator	134
Troubleshooting	135
Resetting EEPROM	139
Revision History	140

Features

- Works with copper lines or Voice Over IP telephone connections.
- The telephone rings only for allowed calls.
- Unknown/unwanted callers can go direct to voice mail, telemarketers are JAMMED (blocked).
- Blocks more than 3,500,000 known telemarketer numbers.
- 80% of telemarketers are recognized and blocked without additional rules.*
- Your telephone Caller ID display can receive actual names rather than WIRELESS CALLER.
- Unlimited caller rules.
- Standard rules to block entire regions such as Jamaica, or Florida.
- Remote configuration and monitoring.


How Does Scammer Jammer Work?

- Scammer Jammer sits between the telephone line and your phone so it can see incoming calls before your phone does:



- When idle, Scammer Jammer leaves the telephone disconnected from the line so it cannot ring.
- If an outbound call is sensed, Scammer Jammer will immediately connect the telephone handset to the telephone line.
- When an inbound call is received, Scammer Jammer looks at the incoming telephone number. It then decides which **Action** to take. The actions are: **Connect**, **Forward**, or **Block**.
 - Connect - calls connect to your phone and ring so you can answer.
 - Forward - calls are sent to voice mail or answering machine and phone the never rings.
 - Block - calls are disconnected and the phone never rings.
- There are multiple sets of rules that can be applied to an inbound call. Perhaps the call is from a friend in your private rules, or a scammer in the scammer list. The action taken will depend upon these rules.

Important Stuff

-  Connect the telephone company's line **ONLY** into Scammer Jammer's LINE jack. Connecting the telephone line into any other of Scammer Jammer's ports may damage it.

- If you remove power from Scammer Jammer, the handset will connect to the telephone line and act exactly as if Scammer Jammer were not installed.
- You will **not** hear the first ring.

The first ring occurs before Scammer Jammer decides if the telephone is to be connected to the line to allow it to ring.

- If you have Call Waiting, Scammer Jammer will not block/forward incoming calls while a call is already in progress. If this is a problem, disable Call Waiting.

Requirements

This section discusses what is required for Scammer Jammer to operate properly.

Additional Parts

Not supplied with the Scammer Jammer:

- RJ45 Cable - You will need a network cable that will reach from your network switch or cable modem to the Scammer Jammer.
- RJ11 Cables - You will minimally need a telephone cable that reaches from the wall jack or cable modem RJ11 port to the Scammer Jammer. You may need other cables / RJ11 accessories to connect the phone into the Scammer Jammer.
- If you are using an external answering machine, you may need an RJ11 cable to connect the answering machine to the Scammer Jammer. The recommended answering machine comes with its own RJ11 cable.
- Scammer Jammer requires a 110V/120V electrical connection. You may need to provide an extension cord to reach from the outlet to the Scammer Jammer.
- It is recommended that Scammer Jammer be plugged into a surge suppressor strip with a UL 1449 rating.

For Use in the United State Only

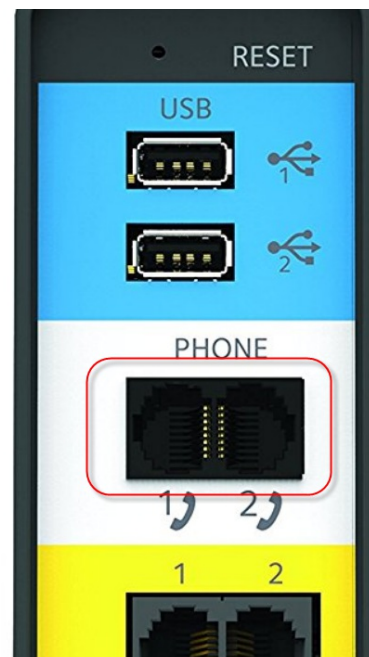
Scammer Jammer was designed specifically for the caller ID standard used in the United States and is only certified for the U.S. telephone system.

Telephone Service Provider

Scammer Jammer must access your telephone service provider via an RJ-11 jack or a VoIP analog telephone adapter jack:



Telephone Line Wall Jack



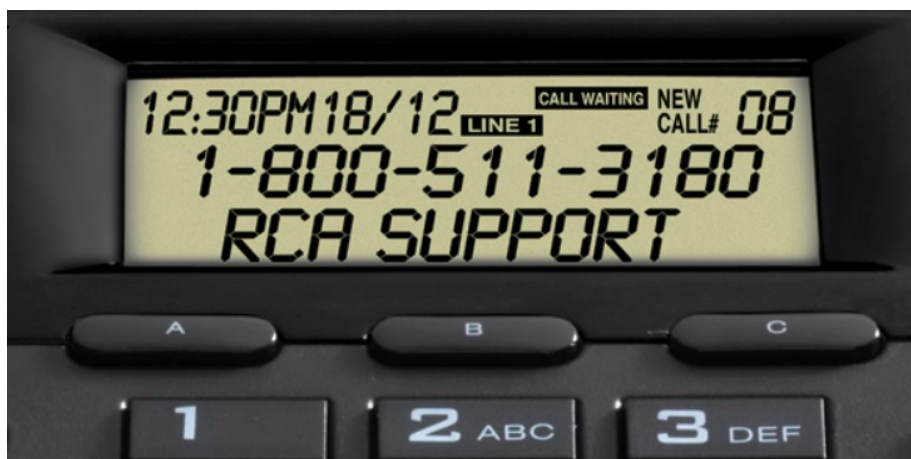
VoIP Analog Telephone Adapter (ATA)

Scammer Jammer works with old-style wired carriers (copper lines) such as CenturyLink, AT&T, and Verizon, Bell South. Scammer Jammer works with VoIP carriers such as Comcast, or Vonage. It also works for VoIP provided by telephone carriers such as CenturyLink's DSL service. Scammer Jammer will work with any VoIP carrier as long as an analog telephone adapter is provided by the carrier. See [Telephone Carrier Compatibility List](#).

Caller ID Service

Your telephone service provider must provide you will Caller ID service for Scammer Jammer to function.

To verify you have caller ID service, when someone calls your phone, the call should show up in the caller ID window on the phone:



If you do not have Caller ID service, you need to subscribe to the service before you can use Scammer Jammer.

Call Waiting Service

Scammer Jammer cannot detect call waiting calls (an incoming call while a call is already in progress). If you have call waiting and a scammer calls during a call, you will still be interrupted by them.

If you are trying to protect, say, a senior from scammers, you may wish to disable call waiting so scammers can't slip through during a call in progress.

Telephones

Scammer Jammer will work with any normal analog telephone handset. To take the best advantage of Scammer Jammer, the handset should have a Caller ID display, though it isn't required.

The optimum telephone handset for use with Scammer Jammer is a cordless system such as this:



Setup of this type of telephone with Scammer Jammer is the easiest.

See [Telephone Compatibility List](#) to review telephone models that have been tested with Scammer Jammer.

Scammer Jammer can also work with old rotary phones IF your telephone service provider supports them; however, these phones don't have a caller ID display which prevents you from using some of Scammer Jammer's features.



Voice Mail or Dedicated Answering Machine

If your telephone service provider provides you with Voice Mail (and you are using it rather than any built-in answering machine on your phone), that is compatible with Scammer Jammer.

If you are using the answering machine on your telephone, then Scammer Jammer is limited in how it handles unknown callers. This limitation can be removed by using voice mail or adding a stand-alone answering machine.

Scammer Jammer will ALWAYS block scammers and those numbers you tell it to block. How you want it to handle other unknown callers determines if you need an external answering machine.

The simplest answer is to subscribe to voice mail. If you don't have and don't want voice mail, then here are your options:

- If unknown callers are acceptable to you (they will always be identified as Unknown by a ? in the caller ID display), then you can continue to use your telephone's built-in answering machine.
- If you DO NOT want unknown callers to ring your phone, e.g. they MUST be sent to the answering machine without ringing your phone, then you will want an external answering machine.

There are not many external answering machines on the market. The recommended model is this AT&T model 1740. It works fine but has the limitation that if a message is left, there is no way to turn off call screening so you may hear an unknown caller leaving a message.



Network Access

Scammer Jammer must access the internet to operate properly. It is critical that the Scammer Jammer Server can be accessed quickly when an inbound call occurs, so there are some limitations on the network connections.

You must provide Scammer Jammer with a wired broadband network connection.

Dial-up networking will NOT work.

Wi-Fi is NOT recommended.

Wi-Fi can be implemented using a Wi-Fi adapter such as the TP-LINK Wireless Nano router. However, accessing the network over a Wi-Fi connection can be slow depending on various factors. The Wi-Fi connection may work fine most of the time but occasionally not get a response back in time, in which case Scammer Jammer will allow the phone to start ringing because it couldn't identify the number quick enough.

Firewall Settings

Scammer Jammer and the configuration software makes outbound connections on ports 11183 (TCP), 11184 (UDP), and 11185 (TCP). In a normal home installation, you will not need to make any special firewall settings for Scammer Jammer.

In office settings where a proxy server may be used, Scammer Jammer cannot use a proxy server. In that case, you will need to make special accommodations for Scammer Jammer.

When you run the sjsconfig program from your PC, Windows might ask if you want to allow sjsconfig to access the network, in which case you must allow access.

Installation

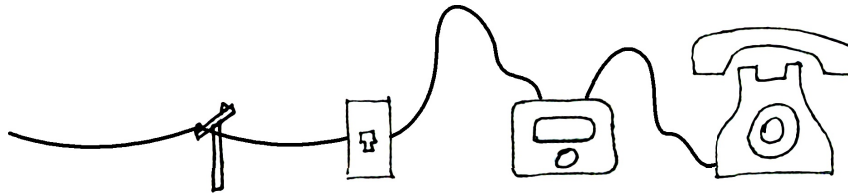
This section covers a typical Scammer Jammer installation. For more complex environments, see [Advanced Installation](#).

Install Scammer Jammer

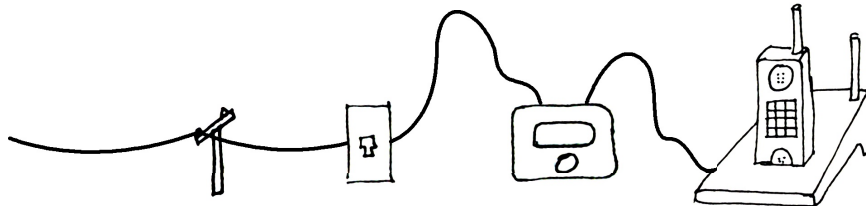


ONLY connect the telephone company's line into Scammer Jammer's LINE jack. Connecting the telephone line into any other jack may damage the Scammer Jammer.

When setting up Scammer Jammer, these instructions assume you are connecting it between a standard handset such as:

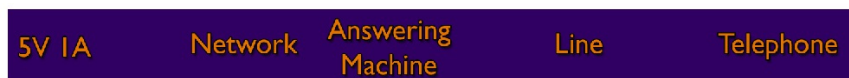





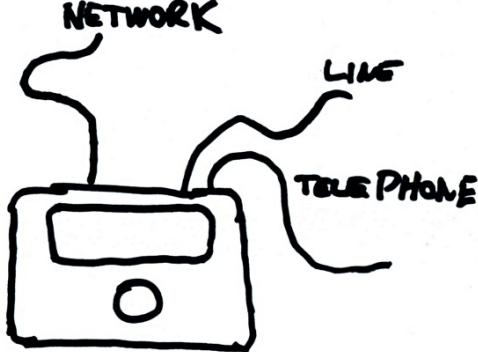
or a wireless base station such as:



While the above diagrams show the handset / base station plugged straight into a wall jack, it could be plugged into a VoIP devices such as a cable router or DSL router as outlined in the requirements.

Scammer Jammer has several jacks. Each jack is labeled on the bottom of the unit:



	<p>Disconnect the existing handset from the wall jack or VoIP unit.</p>
	<p>Connect a telephone cable (RJ11) between the wall jack and Scammer Jammer's <i>Line</i> jack.</p>
	<p>Connect the existing handset into the <i>Telephone</i> jack.</p> <p>You should now have a phone cord in and a phone cord out as shown in the diagram above.</p>
	<p>Connect a network cable from your network into the <i>Network</i> jack on the Scammer Jammer.</p>

Don't plug power in to the Scammer Jammer yet!

Test It!

- With Scammer Jammer OFF, your telephone will work just like it has in the past. Pickup the handset and verify you have dial tone. If you do not, correct the problem before going on.
- Now plug the supplied **power** adapter into the Scammer Jammer and then into the wall. Use **only** the power adapter supplied with the Scammer Jammer. The wrong power adapter will damage Scammer Jammer.
- Verify your Scammer Jammer is running. When you first start Scammer Jammer you will see:

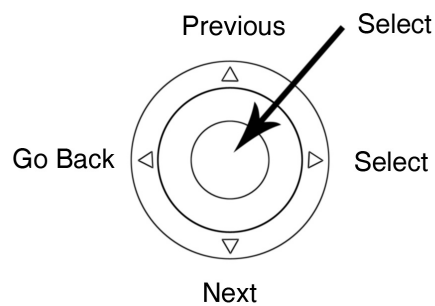
```
Scanner Jammer  
Initializing...
```

then

```
Scanner Jammer  
On
```

Using the Navigation Switch

The navigation switch looks like this:



The outer ring consists of 4 controls: Previous, Next, Select, and Go Back.

The center ring rotates. Rotating counterclockwise is the same as pressing the Previous button. Rotating clockwise is the same as pressing the Next button. While the rotating ring performs the same functions as the Previous / Next buttons, it is a little faster to use.

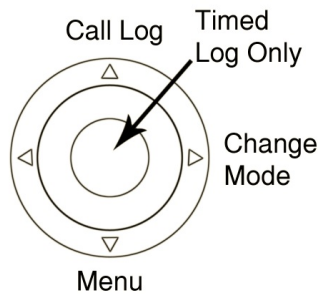
The center of the switch is a button. Most of the time the center button functions the same as pressing the Select button.

Using the Navigation Switch to Select a Function

When Scammer Jammer is in its top menu:

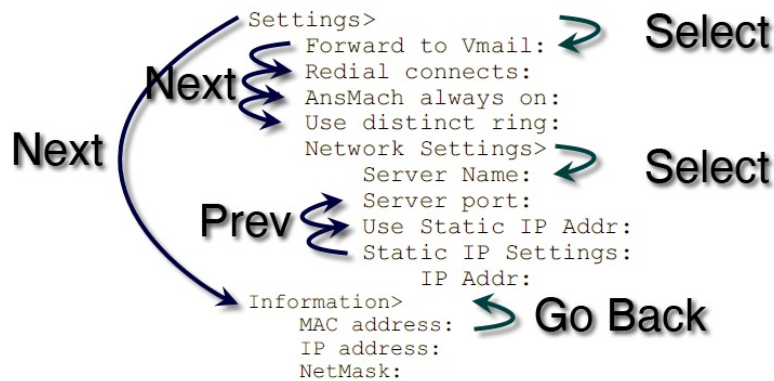
```
Scanner Jammer  
On
```

then the controls are used to jump directly to the most common functions.



Using the Navigation Switch to Navigate the Menus

Use the Prev, Next, Select, and Go Back keys to Navigate the menu like this:



As you can see Next / Previous goes thru the items in a menu. Use Select to go into a menu (menus end with >) and use Go Back to exit out of a menu.

Using the Navigation Switch to Change Settings

While menus end with >, menu items end with a : For example:

```
Forward to VMail:
Off
```

You change the value of items by using the Select button. Press Select and the : changes to a ?:

```
Forward to VMail?
Off
```

If the : does not change to a ?, then you cannot change the value of that item.

Once you see the ?, you can use Previous / Next to change the value:

```
Forward to VMail?  
On
```

Once you are happy with your change press Select and that makes the change permanent. You will see the ? return to :

```
Forward to VMail:  
On
```

If you change your mind, press the Go Back button and that will cancel the change.

Many of Scammer Jammer's settings contain short lists you can easily step thru using previous / next. There are a few exceptions.

Using the Spinner to Quickly Change Values

Some items can have a large range of values such as:

```
Server Port:  
11183
```

The server port could be anywhere from 1024 to 65,000. It would take a long time to get from 1024 to 11183 pressing the up button.

The middle ring that rotates (the spinner) acts like Previous / Next. When you start spinning it it will increment by 1's then 10's, then 100's the longer you spin it. This allows you to quickly go up and down large numbers.

Changing Text Values

Changing text with a navigation button is tedious at best. Fortunately there are only a few configuration items that contains text and it is unlikely you will need to change them.

The Server name is one of the configuration items that requires text:

```
Server name:  
SJS.XYFYX.COM
```

When you press the select button for a text menu item, only the text is shown, on the first line of the LCD display:

```
SJS.XYFYX.COM
```

You will notice a cursor under the first character. Use Go Back / Select to move the cursor left and right. Use Prev / Next to change the letter.

Since Go Back and Select are used to move the cursor, the center Select button will pop up a mini menu:

```
SJS.XYFYX.COM  
Save Changes?
```

Use Prev / Next to cycle thru the mini menu. Use Select to do the mini menu action or Go Back to return to editing the text.

The mini menu actions are:

- **Save Changes?** Saves the changes to the text and exits text edit mode.
- **Set to Default?** Don't want to slowly enter SJS.XYFYX.COM? This will set the text to that value for you.
- **Clear All?** Clears all text so you can start over.
- **Continue Editing?** Return to editing the text.
- **Delete Character?** Delete the character selected by the cursor.
- **Insert Character?** Insert a character to the LEFT of the cursor.
- **Cancel Changes?** Exit text edit mode.

Set Primary Scammer Jammer Settings

There are four primary configuration settings that need to be set properly depending upon how you will be using Scammer Jammer. These four settings are at the beginning of the Settings menu:

```
Settings>
Forward to Vmail:
Redial connects:
AnsMach always on:
Use distinct ring:
```

Here is a brief explanation of each setting. A full explanation can be found in the [Settings Menu](#) appendix.

Forward to VMail	If you are using VMail, this should be set to ON, otherwise OFF
Redial connects	If ON, callers can bypass Scammer Jammer by calling back immediately.
AnsMach always on	Set this to off for now, and you may change it after you review the section on answering machines.
Use distinct ring	If you have multiple phone numbers sharing the same phone line, each will have a different ring pattern, called distinct ring. If you are using distinct ring, you must turn this ON.

This table walks you thru the process of changing the primary configuration settings. It tells you exactly which button to press for each prompt displayed.

LCD Display	Press Button	Notes
Scammer Jammer On	Next / Settings	The Settings button take you into the Main menu.
Settings>	Select	Pressing select here goes into the Settings Menu, and the first setting will be Forward to VMail.
Forward to VMail: OFF	Select	Pressing select here allows you to change the setting's value.
Forward to VMail? OFF	Prev/Next	Press Previous or Next button until you get the proper settings. In this example we will set it to on
Forward to VMail? ON	Select	Pressing Select saves the setting
Forward to VMail: ON	Next	Go to next menu Item
Redial Connects: OFF	Next	Most will not want to enable this, so we will skip to the next settings. If you want to change it, press select and then use Prev/Next/Select to change and save.
AnsMach always on: OFF	Next	As with Redial Connects, most will not want to turn this on, so just press Next to go to next setting.

LCD Display	Press Button	Notes
Use distinct ring: OFF	Go Back	As with Redial Connects, most will not want to turn this on. You are done making configuration changes, so you use Go back to exit the settings menu.
Scammer Jammer On		

Find the Serial Number

Scammer Jammer's serial number is the *MAC Address* of the network module. You will need to know the serial number / MAC Address of your Scammer Jammer so you can properly register it with the server.

The following table walks you through the process of locating the serial number. It tells you exactly which button to press for each prompt displayed.

LCD Display	Press Button	Notes
Scammer Jammer On	Next / Settings	Go into the main menu.
Settings>	Next	Go to next item.
Information>	Select	Go Into the Information menu.
MAC address: xx:xx:xx:xx:xx:xx		Carefully write down this string for later use.
	Go Back	You are done, and Go Back will exit the menu.
Scammer Jammer On		

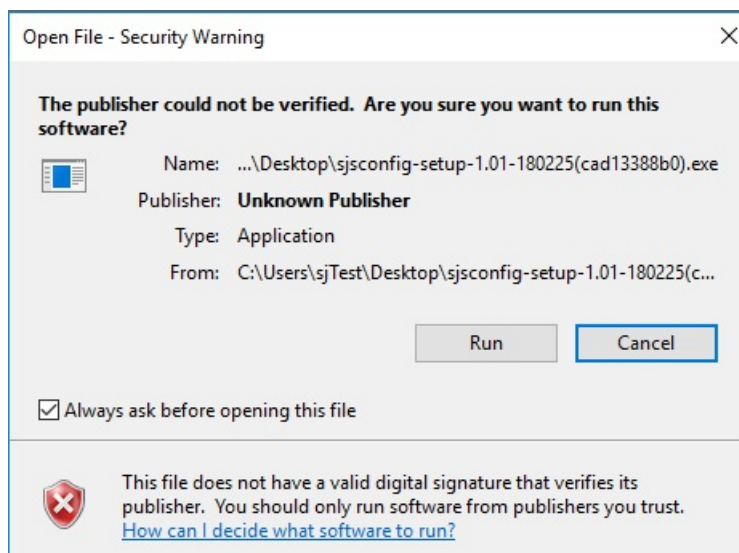
Install Sjsconfig

You will either be supplied a web link to the sjsconfig program or an installation CD.

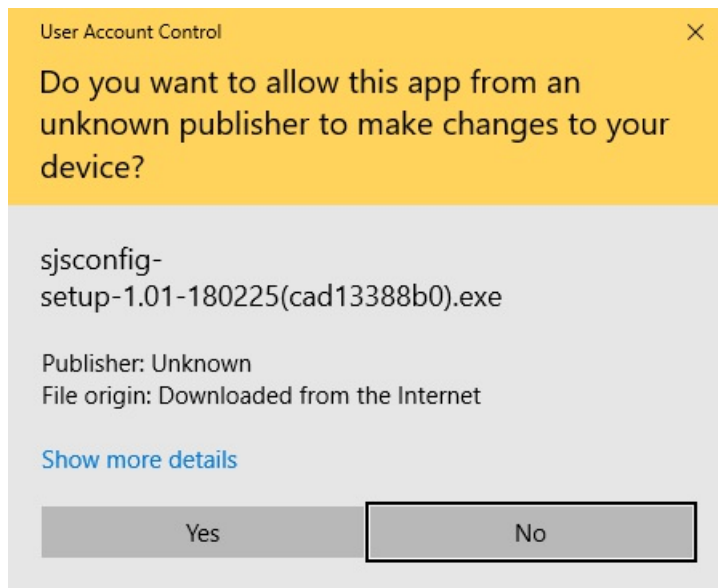
Double click on the installation program (the name for the program you have will be somewhat different).



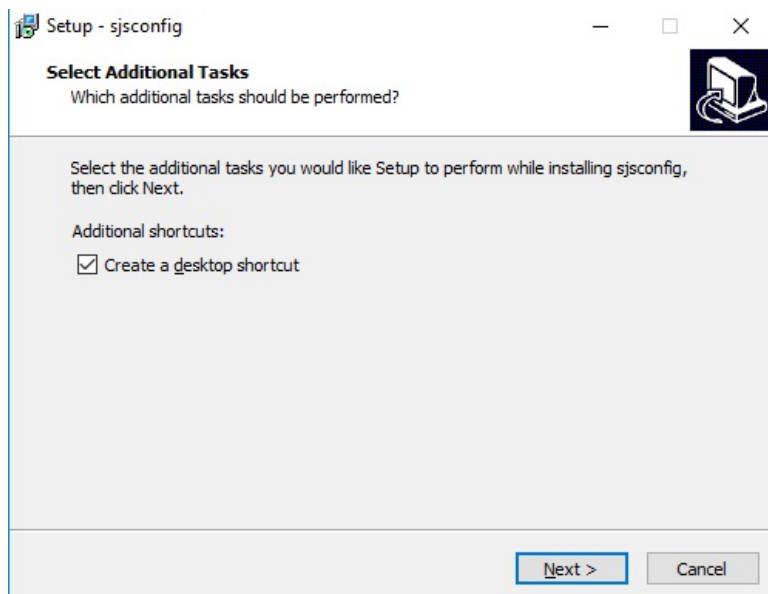
You will see:



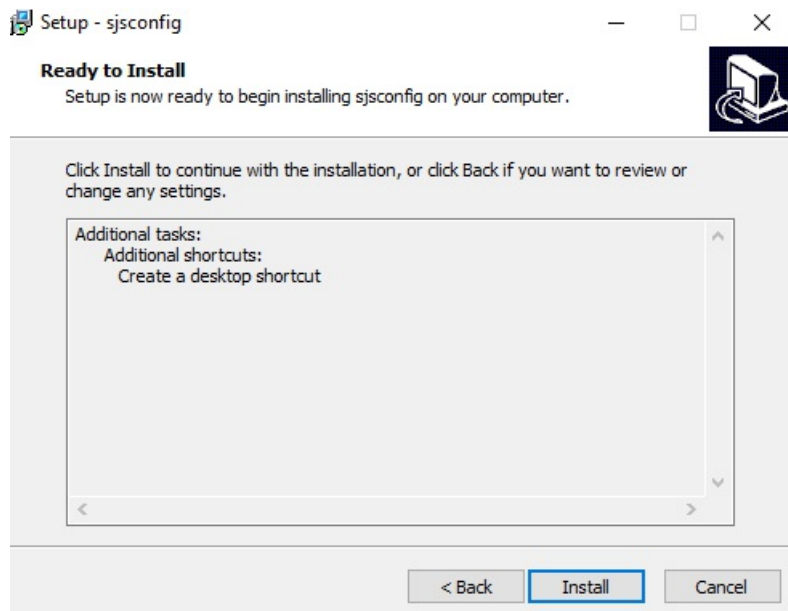
Click on the **Run** button. You will see:



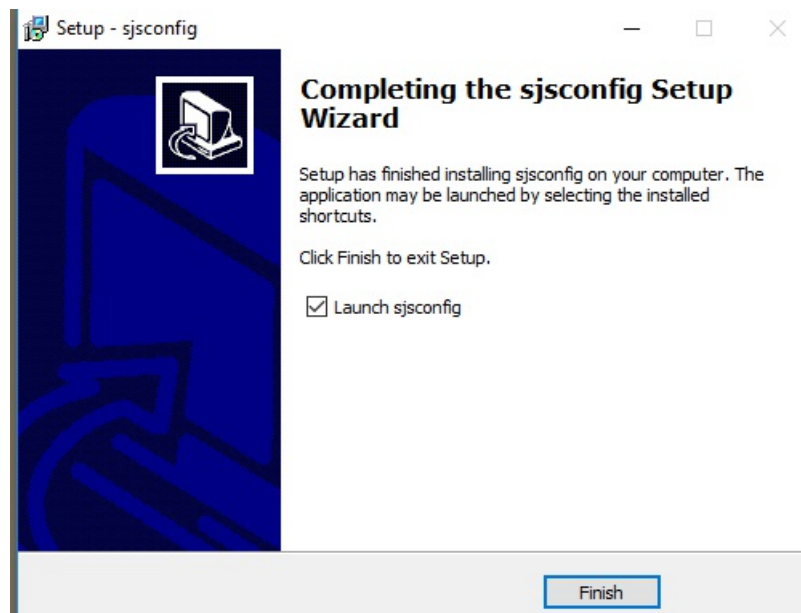
Click on the **Yes** button, you will see:



It is recommended you mark **Create a desktop shortcut**. Then click on **Next**. You will see:



Click on the **Install** button. The installation will proceed and when done you will see:



Click on the **Finish** button and sjsconfig will start, OR double click on its icon on the desktop:



You will see the login window:

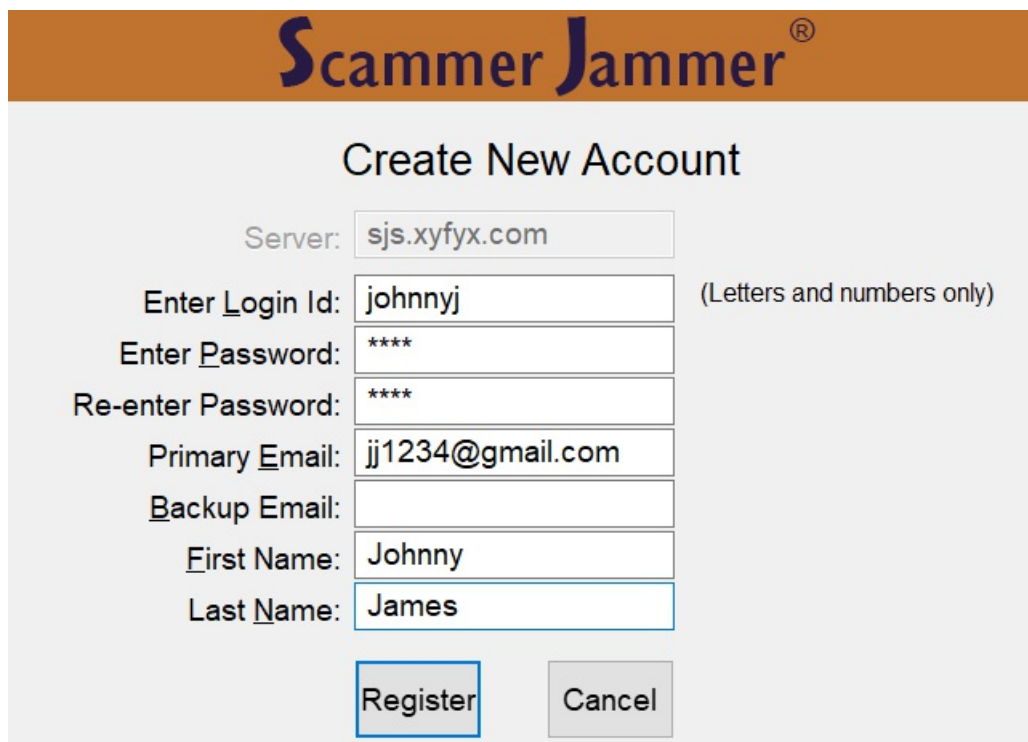
A screenshot of the Scammer Jammer SJS Login window. The window has a title bar with the Scammer Jammer logo and the text "SJS Login". The main content area has a dark blue header with the "Scammer Jammer" logo. Below the header, the text "Login to Server" is centered. There are three input fields: "Server:" with the value "sjs.xyfyx.com", "Login Id:" with the value "johnnyj", and "Password:" with the value "****". Below the input fields, there are three checkboxes: "Save Password" (checked), "Auto Logon" (unchecked), and "Start in Call History Log" (unchecked). At the bottom, there are five buttons: "OK", "Cancel", "New", "About", and "Forgot". The "OK" button is highlighted with a blue border.

Creating a New Scammer Jammer Account

Scammer Jammer must communicate with the Scammer Jammer Server (SJS). To allow this, you must create an account on the server and then add your Scammer Jammer's serial number. First, let's add your account.

Unless you've been otherwise instructed, the server should be *sjs.xyfyx.com*.

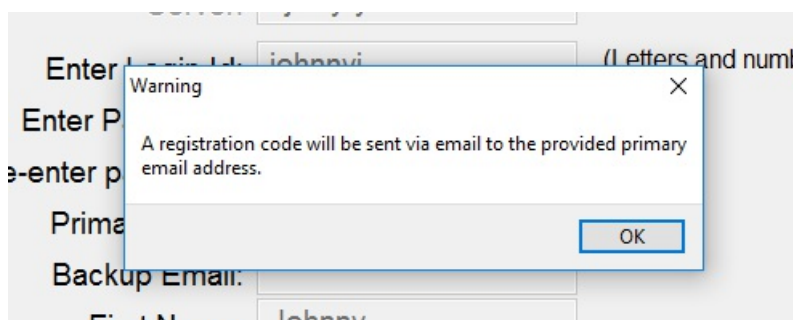
Click on the **New** button. You will see:



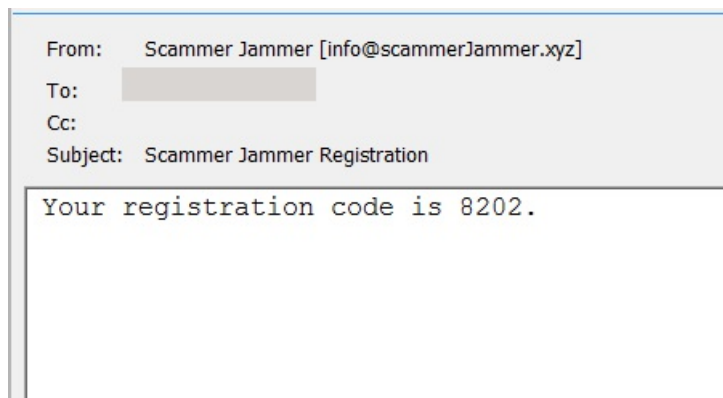
The image shows a web form titled "Scammer Jammer" with a registered trademark symbol. Below the title is the heading "Create New Account". The form contains several input fields: "Server:" with the value "sjs.xyfyx.com"; "Enter Login Id:" with the value "johnnyj" and a note "(Letters and numbers only)"; "Enter Password:" with four asterisks; "Re-enter Password:" with four asterisks; "Primary Email:" with the value "jj1234@gmail.com"; "Backup Email:" which is empty; "First Name:" with the value "Johnny"; and "Last Name:" with the value "James". At the bottom of the form are two buttons: "Register" and "Cancel".

- You must enter a **login id**. You can only use letters and numbers for the login Id.
- You must also enter a **password**. You can use anything for the password, BUT you must retype it exactly the same when you go to login.
- You must enter a **primary email** address. An account creation verification email is sent to this email address.
- The **backup email** address is optional. Should you need to reset your account, a new password is sent to BOTH email addresses.
- First name, last name are optional.

Once you have filled out the Create New Account window, press the **Register** button. You will now see:



Check your **email box** for an email from Scammer Jammer. It shouldn't take more than a few minutes. You will receive an email much like this:



Now, enter the **registration code** into the registration code box:

and press the **Confirm** button. If you don't receive the email, or have some other issue, you can press the **Do Over** button to change the registration fields and then request a new email.

When you press on **Confirm** with a valid registration code, you will be returned to the login window with your user name already filled in for you:



The image shows a window titled "SJS Login" with the "Scammer Jammer" logo at the top. The main heading is "Login to Server". Below this, there are three input fields: "Server:" with the value "sjs.xyfyx.com", "Login Id:" with the value "johnnyj", and "Password:" with the value "****". Below the input fields, there are three checkboxes: "Save Password" (checked), "Auto Logon" (unchecked), and "Start in Call History Log" (unchecked). At the bottom, there are five buttons: "OK", "Cancel", "New", "About", and "Forgot". The "OK" button is highlighted with a blue border.

Server: sjs.xyfyx.com

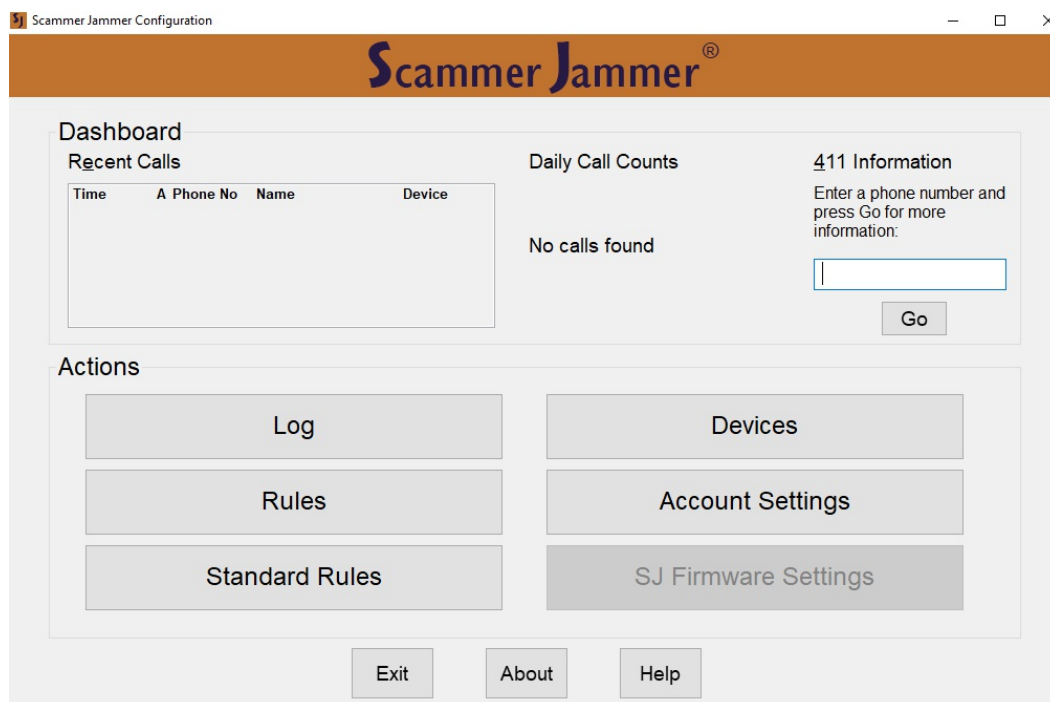
Login Id: johnnyj

Password: ****

☒ Save Password ☐ Auto Logon ☐ Start in Call History Log

OK Cancel New About Forgot

Enter your **password**. You may also click on the **Save Password** box so you don't have to re-enter your password in the future. Click on **OK** to login. You will see the main window:



The image shows a window titled "Scammer Jammer Configuration" with the "Scammer Jammer" logo at the top. The main heading is "Dashboard". Below this, there are three sections: "Recent Calls", "Daily Call Counts", and "411 Information".

Recent Calls

Time	A Phone No	Name	Device
------	------------	------	--------

Daily Call Counts

No calls found

411 Information

Enter a phone number and press Go for more information:

Go

Actions

Log Devices

Rules Account Settings

Standard Rules SJ Firmware Settings

Exit About Help

Adding a Scammer Jammer Device to an Account

Click on the **Devices** button to add a new Scammer Jammer. You will see:

Device Settings

Scammer Jammer®

SJ Device Settings

Device Name:

MAC Addr:

Default Action:

Phone No:

Your timezone:

Daylight Savings:

SJ is Active:

Master Device:

☐ Except From: To:

Days: ☒ S ☒ M ☒ T ☒ W ☒ T ☒ F ☒ S

Use Scammer Detection:

Detector Sensitivity:

Scammer Action:

Reject Call if Score >=

Days to Keep Log Data:

and age in days <

Extended Cnam Lookup:

To begin using Scammer Jammer, only a few of these fields needs to be set:

- You must enter a **device name** to identify your Scammer Jammer, but it can be anything you wish.
- You **must** enter a MAC Address. This is the *serial number* of your Scammer Jammer that you already recorded. You **must** enter the correct MAC Address assigned to your Scammer Jammer; otherwise, it will fail to connect to the server.
- **Phone number** is optional, but useful. This is the phone number of the telephone line connected to your Scammer Jammer.
- You should adjust the **time zone** and indicate if you observe **daylight savings**; otherwise, times of calls will not appear correct in the log.
- You do not need to change any other fields from their defaults and shouldn't until you understand what they do.

Click on the **save** button.

Place a Test Call

Let's make sure your Scammer Jammer is functioning properly.

First, pickup the telephone handset you connected to your Scammer Jammer. You should hear dial tone like usual and the LCD on the Scammer Jammer will read:

```
Scanner Jammer  
Outbound Call...
```

Now hang up and place a test call from another telephone, such as your cell phone.

When the call comes in, on the Scammer Jammer LCD you will first see

```
Scanner Jammer  
Inbound Call...
```

Once the Caller Id of the caller becomes available, it will show something like

```
?WIRELESS  
210-555-1212
```

Then your phone will ring, with the same caller Id name (including the leading question mark):

```
?WIRELESS  
210-555-1212
```

You must have a ? in front of the caller name. That means Scammer Jammer is working.

If instead of ? you see:

! (exclamation point): This means Scammer Jammer could reach the server. There is a network problem. Make sure your network connection is correct. You should see a green light on your Scammer Jammer's network jack.

| (vertical bar): This means the server didn't recognize your Scammer Jammer - authentication failed. Make sure you entered the proper MAC Address / serial number in sjsconfig and double check it is active:

SJ Device Settings

Device Name:

MAC Addr:

Default Action:

Phone No:

Your timezone:

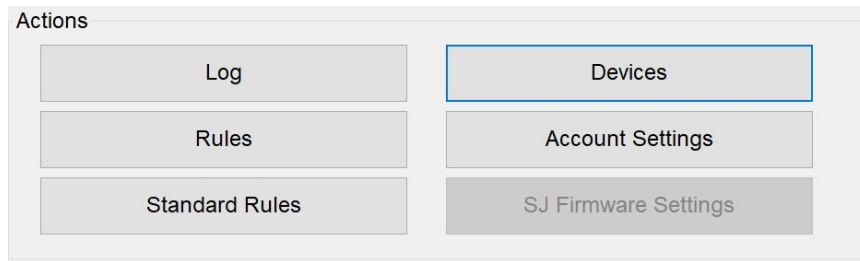
Use Daylight Savings:

SJ is Active:

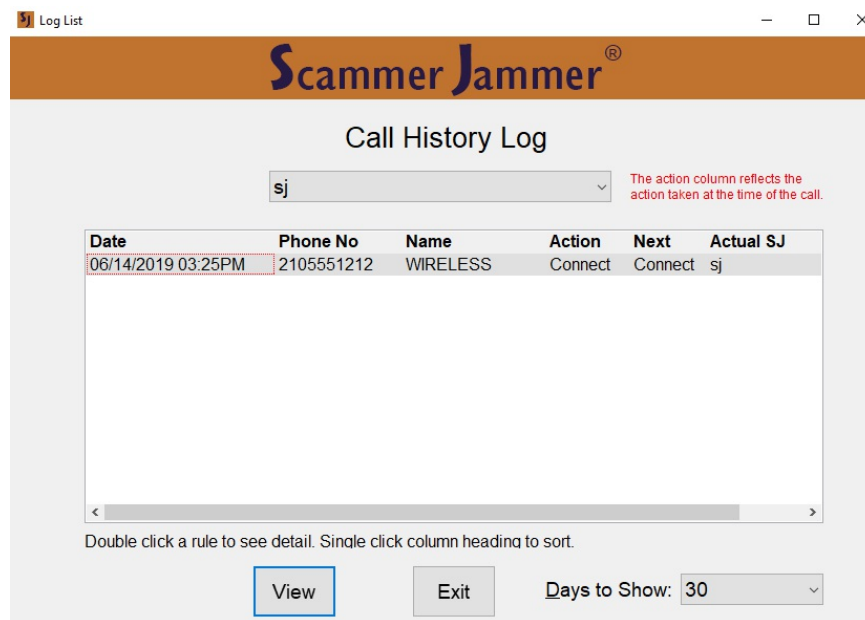
Master Device:

Review the Log in sjsconfig

In sjsconfig, click on the **Log** button:



You will now see the log of calls for your Scammer Jammer and you should see your test call:



Using an Answering Machine with Scammer Jammer

If you use voice mail, which is recommended, you can skip this section, and go to [Testing Voice Mail / the Answering Machine](#).

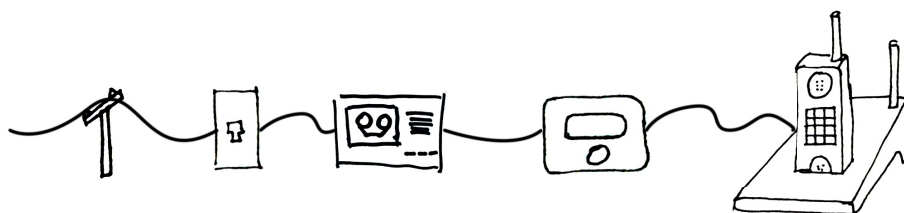
If you don't use voice mail, then you will need to set up an answering machine. Read on.

There are 3 ways to set up an answering machine on Scammer Jammer:

Method	Explanation
1. Answering Machine Connected before Scammer Jammer	If you don't have voice mail, this is the recommended setup. It gives you the same flexibility as voice mail.
2. Answering Machine Built into Telephone	This answering machine has limitations. You cannot <i>forward</i> calls because the handset and the answering machine are one in the same.
3. PBX or Answering Machine Connected to Answering Machine Jack	This setup is primarily used for PBX / special equipment.

If possible, the most useful and easiest solution is #1. It requires an external answering machine, but they are quite inexpensive.

Answering Machine Connected before Scammer Jammer



The answering machine works like voice mail. A call rings both the answering machine and Scammer Jammer. If the call isn't picked up after a predetermined number of rings, the answering machine answers.

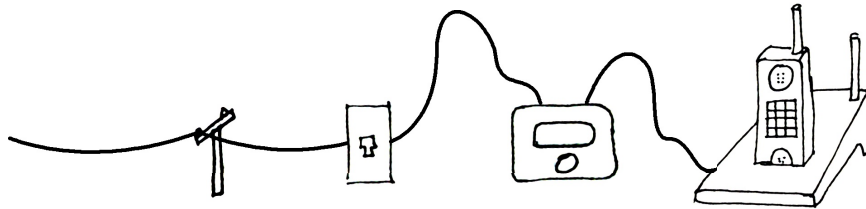
If a call is to be forwarded to the answering machine, Scammer Jammer just lets the call ring until the answering machine picks up. The handset never rings.

Settings

To use this option, set `Forward to VMail` to ON as outlined above in [Set Primary Scammer Jammer Settings](#).

Answering Machine Built into Telephone

Many wireless handsets have a built-in answering machine:



Using an built-in answering machine has certain limitations. You **cannot** forward calls to an answering machine without ringing the handset.

There are two situations where using a built-in answering machine is acceptable:

- Use Scammer Jammer to **only** block scammers. Unknown callers are allowed to ring the phone.
- Scammer Jammer to blocks **all** numbers except for those you allow to connect.

Settings

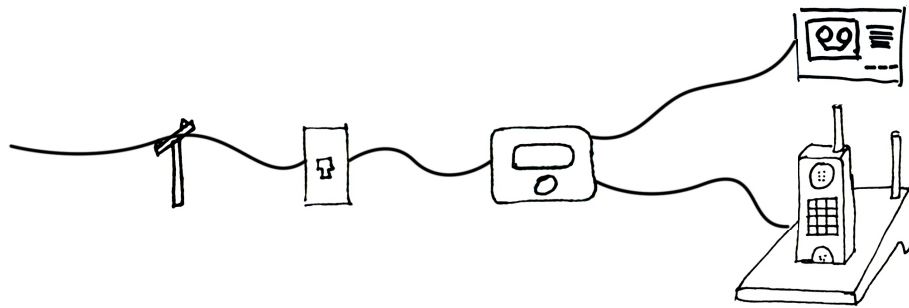
- In sjsconfig, set **Default Action** to **Connect** if blocking only scammers. Set to **Block** if blocking all callers except known callers.

SJ Device Settings	
<div></div>	
Device Name: <input type="text"/>	Your timezone: PST <div></div>
MAC Addr: <input type="text"/>	Use Daylight Savings: Yes <div></div>
Default Action: Connect <div></div>	SJ is Active: Yes <div></div>
Phone No: <input type="text"/>	Master Device: *NONE* <div></div>

- Rules should **never** use the **forward** action.
- Use mode **Block-Only** to guarantee the forward action is ignored. See [Modes - Alter the Processing of Actions](#) on using modes.

Scammer Jammer
Connect Forwards

PBX or Answering machine Connected to Answering Machine Jack



Calls that are *Forwarded* can be sent to the Scammer Jammer's Answering Machine port.

This allows Scammer Jammer to function with certain PBXs. You may also connect an answering machine to this port.

Caller Id information is **not** sent to the PBX or answering machine.

When a call is forwarded, Scammer Jammer will connect the call to the Answering Machine jack. The call can be fed to another port on the PBX that sends all calls to its own voice mail.

Settings

To use this option, set `Forward to VMail` to OFF as outlined above. See [Set Primary Scammer Jammer Settings](#).

Testing Voice Mail / the Answering Machine

Now that it is configured, let's force a call through the answering machine to verify it works.

LCD Display	Press Button	Notes
Scammer Jammer On	Select / Mode	Initiate changing the mode.
Mode ? On	Next	Change from On to Forward Connects
Mode ? Forward Connects	Select	Select Forward Connects
Scammer Jammer Forward Connects		Scammer Jammer will now FORWARD all calls that would normally connect.

Now place a call to your Scammer Jammer. On the Scammer Jammer display you will see:

Scanner Jammer
Inbound Call...

followed momentarily by your caller Id information which might look something like

?Your Name
nnn-nnn-nnnn

Your telephone should never ring and the answering machine will pick up.

IMPORTANT - Restore your Scammer Jammer back to **On** mode:

LCD Display	Press Button	Notes
Scanner Jammer On	Select / Mode	Initiate changing the mode.
Mode ? Forward Connects	Previous	Change from Forward Connects to On
Mode ? On	Select	Select On
Scanner Jammer On		Scammer Jammer is back in normal mode.

Scammer Jammer is **now configured** to block known scammers, telemarketers, telephone polls, political callers, charities, etc.

Using Scammer Jammer

Once Scammer Jammer is running, using the unit itself is easy.

When Scammer Jammer is Idle, you will see:

```
Scanner Jammer  
On
```

When you are making a call, you will see:

```
Scanner Jammer  
Outbound call...
```

When a call comes in, you will see

```
Scanner Jammer  
Inbound call...
```

and once the Caller Id information is available you will see that instead on both the Scammer Jammer unit **and** on the telephone handset if it rings.

```
?Caller Name  
nnn-nnn-nnnn
```

Call Indicator

The ? shown in the example above is the **call indicator**. The call indicator gives you extra information about the call. The most common call indicators are:

Indicator	Meaning
+	Connect Caller (known caller) - there is a rule to connect this caller to the handset and let it ring.
-	Block Caller - There is a rule to block the caller from being connected or forwarded.
\$	The caller is a telemarketer. Typically these calls are blocked.
?	Unknown Caller or Forward Caller - Either there is no rule that applies to the caller or the rule is to forward it to voice mail. In general, if a number isn't known (+) or blocked (- or \$), then it is unknown (?).
!	Network Failure - Scammer Jammer was not able to communicate with the server. When this happens, the call is always connected.

Inbound calls with the call indicator always show up on the Scammer Jammer. They will only show up on the handset if the phone rings.

Call Log

The Scammer Jammer Call Log allows you to review prior calls. You can also use the call log to set rules for callers.

The call log is reset when Scammer Jammer is restarted.

This example shows how to enter the call log and review calls:

LCD Display	Press Button	Notes
Scanner Jammer On	Previous / Call Log	Enter the call log
Wireless 210-555-1212	Previous or Next	Once in the call log you can use Previous and Next to scroll through the call log
John Smith 666-233-5959	Goback	Use GoBack to Exit the call log
Scanner Jammer On		

Creating or Changing a Rule using the Call Log

This example shows how to change a phone numbers rule:

LCD Display	Press Button	Notes
Scanner Jammer On	Select / Mode	Enter the call log
Wireless 210-555-1212	Select	Pressing Select lets you change the rule. After pressing connect, you will see the Caller Name and the current action for that caller - in this case connect .
Wireless Action? Connect	Previous or Next	By pressing Previous or Next, the action will change between connect , forward , and block . For this example, we will select forward.
Wireless Action? Forward	Select	Pressing Select will create a new rule or change the existing rule to now forward calls coming from 210-555-1212.
Scanner Jammer On		

After changing the rule from Scammer Jammer, you can use the same procedure as above to go back and review your change like this:

LCD Display	Press Button	Notes
Scanner Jammer On	Select / Mode	Enter the call log
Wireless 210-555-1212	Select	Pressing Select lets you change the rule
Wireless Action? Forward	Go Back	Verify the action is forward then press Go Back to return to main menu.
Scanner Jammer On		

As discussed in the sjsconfig section of this manual, you can also review (and set) rules. This rule appears like this in sjsconfig:

Rule Definition

Rule: 2105551212

Name Override:

Action: Forward

Rule is Active: Yes

Comment:

Save Cancel New Delete

Using sjsconfig

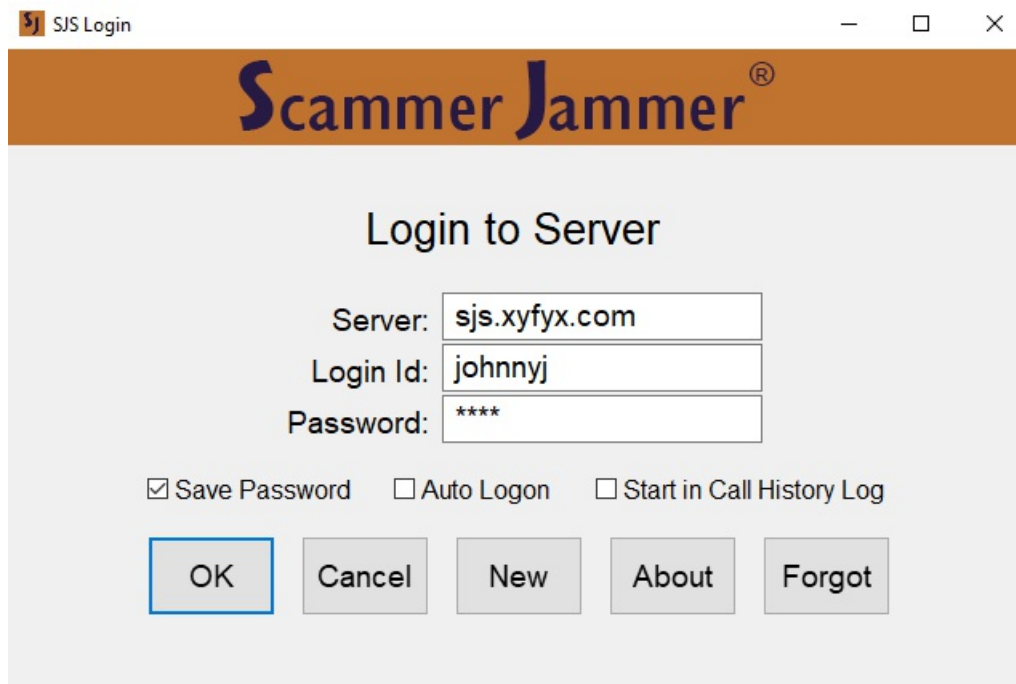
sjsconfig is the windows-based program used to view and configure settings on the Scammer Jammer server.

The Scammer Jammer server is responsible for determining which rule will apply to a call. It also contains information about your account, your Scammer Jammer devices, and a log of calls made to your Scammer Jammer.

If not already installed, see [Install sjsconfig](#).

Logging in to the Scammer Jammer Server

When you first start sjsconfig, you will be shown the login window:



You should always use **sjs.xyfyx.com** as the server name.

sjsconfig will **remember the last login** Id you used.

If you check the **Save Password** box, the password will be remembered for you. Be advised that if you decide to save your password, it will be stored on disk where it could be retrieved by others.

If you check the **Auto Logon** box, the next time you run the sjsconfig program, it will skip the logon window if the username/password are correct.

If you check the ***Start in Call History Log***, then every time you start Scammer Jammer and login, the Call History Log will be displayed automatically.

Press the **OK** button to login.

If you need to create a new account, press the **New** button, and see [Creating a New Scammer Jammer Account](#).

Forgotten Login or Password

If you have forgotten your login id or password, you can press the **Forgot** button in the login window. This will bring up the password reset window:



Forgot Login

Scammer Jammer®

Forgotten Login or Password

Enter your login Id or your email address. Your password will be reset and the login id and new password will be sent to your email address.

Login Id: johnnyj

Email Address:

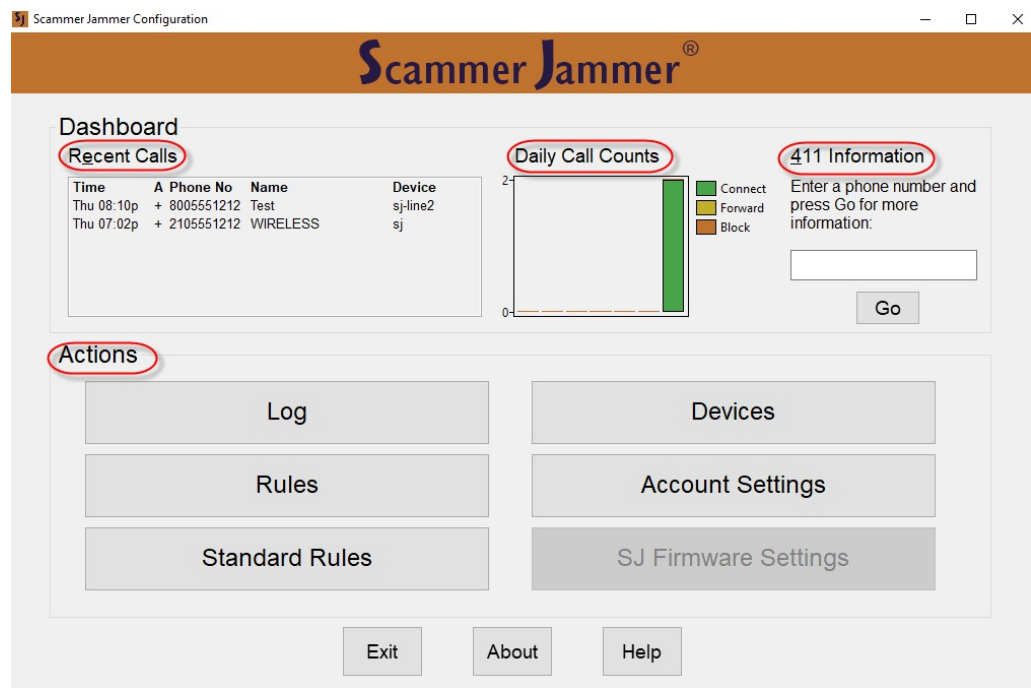
Cancel Reset

To use this window, enter either your login id or the email address with which you registered.

Once you press the **Reset button**, the Scammer Jammer server will reset your password and send an email with your login id and new password. It will **send the email to both of the email addresses** you included in your account information.

Main Window

After you login you will see the main window:

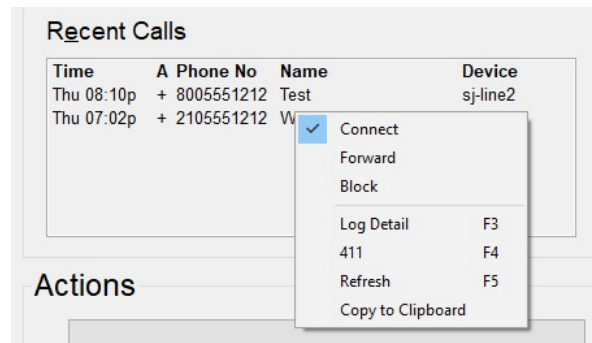


There are 4 sections to the main window:

Recent Calls

This contains a list of all recent calls to your Scammer Jammers. Press F5 at any time to update the list.

Right clicking on a line gives you a popup menu with some additional options:

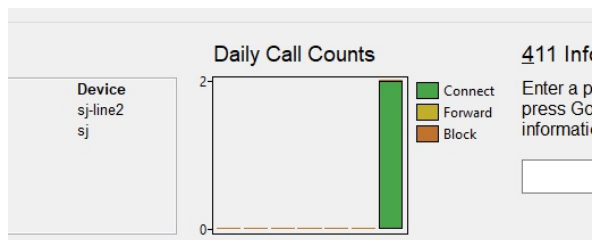


You can enable/create private rules to Connect, Forward, or Block the phone number. If you uncheck a checked action, then the associated rule is disabled, but not deleted.

You can also directly go to the Log Detail or 411 Information windows using the popup menu.

Daily Call Counts

This graph shows the types and count of call for the past 7 days:



The right-most bar is the number of calls for TODAY. So this SJ has received 2 calls today that were connected.

The bar directly left of that contains the number of calls for yesterday (of which there are zero), then the day before yesterday, etc.

411 Information

The 411 Information section of the main window is used to view the action to be taken for a telephone number. Enter a telephone number, click on Go, and further information will be displayed.

411 Information is discussed fully in [411 Information Window](#).

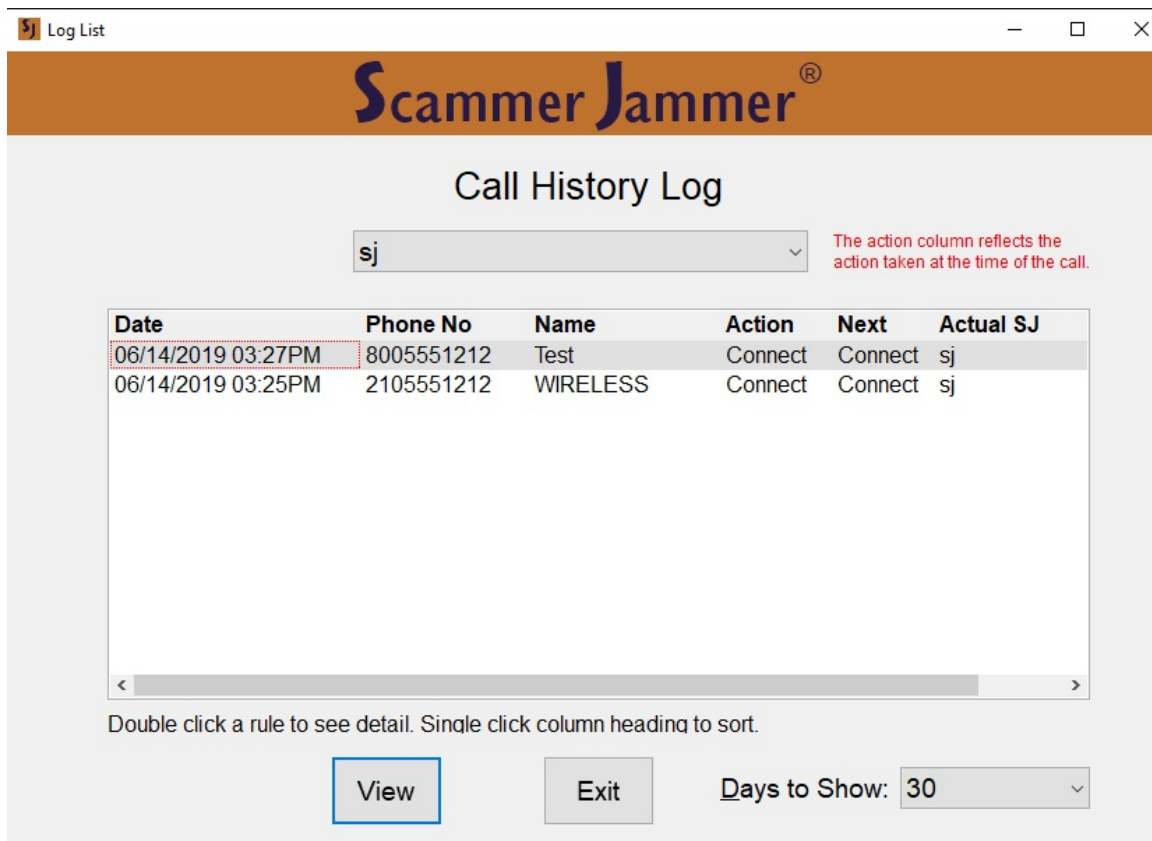
Actions

Each of the buttons in the **Action section** of the main window will take you to a new window where you can further view or change Scammer Jammer server settings.

Call History Log Window

The Call History Log window allows you to see all of the calls that have been received, and view details for those calls.

From the main window, if you click on the Log button you are taken to the Call History Log window:



In the Call History log, you can see the date & time of each call, the calling telephone number, the name of the caller, and the action taken.

You can go **back further** in the log by changing *Days to Show*.

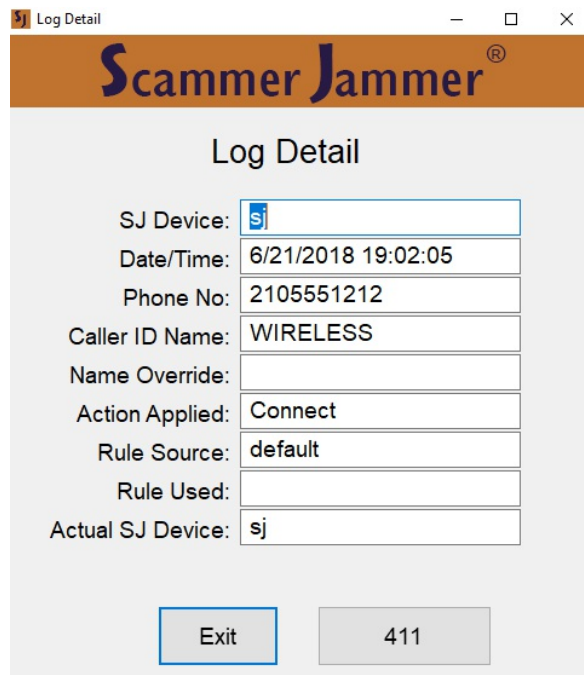
A call's action in the Call History log **reflects the action taken at the time of the call**. If the action for caller 2105551212 is changed to Block, it will still show in the call history log as Connect.

You can **sort** on columns by single clicking on a column name.

Double-click on a call to see the Log Detail window.

Action verses **Next** columns: The Action column indicates the Action performed WHEN the call occurred. The Next column indicates how the call would be handled if it were to call right now.

Log Detail Window



SJ Device:	<input type="text" value="sj"/>
Date/Time:	<input type="text" value="6/21/2018 19:02:05"/>
Phone No:	<input type="text" value="2105551212"/>
Caller ID Name:	<input type="text" value="WIRELESS"/>
Name Override:	<input type="text"/>
Action Applied:	<input type="text" value="Connect"/>
Rule Source:	<input type="text" value="default"/>
Rule Used:	<input type="text"/>
Actual SJ Device:	<input type="text" value="sj"/>

The Log Detail window will show everything Scammer Jammer server has recorded about the call include the date, time, calling phone number, caller ID name, name override, and the action.

Like the Call History Log, the Log Detail shows how the call **was** handled. If you want to know how the call **will be** handled, press the 411 button. 411 Information is discussed in [411 Information Window](#).

Rule Source is discussed in [Rule Sources and Source Order](#).

Actual SJ Device is discussed in [Master Scammer Jammer Units](#).

411 Information Window

The 411 Information window allows you to review **all available information** for any telephone number. It will tell you the current action, which rule will be applied and if the telephone number is a known scammer. You can setup rules for the telephone number or further research it.

You can get into the 411 Information window from the main window by pressing the **Go** button:

Daily Call Counts

2

0

Connect
Forward
Block

411 Information

Enter a phone number and press Go for more information:

Go

or from the Log Detail window by pressing the **411** button:

Log Detail

SJ Device:

Date/Time:

Phone No:

Caller ID Name:

Name Override:

Action Applied:

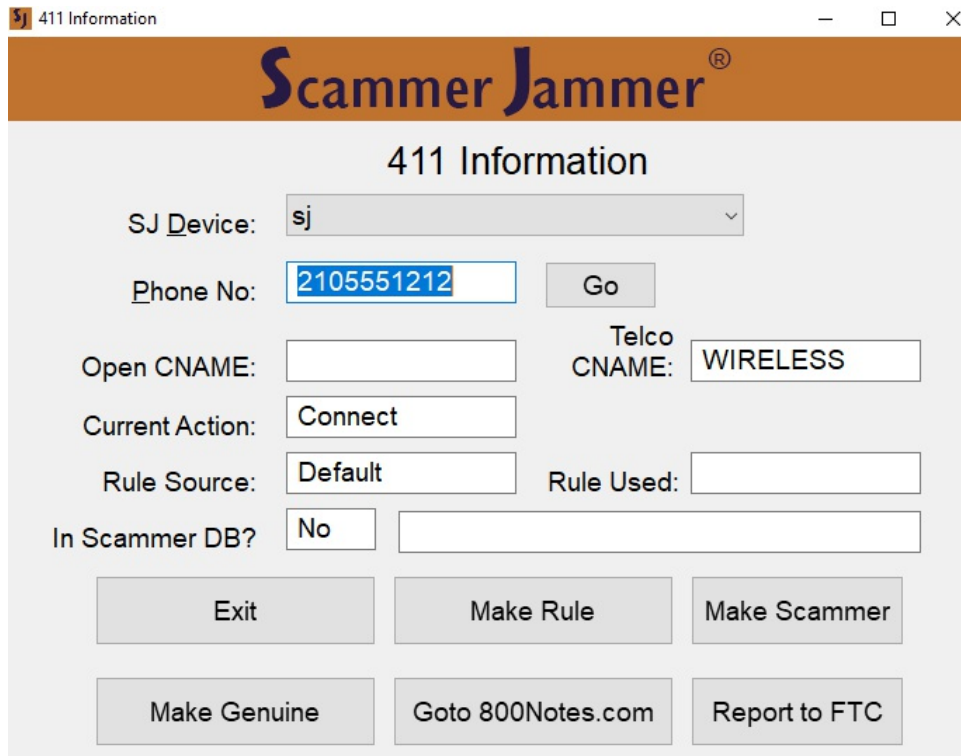
Rule Source:

Rule Used:

Actual SJ Device:

Exit 411

The 411 Information window will then appear:



411 Information

SJ Device: sj

Phone No: 2105551212 Go

Open CNAME: Telco CNAME: WIRELESS

Current Action: Connect

Rule Source: Default Rule Used:

In Scammer DB? No

Exit Make Rule Make Scammer

Make Genuine Goto 800Notes.com Report to FTC

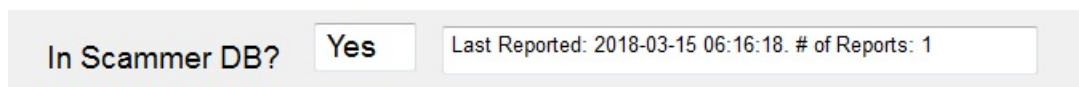
The 411 Information window tells you what the **current action will be** for a caller's phone number. In the above example, if 2105551212 calls, it will be connected to the telephone handset based on the default rule.

You can type or paste any telephone number into the Phone No field, then press the **Go** button to review the action for that telephone number.

The open CNAME and Telco CNAME values will be displayed if they are available.

Rule Source is discussed in [Rule Sources and Source Order](#).

If the phone number is in the scammer database, **In Scammer DB** will be Yes:



In Scammer DB? Yes Last Reported: 2018-03-15 06:16:18. # of Reports: 1

The buttons at the bottom of the window allow you to take further actions on the telephone number.

Make Rule

If you press the Make Rule button, you will be taken to the Rule Definition window. This window allows you to create or change a rule for the telephone number. The Rule Definition window is discussed in [Rule Definition Window](#).

Make Scammer

Scammer Jammer allows you to quickly and easily mark a telephone number as a scammer so the caller cannot call you or any other Scammer Jammer user again. Once a telephone number is marked as a scammer, **it cannot be undone!** Be sure a caller is a scammer before marking it.

For Scammer Jammer, a ‘*scammer*’ is defined as any unsolicited caller:

- Scammers
- Robo-callers
- Telemarketers
- Charities
- Political Organizations
- Pollsters
- Telephone Surveys

Some phone numbers should not be considered scammers because they may be useful to others:

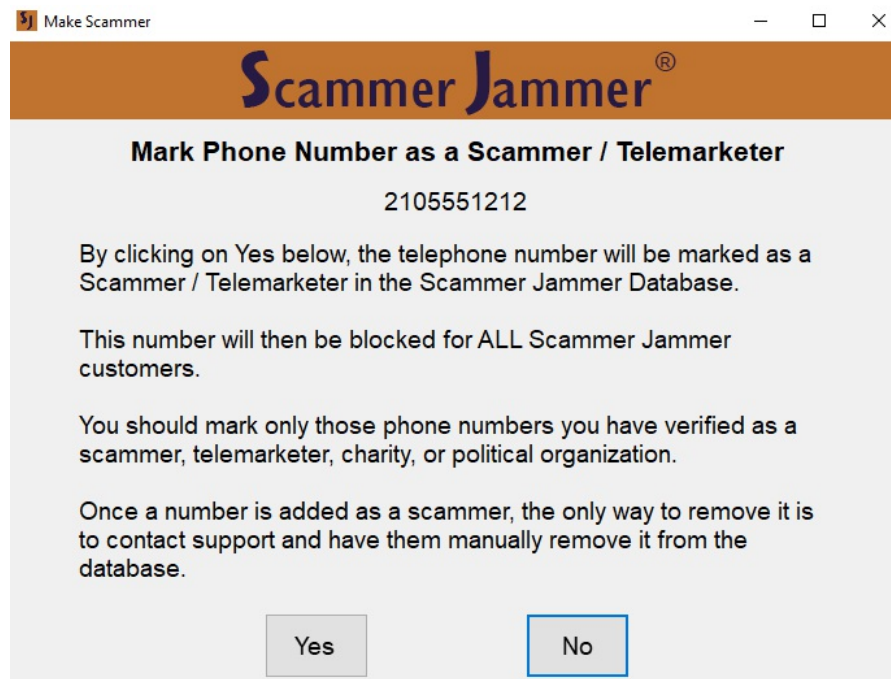
- Wrong numbers
- Spoofed numbers *
- Government Numbers
- Public Alert Numbers
- Company Customer Service

* Spoofed numbers present a unique problem which is further discussed in [Blocking Local Exchange Spoofed Calls](#).

Amazon Customer Service would be a valid phone number. Remember, if you get a call from a non-‘*scammer*’ you can still create a rule to block or forward it just for you.

You can use the **800Notes.com** button to further research a call, as outlined below, before marking it as a scammer.

When you click on the Make Scammer button you will see:



The screenshot shows a window titled "Make Scammer" with a standard Windows title bar (minimize, maximize, close buttons). The window has an orange header bar with the "Scammer Jammer®" logo. Below the header, the text "Mark Phone Number as a Scammer / Telemarketer" is displayed in bold. The phone number "2105551212" is shown in the center. Below the number, there are four lines of instructional text: "By clicking on Yes below, the telephone number will be marked as a Scammer / Telemarketer in the Scammer Jammer Database.", "This number will then be blocked for ALL Scammer Jammer customers.", "You should mark only those phone numbers you have verified as a scammer, telemarketer, charity, or political organization.", and "Once a number is added as a scammer, the only way to remove it is to contact support and have them manually remove it from the database." At the bottom of the window, there are two buttons: "Yes" and "No". The "No" button is highlighted with a blue border.

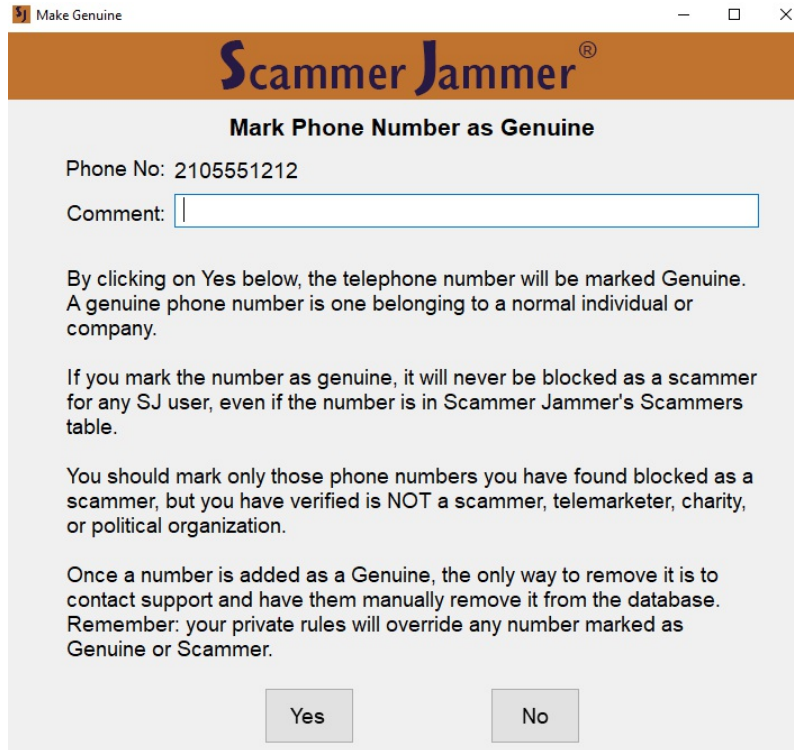
click Yes or No as desired.

Make Genuine

A *genuine* telephone number is the opposite of a *scammer*. Genuine numbers are **known to not be scammers**. Using Amazon Customer Service as an example, its telephone number should not be in the scammers database.

The source of the scammers database is the FTC Do-not-Call violations database. This database is populated by users reporting calls to the FTC (see Report to FCC button below). Unfortunately, sometimes the FTC's database is wrong. In fact, the Amazon Customer Service telephone number is in this database.

You may mark a telephone number as Genuine by pressing the Make Genuine button. You will see:



The screenshot shows a window titled "Make Genuine" with the "Scammer Jammer®" logo at the top. The main heading is "Mark Phone Number as Genuine". Below this, the "Phone No:" is displayed as "2105551212". There is a "Comment:" label followed by an empty text input field. The dialog contains several paragraphs of text explaining the process and rules for marking a number as genuine. At the bottom, there are two buttons: "Yes" and "No".

Scammer Jammer®

Mark Phone Number as Genuine

Phone No: 2105551212

Comment:

By clicking on Yes below, the telephone number will be marked Genuine. A genuine phone number is one belonging to a normal individual or company.

If you mark the number as genuine, it will never be blocked as a scammer for any SJ user, even if the number is in Scammer Jammer's Scammers table.

You should mark only those phone numbers you have found blocked as a scammer, but you have verified is NOT a scammer, telemarketer, charity, or political organization.

Once a number is added as a Genuine, the only way to remove it is to contact support and have them manually remove it from the database. Remember: your private rules will override any number marked as Genuine or Scammer.

Please enter the name or company of the owner of the telephone number in the comment field in case there are any future questions regarding the telephone number.

Then click on the Yes or No button as desired.

Goto 800Notes.com

The 800notes.com website is useful for determining if a telephone number is being used by a scammer.

When you press the Goto 800Notes.com button, your browser will start and go to the 800notes.com website, requesting information for the number you are researching:

800-555-1212

800 area code: Toll-free

Resolve financial obligations online.
Build custom payment plans and
view available discount offers. [See Offers](#)

AdChoices

mcm Midland Credit
Management, Inc.

Read comments below about 8005551212. [Report unwanted calls](#) to help identify who is using this phone number.

1 2 3 4 5 6 7 ... 36 37 38 Next

eastcoast
5 Jul 2007 | 67 replies

no message left

Reply !

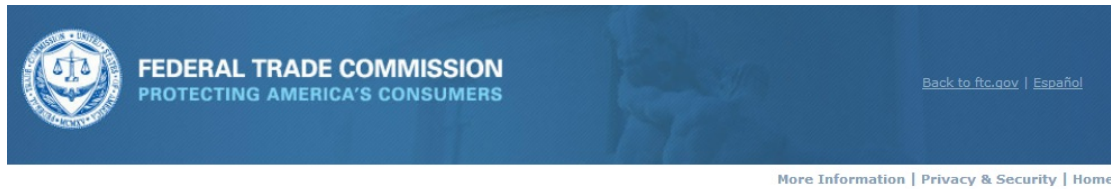
Once 800notes.com starts, you will see the telephone number at the top (800-555-1212), the number of pages of comments(1 .. 38 Next), and the oldest comments first.

If there are **no** comments, or just a couple, the telephone number is probably not that of a scammer.

In this example, there are **38 pages of comments**. Clearly, this telephone number is a scammer!

Report to FTC

If you press the Report FTC button, you will be taken directly to the FTC website where you can report the caller. The clipboard will contain the telephone number of the caller so you can paste it directly into their form.



National Do Not Call Registry

[En Español](#)

REPORT UNWANTED CALLS

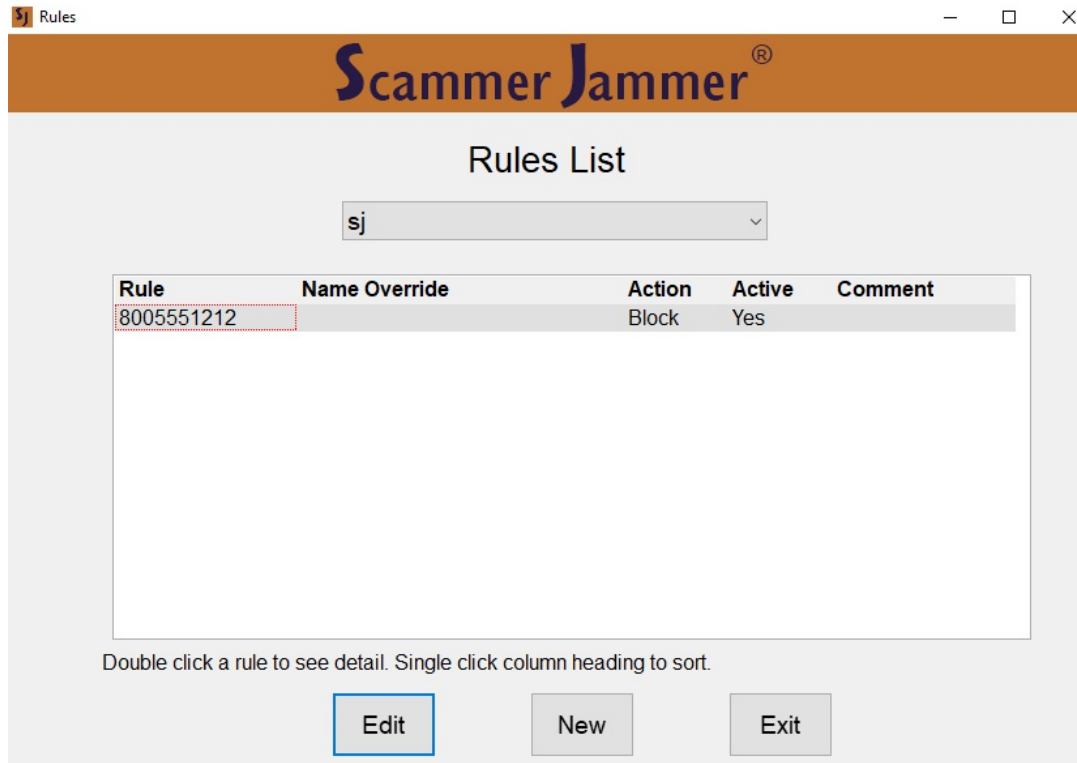


- **Do Not Call:** After your number is on the registry for 31 days, you can report unwanted sales calls.
- **Robocalls:** Report calls that use a recorded message instead of a live person (whether or not your number is on the Registry).

Rules List Window

Rules are used to assign actions to calls based on the call's telephone number.

The Rules window is used to add or change your rules. When you press the Rules button in the main window, the Rules List window is displayed



To add a new rule, press the **New** button.

To edit a rule, **double-click** the rule.

Click on a column heading to sort on that column.

Creating a new rule or editing an existing rule will display the Rule Definition Window.

Rule Definition Window

The rule definition window is used to enter a new rule or edit an existing rule.

Rule Definition

Rule: 8005551212

Name Override:

Action: Block

Rule is Active: Yes

Comment:

Save Cancel New Delete

The **Rule** is the telephone number of the caller. Typically this is a full 10 digit telephone number such as 8005551212. If you enter less than 10 digits, the rule is a partial match rule. Partial match rules are discussed in [Partial Match Rules](#).

You may also specify a caller ID name in the rule. For more information on using caller ID names, please see the section "Caller ID Name Based Rules".

The **Name Override** will be sent to your telephone handset instead of the telephone companies caller ID. It will also show up in other parts of sjsconfig to help identify the telephone number.

If a frequent caller has a caller ID of *WIRELESS CALLER* you can override it by putting his name in the Name Override. Then when he calls, his name will show up on your telephone handset.

Select the **action** you wish to take for that caller: Connect (ring the telephone handset), Forward (to voice mail), Block (disconnect the caller), or Default. See *Using the Default Action when Defining a Rule* in Advanced Topics.

If you want to temporarily disable a rule without deleting it you can set **Rule is Active** to No.

You can leave a note to yourself regarding the rule in the **Comment** field.

If you are editing an existing rule, **you can delete** it by pressing the Delete button.

Default Action

When a call is received that has no rule, the call will be assigned the default action. The default action is defined in the Scammer Jammer device settings:



Scammer Jammer®	
SJ Device Settings	
sj	
Device Name: sj	Your timezone: PST
MAC Addr: 101010101010	Daylight Savings: Yes
Default Action: Connect	SJ is Active: Yes
Phone No: 2065551212	Master Device: *NONE*

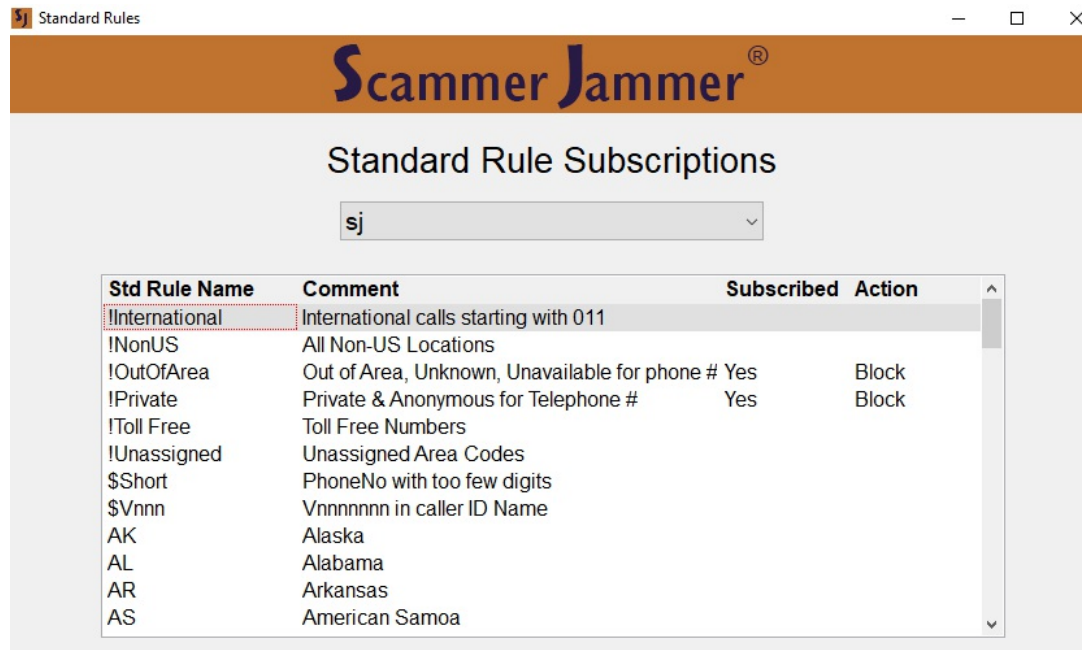
Normally the **default action is connect**. You can change it to Forward. If you change the default action to forward, all calls for which there is no rule will be sent to voice mail.

You may also change the default action to Block, but this is not recommended.

Standard Rule Subscriptions

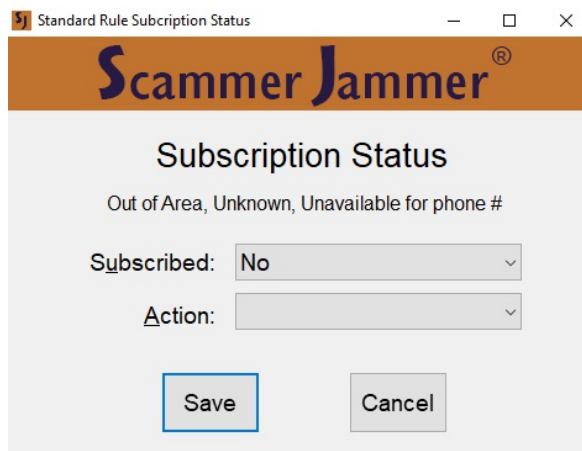
Standard Rules allow you forward or block calls from large areas such as an entire state or all international calls. There are also standard rules that can handle odd situations for which a normal rule won't work.

When you press the Standard Rules button on the main window, you will see the Standard Rule Subscriptions window:



Subscribing to a Standard Rule

To use a Standard Rule, you *subscribe* to it. Subscribing is easy. Just double-click on the rule. To subscribe to the !OutOfArea rule, double click on it and you will see:



Standard Rule Subscription Status

Scammer Jammer®

Subscription Status

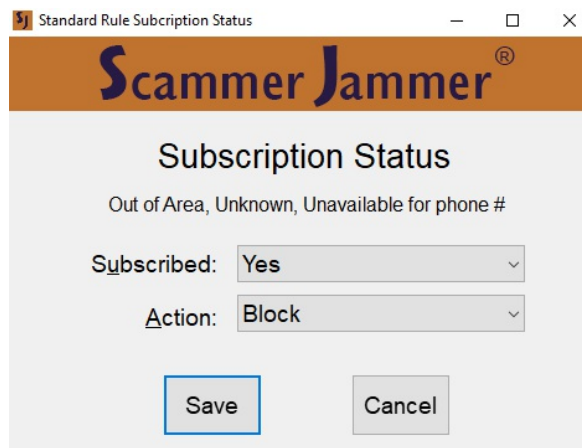
Out of Area, Unknown, Unavailable for phone #

Subscribed: No

Action:

Save Cancel

In the **subscribed box**, just change the No to Yes and the action will default to Block:



Standard Rule Subscription Status

Scammer Jammer®

Subscription Status

Out of Area, Unknown, Unavailable for phone #

Subscribed: Yes

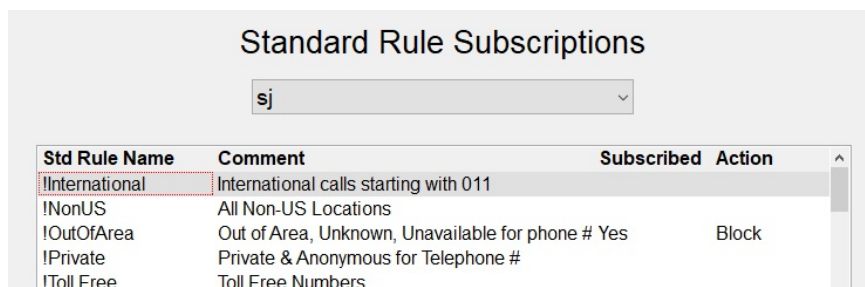
Action: Block

Save Cancel

You can **change the action** from Block to Forward or Connect. Then press the **Save** button.

Unsubscribing from a Standard Rule

Assuming you are subscribed to the !OutOfArea rule:



Standard Rule Subscriptions

sj

Std Rule Name	Comment	Subscribed	Action
!International	International calls starting with 011		
!NonUS	All Non-US Locations		
!OutOfArea	Out of Area, Unknown, Unavailable for phone #	Yes	Block
!Private	Private & Anonymous for Telephone #		
!Toll Free	Toll Free Numbers		

to **unsubscribe** from it, double-click on the standard rule and you will see:

In the **Subscribed** box, change Yes to No and press the **Save** button.

Viewing All Subscriptions

If you single click twice on the Subscribed column, it will do a **reverse sort** and all subscribed rules will be at the top:

Std Rule Name	Comment	Subscribe	Action
!OutOfArea	Out of Area, Unknown, Unavailable for phone #	Yes	Block
FL	Florida	Yes	Block
!Private	Private & Anonymous for Telephone #	Yes	Block
!International	International calls starting with 011		
!NonUS	All Non-US Locations		
!Toll Free	Toll Free Numbers		

Standard Rule Definitions

Here are the functions of the standard rules.

Std Rule Name	Purpose
!International	Use this standard rule to assign an action to any international telephone number which starts with 011.

Std Rule Name	Purpose
!NonUs	<p>Use this standard rule to assign an action to any telephone number that looks like like a U.S. telephone number (doesn't start with 011) but is international. This includes many Carribean countries such as Jamaica, Barbados, and the Cayman Islands.</p> <p>It also includes Canada.</p>
!OutOfArea	<p>Use this rule to assign an action to calls with Out of Area, Unknown, and Unavailable in the telephone number. This rule doesn't apply if the telephone number is valid.</p> <p>Some telephone companies don't provide international caller ID. You may receive international calls with Out of Area as the telephone number.</p>
!Private	Use this rule to assign an action to calls with Private or Anonymous as the telephone number.
!ScamCName	Use this rule to block various scammers based on their Caller ID Name . This will block callers such as <i>Fire Assoc, NRA, RNC</i> , etc.
!Toll Free	<p>Use this rule to assign an action to any call with a Toll free number such as 800 or 888.</p> <p>Use with care as customer service calls could use a toll-free number.</p>
!Unassigned	<p>Use this rule to assign an action to any call with an invalid area code.</p> <p>Scammers sometimes will use area codes that do not exist.</p>
\$Predict	<p>Predictive Scammer Blocking. Uses an algorithm to predict if the number is a scammer.</p> <p>It is possible this rule can have false positives (calls are incorrectly classified as scammers). While false positives are infrequent, you should FORWARD calls using this rule, not BLOCK them.</p>
\$Short	<p>Use this rule to assign an action to any call with too few digits in the telephone number. All US telephone numbers are 10 digits long. Sometimes scammers will use fewer than 10 digits. This rule will catch those calls.</p> <p>Trying to create your own rule for telephone numbers with too few digits is difficult because the rule acts as a partial match rule.</p>
\$Vnnn	<p>Some telemarketers use a long numeric string starting with V in the caller ID name such as V40216491.</p> <p>Many of these will already have been reported as a scammer, but not all. This rule will catch all such calls.</p>
360	Assign an action to all 360 area codes. This is Olympia, Washington and it the source to many political calls to other areas of the state.

Std Rule Name	Purpose
509 Onvoy	Assign an action to the area codes served by the Onvoy VoIP carrier. This carrier is a large source of scam calls in the Washinton state area.
509 Tri-Cities	Assign an action to the area codes of the Tricities in Washington state. A source of many scam calls to the rest of the Washington state area.
Cname Toll Free Call	Assign an action to any call with 'Toll Free' or 'Toll Free Call' in the caller ID <i>name</i> . Often, but not always a source of unwanted calls. It is recommended you forward, not block these calls.
Pay Services	All 900 type <i>premium rate</i> telephone numbers. Scammers will spoof such a number and leave a vague (or no) message hoping you will call back to one of these numbers and incur a large fee.
State / Country	The rest of the standard rules are geographic areas. For example, FL will allow you to assign an action to all numbers in Florida.

Recommended Subscriptions

When you first setup your account you are **not subscribed to any Standard Rules**. You should determine which standard rules best apply to your situation.

It is a good idea to **use the FORWARD action to start**. Then if you are sure there are no valid calls coming from a standard rule, you can change it to block if desired.

Most people will want to subscribe to:

!Private
!Unassigned
\$Short
\$Vnnn

If you never receive calls from Canada or the Carribean, add:

!NonUs

If you never receive international calls, add:

!OutOfArea
!International

To more aggressively block scammers, use this rule:

\$Predict

SJ Device Settings

The SJ Device Settings window is used to change the settings for your Scammer Jammer that are maintained on the server.

When you press the Devices button on the main window, you will see the SJ Device Settings window:

Scammer Jammer®

SJ Device Settings

Device Name: Your timezone:

MAC Addr: Daylight Savings:

Default Action: SJ is Active:

Phone No: Master Device:

☐ Except From: To:

Days: ☒ S ☒ M ☒ T ☒ W ☒ T ☒ F ☒ S

Use Scammer Detection: Detector Sensitivity:

Scammer Action: Reject Call if Score >=

Days to Keep Log Data: and age in days <

Extended Cnam Lookup:

Selecting a Device to Change

If you have more than one Scammer Jammer, select the one you wish to modify:

Scammer Jammer®

SJ Device Settings

Device Name:

MAC Addr: Daylight Savings:

Common Settings

The most common settings are in the first section:

Device Name:	<input type="text" value="sj"/>	Your timezone:	<input type="text" value="PST"/>
MAC Addr:	<input type="text" value="101010101010"/>	Use Daylight Savings:	<input type="text" value="Yes"/>
Default Action:	<input type="text" value="Connect"/>	SJ is Active:	<input type="text" value="Yes"/>
Phone No:	<input type="text" value="2065551212"/>	Master Device	<input type="text" value="*NONE*"/>

You can change the **Device Name** of your Scammer Jammer to anything meaningful to you.

The **MAC Addr** is the serial number of your Scammer Jammer. It is important that this number exactly match. If it doesn't match the server can't tie your Scammer Jammer to your account and it will not process calls.

The **Default Action** is the action to be taken if no rules apply to an incoming call. The default is **Connect** - unknown callers (but not scammers) will be allowed to ring your telephone. You can change this to **Forward** - then unknown callers are sent to voice mail.

The **Phone No** is the telephone number of the line to which your Scammer Jammer is connected. This field is not required, but can aid in troubleshooting and may be used in the future to help avoid spoofing calls by scammers.

The **timezone** and **Daylight Savings** fields should be set properly for your location. This allows the Call History Log window to show the correct time for calls.

The **Master Device** field is used to tie multiple Scammer Jammers together so they all appear as a single Scammer Jammer. This is useful for a single user with multiple lines. For a discussion, see [Master Scammer Jammer Units](#).

Except Action

The second block contains settings for using the **Except** action. The except action allows you to use a different default action during a time range.

<input type="checkbox"/> Except	<input type="text" value="Connect"/>	From:	<input type="text" value="8:00 AM"/>	To:	<input type="text" value="5:00 PM"/>				
		Days:	<input checked="" type="checkbox"/> S	<input checked="" type="checkbox"/> M	<input checked="" type="checkbox"/> T	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> T	<input checked="" type="checkbox"/> F	<input checked="" type="checkbox"/> S

The Except action will override the Default action during a time range.

For example, if the default action is Connect, it can be **overrode** to Forward from 5PM to 8AM like this:

Device Name:	sj	Your timezone:	PST
MAC Addr:	101010101010	Daylight Savings:	Yes
Default Action:	Connect	SJ is Active:	Yes
Phone No:	2065551212	Master Device:	*NONE*
<input checked="" type="checkbox"/> Except Forward From: 5:00 PM To: 8:00 AM Days: <input checked="" type="checkbox"/> S <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> W <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> F <input checked="" type="checkbox"/> S			

The *Days* indicate which days of the week to which the Except option applies.

Scammer Detection Tuning

The last section is used to fine tune how Scammer detection functions.

Use Scammer Detection:	Yes	Detector Sensitivity:	High
Scammer Action:	Block	Reject Call if Score >=	1
		and age in days <	360

Scammer Detection allows you to disable scammer detection. If disabled, calls are not tested against the scammers database.

You can also specify which action to take when a scammer is found with **Scammer Action**. Typically one would block scammers, but you may want to forward them instead. This is useful if you are in a position where you cannot risk losing an important call.

Detector Sensitivity determines how many scammers will be blocked. It can be set to High, Medium, or Low which, in turn, sets values for *Reject Call if Score* and *and age in days*.

- **High** will block the most number of scammers and is recommended for most users.
- If High is blocking valid callers too often, use **Medium** instead. Medium will not block numbers that have been reported very infrequently.
- If it is important that the fewest possible calls get improperly blocked as scammers, use the **Low** setting. This will block only those numbers that have been reported many times.

The **Reject Call if Score is >=** is used to determine if a call from a telephone number should be blocked based on the number of times the telephone number was reported as a scammer. It is best to set Detector Sensitivity instead.

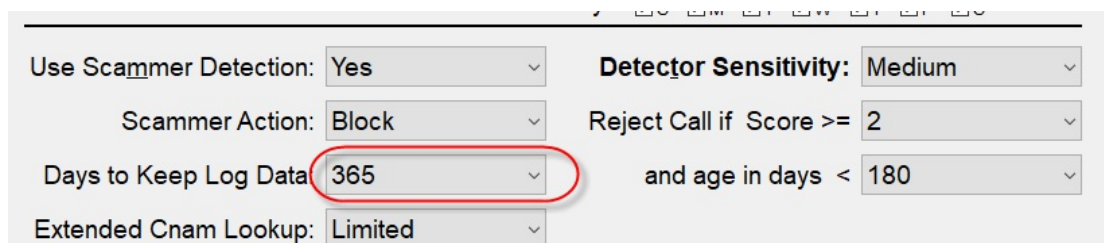
More than half of the telephone numbers in the scammers database have only been reported one time. If the default of **Reject Call if Score >= 2** is used, these telephone numbers will not be blocked from calling you. It is best to set Detector Sensitivity instead.

If you find that you are getting too many scammers calling, setting **Reject Call if Score ≥ 1** will block more numbers. If you are having too many non-scammers blocked as scammers, you can increase this value to allow more calls through.

The **age in days** box further controls if a number is considered a scammer. By default, any number that has been reported in the last year will be considered a scammer. If it has been more than a year since the last report, the number will not be considered a scammer.

Deleting old Call Log Data

By default, the Scammer Jammer server will save your call log records for a year:



Use Scammer Detection:	Yes	Detector Sensitivity:	Medium
Scammer Action:	Block	Reject Call if Score \geq	2
Days to Keep Log Data	365	and age in days <	180
Extended Cnam Lookup:	Limited		

You can specify shorter periods by changing this value.

The Scammer Jammer server actually deletes the records. If you change this setting, it will not be applied until the next time the server deletes records, typically the next night.

Extended CNAM Lookup

Extended Cnam Lookup specifies if/when to use extended CNAM lookup. The ‘CNAM’ is the name of a caller associated with his phone number. Normally this comes from the telephone company as part of the call. However, Scammer Jammer can also use an alternative database of CNAMs.

The options are *None*, *Limited*, and *Full*.

None means the alternative database is never used.

Limited means the telephone company’s CNAM is used unless it is OUT OF AREA or WIRELESS CALL in which case the alternative database is used.

Full means the alternative database is used for all calls.

This should normally use the default of *limited* as the telephone company’s data, if provided is a little more accurate. *Full* should only be used for those few telephone companies (such as Google voice) that don’t provide CNAM lookup at all.

SJ Device Settings Buttons

While in the SJ Device Settings window, there are several buttons available to you:



The **Save** button will save any changes made so far and return you to the main window.

The **Cancel** button will return to the main window **without saving** your changes.

The **New** button will clear the existing data from the window and allow you to enter information for a **new Scammer Jammer**.

The **Delete** button will delete the Scammer Jammer device displayed. **Deleting cannot be undone.** When a Scammer Jammer is deleted, so is all of its rules, its log, and any standard rules subscribed.

Account Settings

The Account Settings window is used to change the account level settings for your Scammer Jammer that are maintained on the server.

When you press the Account button on the main window, you will see the Account Settings window:

To **change your password**, enter the new password in the Enter Password box and repeat it again in the Re-enter password box. Press **Save** to change it.

If **Save Password** is selected, you don't have to enter your password each time you start sjsconfig.

The **Auto Logon** box allows you to enable/disable the auto logon feature. If selected, sjsconfig will start automatically as long as the saved username/password are correct.

If **Start in Call History Log** is selected, when sjsconfig starts, it will automatically bring up the Call History Log window.

If **Exit Confirmation** box is checked, then a warning occurs when you attempt to exit sjsconfig to verify you really want to exit.

The **Reset Forms** button will cause the size and placement of all windows to return to the defaults.

Delete Account

Pressing the Delete button will **delete your account**. Deleting **cannot be undone**. When an account is deleted, all associated Scammer Jammers and their rules, logs, and standard rules are deleted as well.

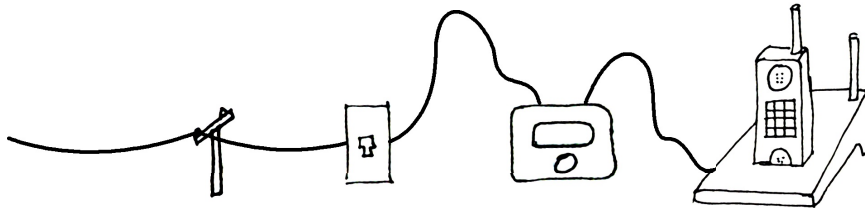
Advanced Topics

Advanced Installation

Using Scammer Jammer with Multiple Telephones

Note: Modifying your house telephone wiring can lead to a service failure if you are not familiar with telephone wiring. It is recommended you locate a telephone wiring specialist to help implement a multi-telephone installation.

Many homes now use just a wireless telephone base with wireless handsets. There is only one wired connection to the telephone system:

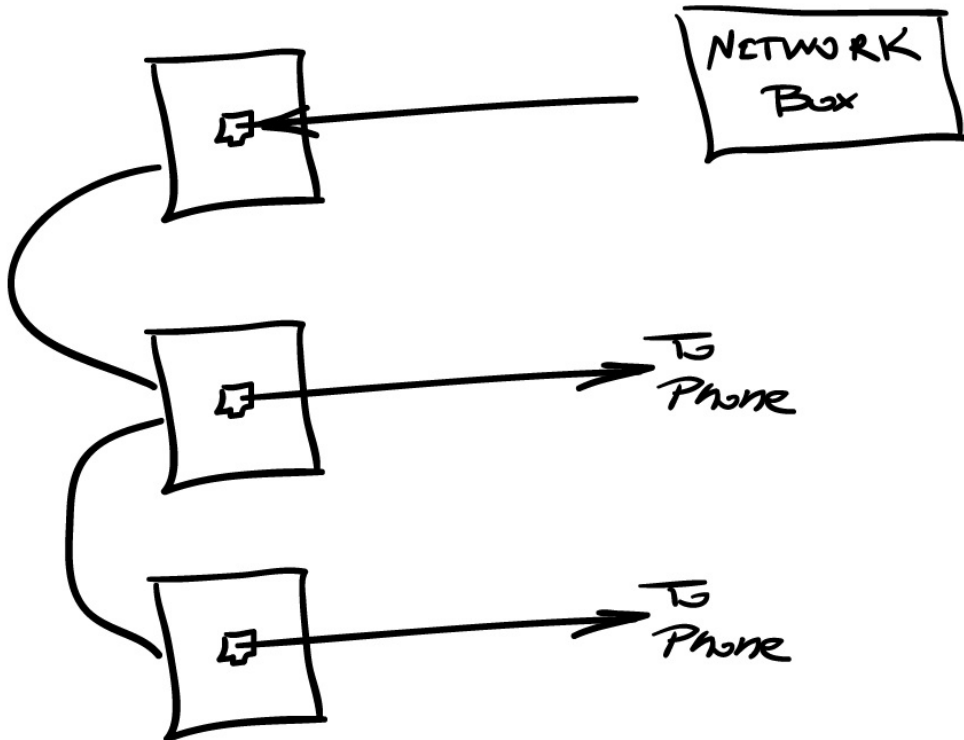


The basic installation instructions assume this type of setup (see [Install Scammer Jammer](#)).

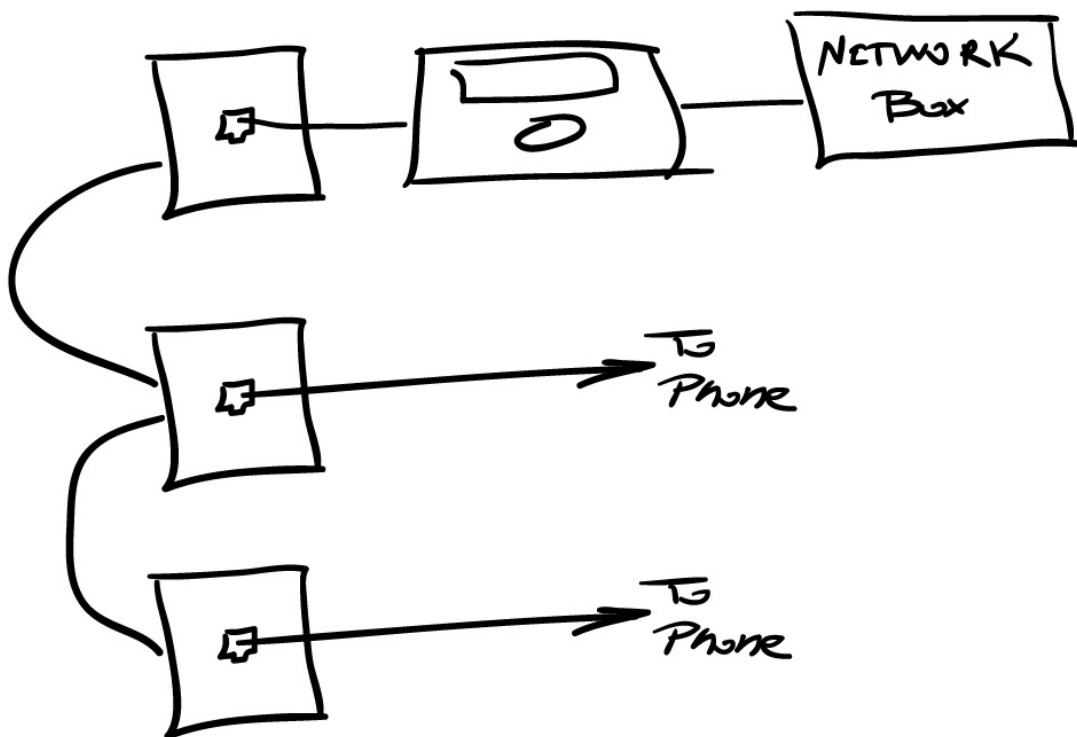
If you need to support more than one wired telephone handset, this section discusses ways to support multi-telephone installations.

Multi-Telephone Wiring for VoIP

It is usually easier to implement multi-telephone wiring for VoIP connected houses. When your VoIP provider setup your internet and telephone connection, he most likely simply connected the network box's telephone connector (the ATA port) directly into a wall jack like this:

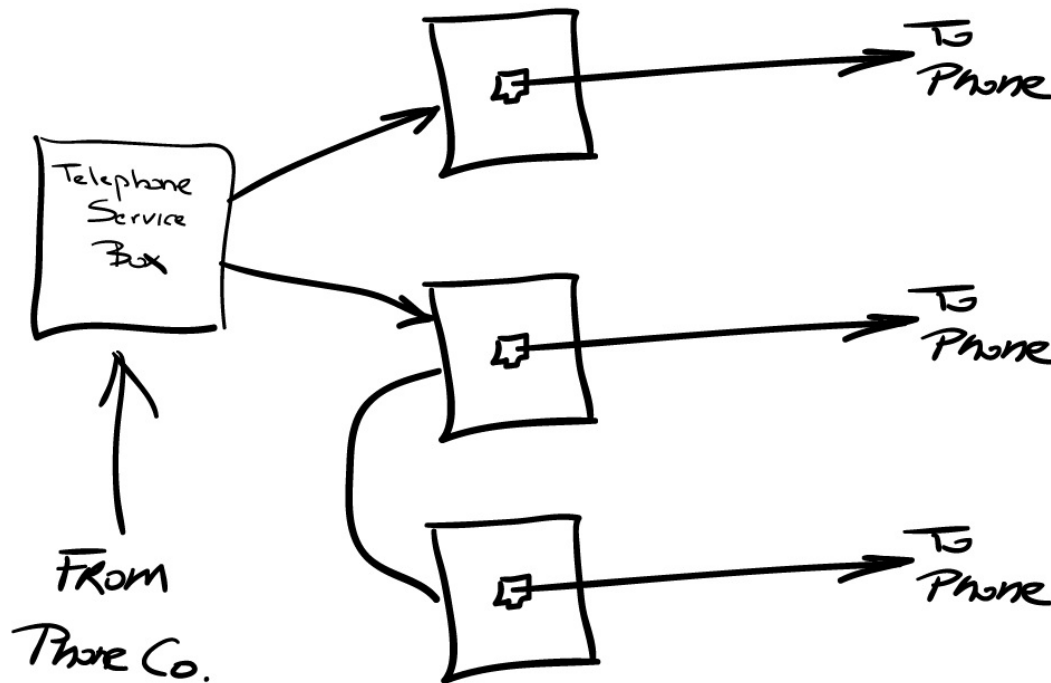


If your VoIP network box was wired into house wiring in this manner, simply insert the Scammer Jammer between the network box's ATA port and the wall jack:



Multi-Telephone Wiring for Land Lines

Land Line wiring is more complicated. The telephone line comes into a telephone service box on the outside of your house. One or more lines will feed from that box into your house wiring:

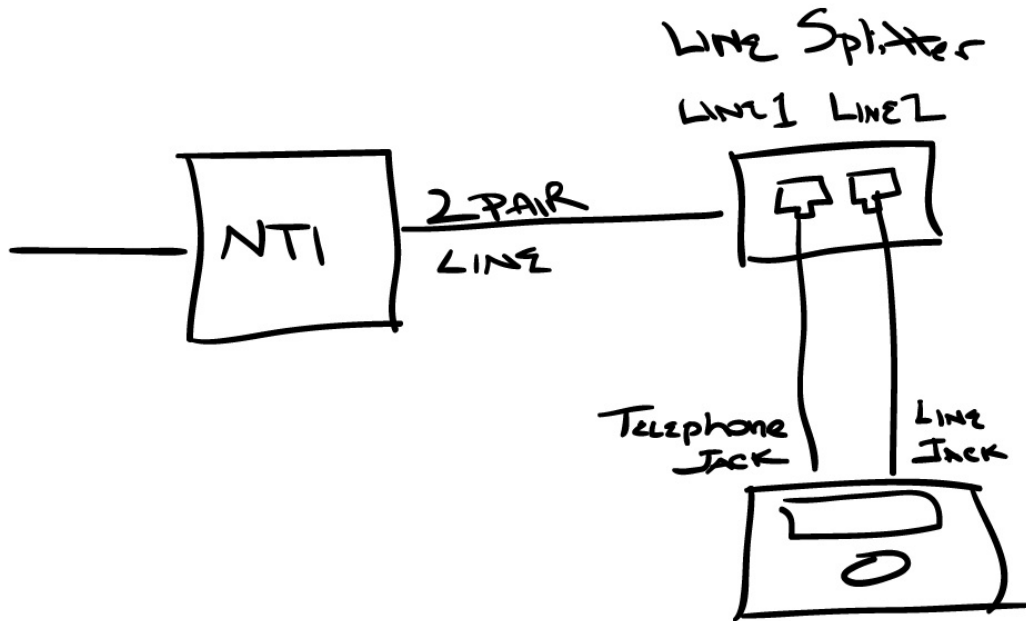


The Scammer Jammer must be installed AFTER the telephone service box, but there is no one place where it can be inserted to control all telephones.

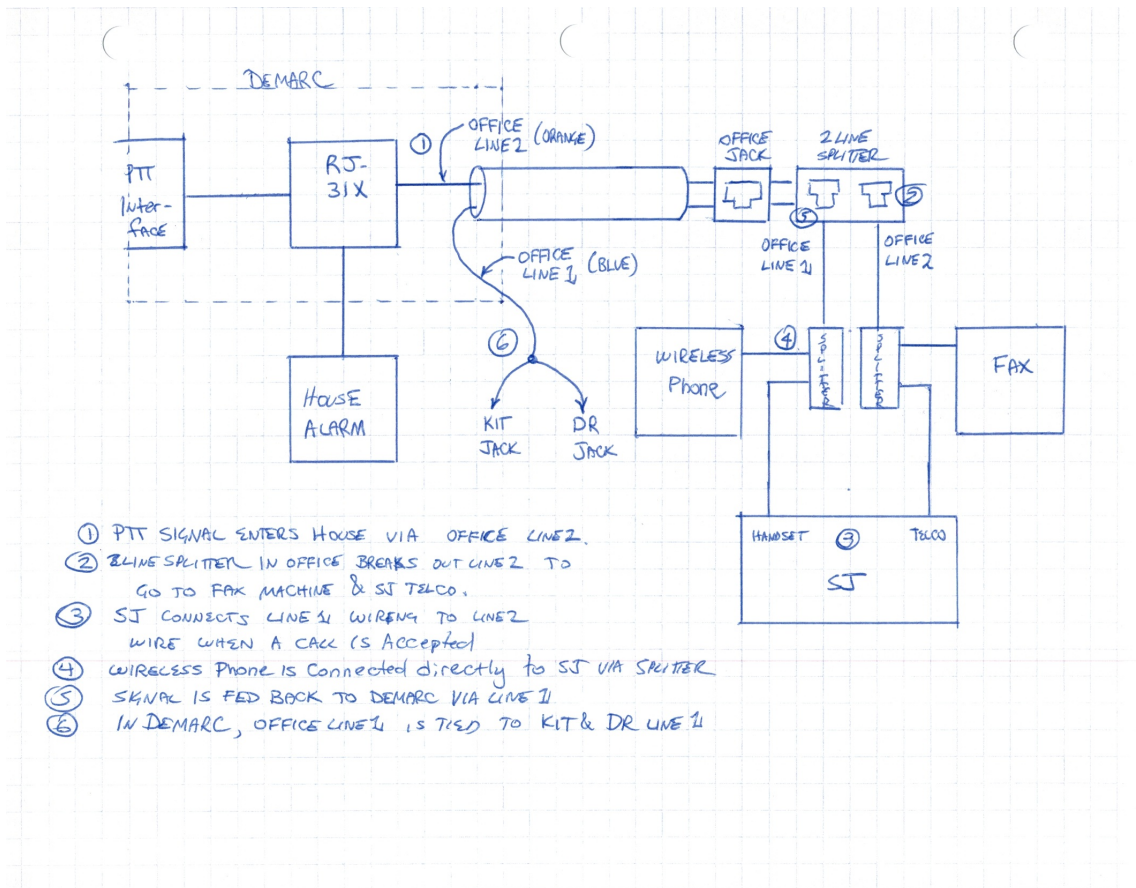
In this situation, you should call a telephone wiring specialist / electrician to help with the installation. The rest of these instructions assume you understand telephone wiring.

The easiest way to implement Scammer Jammer in a multi-telephone installation is to carry the inbound call from the NTI (telephone service box) to Scammer Jammer on line 2. This method assumes the wiring from the NTI to SJ has two pairs, and only line 1 is being used by existing telephones.

You connect the incoming phone line to line 2 of the house wiring. Line 2 of the house wiring connects to Scammer Jammer's line jack and line 1 connects into the house wiring.

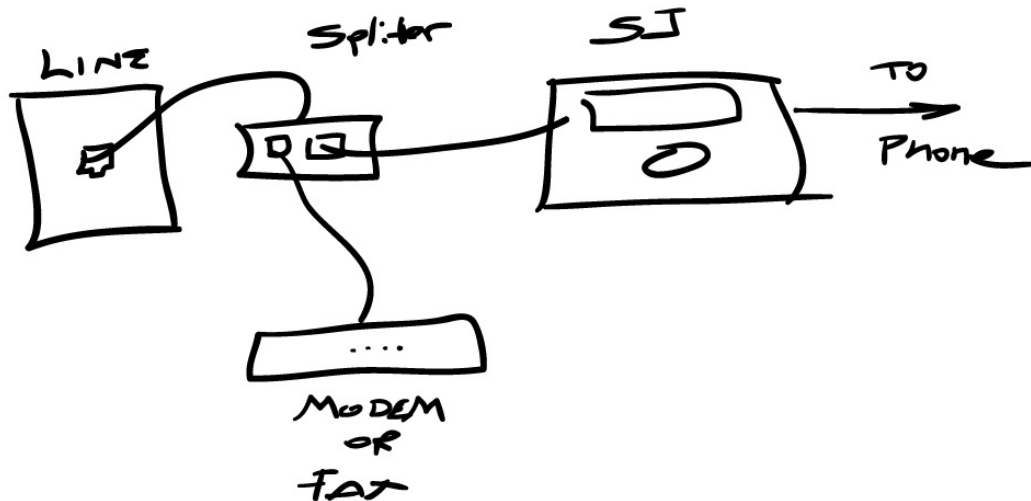


Here is a detailed diagram of an installation that uses line 2 to deliver the call to SJ and line 1 for SJ to deliver the call to all other phones:



Using Scammer Jammer with a MODEM or Fax Machine

Special equipment like a MODEM or Fax machine should be connected directly to the phone line. A telephone line splitter can be used as shown below.



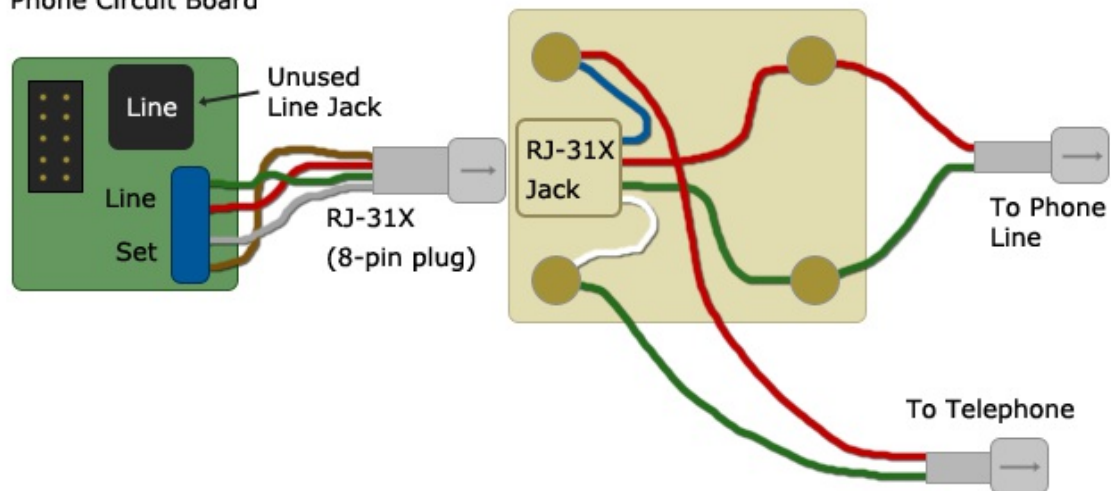
It is possible to place a MODEM or fax machine on Scammer Jammer's telephone port. This will work if the MODEM/Fax machine is used for outbound calls only. It can also work for inbound calls if you have rules to Connect all possible inbound telephone numbers.

If you do place the MODEM or Fax machine on Scammer Jammer's telephone port, your other telephones will ring when incoming data or fax calls occur.

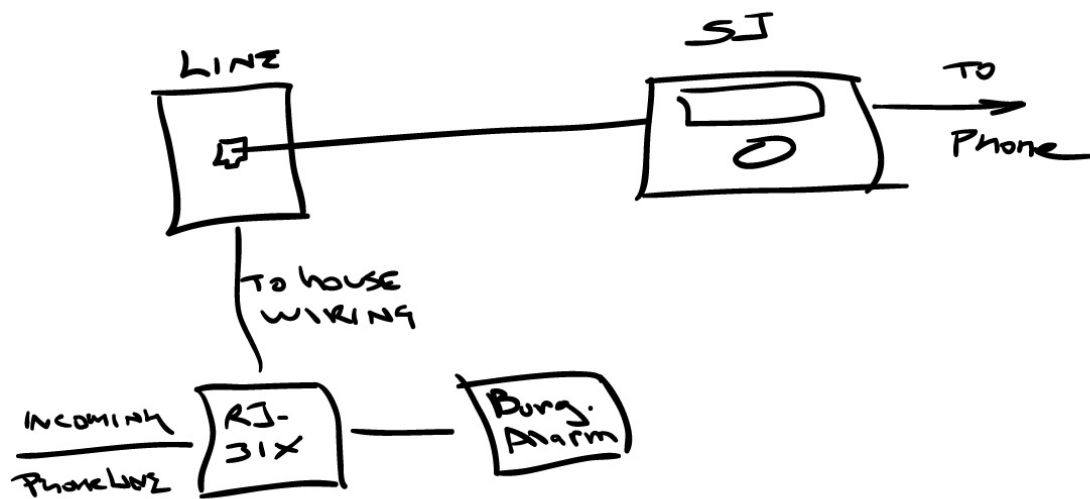
Using Scammer Jammer with a Burglar Alarm

A properly connected burglar alarm will have an RJ-31X jack box. The RJ-31X box allows the burglar alarm to seize the telephone line, if in use, and place an alarm call. The RJ-31X box goes between the incoming telephone line and the outgoing house wiring (indicated as To Telephone in this diagram):

SecureLinc 2 Phone Circuit Board



The Scammer Jammer is then placed between the RJ-31X Jack and the telephone:



When the burglar alarm connects to the monitoring station, it will disconnect the house wiring from the telephone line. When the disconnect happens you might notice a brief message on your Scammer Jammer:

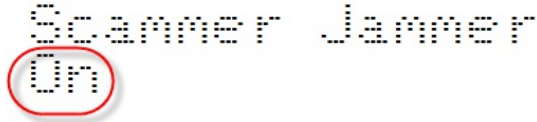
```
No Dial Tone!  
Check Telco Jack
```

Once the burglar alarm releases the line, this message will go away.

Modes - Alter the Processing of Actions

When Scammer Jammer sends a call to the Scammer Jammer server, the server looks at all of the rules and returns an action of Connect, Forward, or Block. Modes allow you to alter how Scammer Jammer processes these actions.

In normal operation, your Scammer Jammer will be in the **On** mode as can be seen in the main menu of the LCD display:



The mode can be changed from On to **Forward Connects**, **Connect Forwards**, or **Connect ALL**. These modes are named in the form *newAction OldAction*. *Forward Connects* means any incoming Connect action is changed to a Forward action.

Forward Connects is used to force all Connect actions to **instead be forwarded to voice mail**. This is useful if you want some quiet time and wish for all calls to go to voice mail. Blocked calls **are still blocked**.

Connect Forwards is the opposite of Forward Connects. With this mode is enabled, any call with a **Forward action will instead be connected**. Blocked calls **are still blocked**.

Connect ALL connects ALL calls, including Forwards, Blocks, and Scammers to ring your telephone handset. Even though all calls will now ring your telephone handset, you **will still see the appropriate call indicator** (see [Call Indicator](#)).

Even though a scammer's call will ring your telephone handset, the **Caller ID Name** will be prefixed with \$ so you still know the caller is a scammer.

Changing the Mode

Here is an example of changing the mode from On to Connect ALL.

LCD Display	Press Button	Notes
Scanner Jammer On	Select / Mode	From the main menu, Mode allows you to change the mode.
Mode? On	Previous or Next	Press previous or next repeatedly until you get to <i>Connect ALL</i> .
Mode? Connect ALL	Select	This select the <i>Connect ALL</i> mode.
Scanner Jammer Connect ALL		Scammer Jammer is now in <i>Connect ALL</i> mode.

Returning to On mode, or selecting another mode is done in the same manner.

Timed Connect ALL

You may sometimes want to use the **Connect ALL** mode to allow through all calls. For example, if you **expect a call from an telephone unknown telephone number**, you can use Connect ALL to simply **allow all calls until you get the expected call**.

If you find you do this frequently, you can **use Timed Connect ALL**. Timed Connect ALL will use the Connect ALL mode for **a specified amount of time**, then return to the prior mode.

Here is how:

LCD Display	Press Button	Notes
Scanner Jammer On	Center (Select)	From the main menu, the center button enters Timed Connect ALL
Connect ALL Timer: 1:00	Previous or Next	The amount of time is displayed and you can change it with the Previous and Next buttons. Change time to 8:00.
Connect ALL Timer: 8:00	Select	This selects Connect ALL for 8 hours
Scanner Jammer Connect ALL 8:00		Scammer Jammer is now in Connect ALL mode for the next 8 hours. The timer will count down so you know the remaining time.

Cancel Timed Connect ALL

If you want to cancel Time Connect ALL mode early, you just set the time to 0:00:

LCD Display	Press Button	Notes
Scanner Jammer Connect ALL 7:48	Center (Select)	Press the Center Select button to initiate changing of Timed Connect ALL.
Connect ALL Timer: 0:00	Select	If the timer is already active, then the new time will be set to 0:00 automatically. Press Select to use 0:00.
Scanner Jammer On		Scammer Jammer is now back in the prior mode.

Old Mode Names

Prior to firmware version 1.02, mode names were different. If you are using an older version of Scammer Jammer, this table maps the old mode name to the new names

Old Mode	New Mode
Answer Only	Forward Connects
Block Only	Connect Forwards
Log Only	Connect All
Timed Log Only	Timed Connect ALL

Caller ID Name Based Rules

As of Oct 2019, private rules may contain a Caller ID Name rather than a phone number.

When a new call occurs, Scammer Jammer will first compare the call's phone number against private rules with phone numbers. If no match is found, the call's Caller ID name will be matched against rules containing caller ID names.

A call can have two different caller ID names: one provided by the telephone company, and one provided by openCnam.com (the extended caller ID Name). If available, the extended Caller ID name is matched against rules first. If no match is found, the telephone company's Caller ID name is then matched against rules.

The telephone company Caller ID Name and the extended Caller ID Name can both be found in the log detail window for an existing call.

The Caller ID Name must match the rule exactly, including spaces and punctuation. "SMITH JOHN" does not match "JOHN SMITH" nor "SMITH, JOHN".

The case of the rule doesn't matter. "John Smith" matches "JOHN SMITH".

It is preferable to use telephone number based rules when possible. Caller ID name based rules may match calls incorrectly and unexpectedly.

Using caller ID names that would match large numbers of calls such as "OUT OF AREA" or "SEATTLE, WA" are not recommended.

Partial Match Rules

You can use partial match rules to match a large number of telephone numbers allowing you to set actions for entire area codes or all of the telephones for a particular company.

Typically, a rule is created for a specific telephone number such as

Rule Definition

Rule:	<input type="text" value="2105551234"/>
Name Override:	<input type="text" value="Mom"/>
Action:	<input type="text" value="Connect"/>
Rule is Active:	<input type="text" value="Yes"/>
Comment:	<input type="text"/>

Here you see a full 10 digit telephone number AND a name override has been included.

If you remove the last 4 so the rule is **210555123**, this is a *partial match rule*.

Rule Definition

Rule:	<input type="text" value="210555123"/>
Name Override:	<input type="text"/>
Action:	<input type="text" value="Connect"/>
Rule is Active:	<input type="text" value="Yes"/>
Comment:	<input type="text"/>

What telephone numbers does this partial match rule match? It matches all telephone numbers that **start with** 210555123: it will match 210-555-1230, 210-555-1231, 210-555-1232, 210-555-1233, etc. Because the action is connect, all of those telephone numbers will connect.

Using Partial Match Rules for a Company

You may notice many companies, schools, and government bodies use telephone numbers that start the same way. For example, one companies telephone numbers all start with 206-555-34xx. If you want all calls from this company to go to voicemail, use a partial match rule for 20655534:

Rule Definition

Rule:	<input type="text" value="20655534"/>
Name Override:	<input type="text"/>
Action:	<input type="text" value="Forward"/>
Rule is Active:	<input type="text" value="Yes"/>

Using Partial Match Rules to Forward Local Spoofing

Scammers like to use your telephone number's **same area code and exchange** to try and fool you into picking up a call by tricking you into **thinking it is a local call**.

If your telephone number is 210-555-1212, they might call you from 210-555-3456. You'll see the 210-555 and think you should answer. You can Forward all of these calls **to voice mail instead**.

First, it is a good idea to **add rules for any known telephone numbers** in your area code / exchange. If you don't know these now, you can add them as necessary. That way known callers don't get sent straight to voice mail.

Then you create a partial match rule for 210-555 to forward calls:

Rule Definition

Rule:	<input type="text" value="210555"/>
Name Override:	<input type="text"/>
Action:	<input type="text" value="Forward"/>
Rule is Active:	<input type="text" value="Yes"/>

Using Partial Match Rules to Block an Entire Area Code

Many Scammers call from Jamaica. Jamaica's area code is 876. If you don't know anyone in Jamaica, you may wish to **BLOCK all calls** from Jamaica. This is a snap:

Rule Definition

Rule:

Name Override:

Action:

Block

▼

Rule is Active:

Yes

▼

Remember, there is also a Standard Rule for blocking Jamaica.

Using Name Override and Partial Match Rules

Usually it doesn't make sense to use name override with partial match rules. A partial match rule matches many telephone numbers. A name override is used to name an individual or company.

Which Rule will be used?

Since partial match rules match many telephone numbers and there can be multiple partial match rules, which rule will be used?

For example, the following partial matches could be defined:

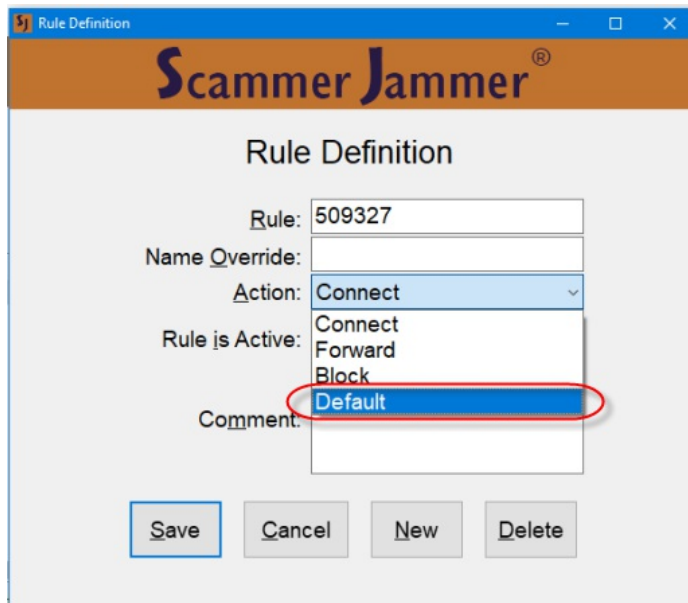
Rule	Action
210	Block
210555	Forward
2105551234	Connect

Scammer Jammer server **will match the longest rule possible** to the incoming telephone number. Using the above rules, here is how various telephone numbers will match:

Telephone	Action	Explanation
210-555-1234	Connect	The 2105551234 rule is the longest that matches.
210-555-1000	Forward	The 210555 rule is the longest rule that matches.
210-800-1000	Block	The 210 rule is the longest rule that matches.
206-555-4000	Connect	There is no rule for this telephone number, so the default rule is applied and the user configured Connect as the default rule.

Using the Default Action when Defining a Rule

As of version 1.05 of sjsconfig, "Default" is an option for the Action field in the Rule Definition window:



When Default is the action for a rule, the actual action depends on the *Default Action* and *Except* settings in the Device (SJ Server) Settings Window. In other words, the rule will act as if there is no rule.

When creating a private rule, there are times when you would rather use the Default Action rather than always force the same action.

When you create a private rule and select Connect, Forward, or Block that action will always be done. Sometimes, you may want to create a rule that simply does the current default action.

Say your dentist shows up on your phone as "out of area". You want to create a rule to change the name to "Dentist". While you are overriding the name, you still want the default action to apply. Then rather than selecting Connect or Forward, you would use Default.

A slightly more complicated example is the handling of spoofed calls in your local exchange.

If your exchange is 509327, then you would create a rule to FORWARD all calls to 509327. Then you add a rule for each legitimate caller:

509327	Forward	Local Exchange
5093271111	Connect	Buddy
5093272222	Connect	Dentist

If 5093271111 is your friend, allowing them to always connect is probably OK, but you may not want your dentist to always ring your phone. Instead, you would use the Default action to Connect during the Day and forward in the evening.

Nuisance Calls - 3rd Party Scammer Testing

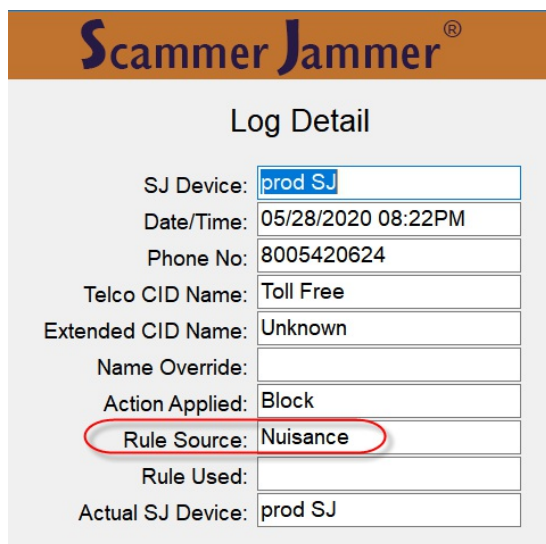
As of May 28, 2020 the Scammer Jammer Server now uses a 3rd party service, Telo, to test for scammers. This is in addition to the existing FTC do-not-call violation database.

The FTC database is very comprehensive, but its data is always at least a couple days old. Zero day scammers are not available and so are able to get past Scammer Jammer.

Telo is used in conjunction with the FTC database. When a call comes in, Scammer Jammer Server will ask Telo if the call is a scammer. If Telo says no, then SJS will search the FTC database. If either says the call is a scammer, then Scammer Jammer will treat it as such.

Telo actively watches for scammers using various techniques and maintains an active list of these scammers. This data is more up to date than the FTC database. On each inbound call, Scammer Jammer Server queries the Telo database for active robocallers.

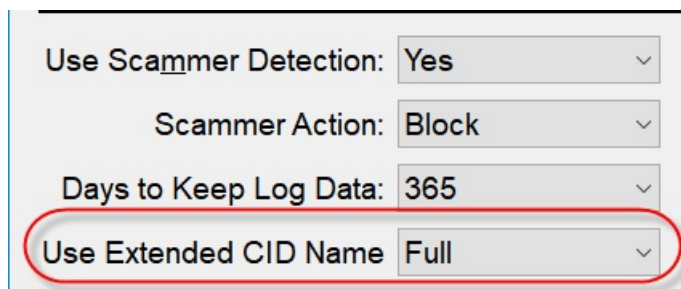
Telo calls these robocallers Nuisance calls. If Scammer Jammer finds a scammer using the Telo service, the source of the call will be **Nuisance**.



The image shows a screenshot of the 'Scammer Jammer' application interface. At the top is a brown header with the 'Scammer Jammer' logo. Below the header is a section titled 'Log Detail'. It contains a list of fields with their corresponding values: 'SJ Device' is 'prod SJ', 'Date/Time' is '05/28/2020 08:22PM', 'Phone No' is '8005420624', 'Telco CID Name' is 'Toll Free', 'Extended CID Name' is 'Unknown', 'Name Override' is empty, 'Action Applied' is 'Block', 'Rule Source' is 'Nuisance' (this field is circled in red), 'Rule Used' is empty, and 'Actual SJ Device' is 'prod SJ'.

Scammer Jammer®	
Log Detail	
SJ Device:	prod SJ
Date/Time:	05/28/2020 08:22PM
Phone No:	8005420624
Telco CID Name:	Toll Free
Extended CID Name:	Unknown
Name Override:	
Action Applied:	Block
Rule Source:	Nuisance
Rule Used:	
Actual SJ Device:	prod SJ

For Scammer Jammer Service to detect Nuisance calls, you must configure your Scammer Jammer device setting *Use Extended CID Name* to FULL. The Caller ID Name service is used to detect Nuisance calls, so it must be enabled.



The image shows a screenshot of the Scammer Jammer configuration settings. It lists several settings with dropdown menus: 'Use Scammer Detection' is set to 'Yes', 'Scammer Action' is set to 'Block', 'Days to Keep Log Data' is set to '365', and 'Use Extended CID Name' is set to 'Full' (this setting is circled in red).

Use Scammer Detection:	Yes
Scammer Action:	Block
Days to Keep Log Data:	365
Use Extended CID Name	Full

Since the Extended CID Name lookup is now enabled for all incoming calls, a side effect of using Telo is that some of your Caller ID names be different. These names are not completely consistent between the various CID name services.

Rule Sources and Source Order

If you look at the Log Detail for a call you will see a field called *Rule Source*:

Log Detail

SJ Device:	sj
Date/Time:	3/21/2018 19:02:05
Phone No:	2105551212
Caller ID Name:	WIRELESS
Name Override:	
Action Applied:	Connect
Rule Source:	default
Rule Used:	
Actual SJ Device:	sj

There are multiple sources of rules that are examined by the Scammer Jammer server. This table shows these rule sources, and the order in which they are searched.

Rule Source	Explanation
Private Rules	<p>Private Rules are those rules you have defined using the Rules button from the main menu. These rules are always applied first.</p> <p>Because private rules are applied first, you can override all other rule sources using a private rule. You can subscribe to a standard rule but override part of it. You can also override a telephone number identified as scammer and connect or forward it.</p> <p>As of Oct 2019, private rules can consist of phoneNo rules as in the past (333, 333444, 3334445555, etc) and now Caller ID Name rules (Smith John).</p> <p>When a new call occurs, phoneNo rules are searched first. Only if there is no match are Caller ID Name rules searched.</p> <p>Further, an incoming call has 2 Caller ID Names: the one supplied by the telephone Company and the one supplied by openCnam.com (Extended Caller ID). Scammer Jammer will look at the extended Caller ID name first to see if there is a matching rule. If not, then the telephone company Caller ID name is tested.</p>

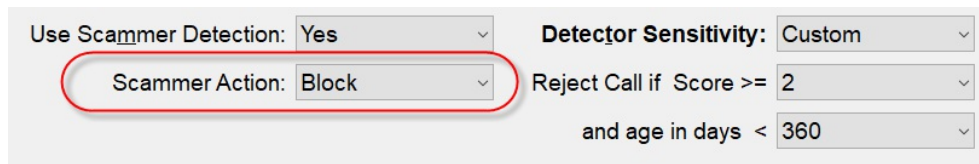
Genuines	If a number is found in this database, then the following Scammer Rules and Nuisance Calls tests are skipped.
Scammer Rules	<p>Scammer Rules consist of two parts - a list of genuine telephone numbers and a list of scammer telephone numbers. A call matches the scammer rules only if it is NOT in the genuine list but IS in the scammers list.</p> <p>Further, once a match is found the scammer's <i>score</i> and <i>age</i> are compared against your settings. The telephone number will only be marked as a scammer if they fall within your criteria.</p>
Nuisance Calls	<p>As of May 28, Scammer Jammer Server started using a 3rd party service to determine if a call is a Scammer. This service calls such calls 'Nuisance' calls.</p> <p>For all practical purposes, Nuisance calls and scammer rules can be thought of as the same thing, but internally Nuisance Calls are searched before Scammer Rules. If a match is found in either search the call is considered a scammer call and will be treated as such.</p>
System Rules	Standard rules that start with a '\$' such as \$Vnnn are <i>system rules</i> .
Standard Rules	<p>Standard rules to which you have subscribed are applied after private rules.</p> <p>Standard rules work very much like a public version of your private rules.</p>
Except or Default Rule	<p>If a call doesn't match a private rule, a standard rule, or a scammer rule, it uses the default rule. The default rule has been defined in the SJ Device Settings window:</p> <div data-bbox="485 1138 1427 1360" data-label="Form"> </div> <p>The Default Action rule can be overridden with the Except Rule for a time interval:</p> <div data-bbox="485 1463 1427 1566" data-label="Form"> </div> <p>If the call comes in during the EXCEPT time interval, then the EXCEPT action will be applied and the rule source will be <i>Except</i>.</p>

What Happens when a call is Blocked?

When a call is blocked, Scammer Jammer will connect to the incoming call for about 1 second, then hang up. No message is played. The most the caller will hear is a click.

If you have a situation where simply hanging up on a caller is not acceptable, then consider using Forward instead of Block - this will allow the caller to hear your voice mail greeting as well as leave you a message.

Scammers can be Forwarded rather than blocked by setting Scammer Action to Forward in the SJ Device Settings window:



The screenshot shows the 'SJ Device Settings' window. The 'Use Scammer Detection' dropdown is set to 'Yes'. The 'Detector Sensitivity' dropdown is set to 'Custom'. The 'Scammer Action' dropdown is set to 'Block' and is highlighted with a red oval. The 'Reject Call if Score >=' dropdown is set to '2'. The 'and age in days <' dropdown is set to '360'.

Use Scammer Detection:	Yes	Detector Sensitivity:	Custom
Scammer Action:	Block	Reject Call if Score >=	2
		and age in days <	360

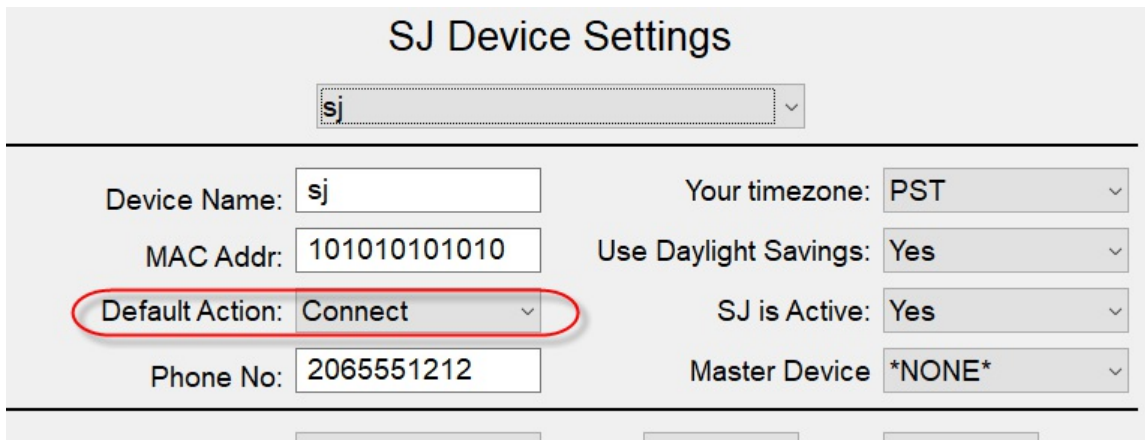
Scammer Jammer Strategies

Here are the most common Scammer Jammer call handling strategies.

Connect Known and Unknown Callers, Block All Others

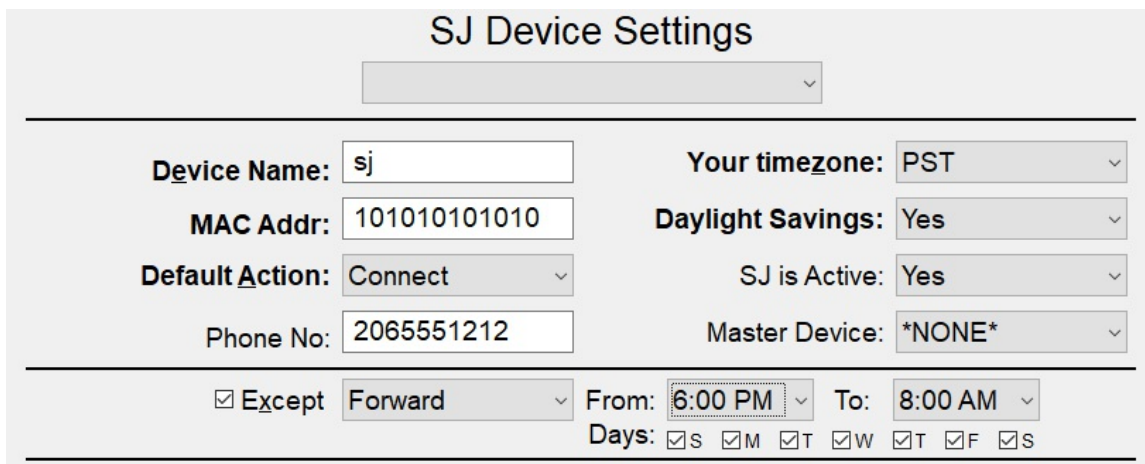
This is the least restrictive strategy. It will allow through most calls. It will only block known scammers and those callers you have created a rule to block. All other calls will be connected to the telephone. This is the default strategy initially configured into your Scammer Jammer.

To use this strategy, set Default Action to **Connect** in the SJ Device Settings window:



The screenshot shows the 'SJ Device Settings' window. At the top is a dropdown menu with 'sj' selected. Below this are several fields: 'Device Name' (sj), 'MAC Addr' (101010101010), 'Phone No' (2065551212), 'Your timezone' (PST), 'Use Daylight Savings' (Yes), 'SJ is Active' (Yes), and 'Master Device' (*NONE*). The 'Default Action' dropdown is highlighted with a red circle and is set to 'Connect'.

If you do not want unknown callers allowed in the evening, then use the EXCEPT option to **Forward** calls. In this example, calls are set to forward to voice mail after 7PM and stop at 8AM:



The screenshot shows the 'SJ Device Settings' window with the 'Except' checkbox checked. The 'Default Action' is set to 'Connect'. Below the main settings, there is a section for 'Except' with a dropdown set to 'Forward'. The 'From' time is set to '6:00 PM' and the 'To' time is set to '8:00 AM'. The 'Days' section shows checkboxes for S, M, T, W, T, F, and S, all of which are checked.

As of version 1.03, you can also specify which days *Except* will be applied. If you only want unknown callers able to reach you during 'business' hours (8-5 M-F), then setup Except to always forward except 8-5 M-F:

Device Name: sj	Your timezone: PST
MAC Addr: 101010101010	Daylight Savings: Yes
Default Action: Forward	SJ is Active: Yes
Phone No: 2065551212	Master Device: *NONE*

☒ Except Connect From: 8:00 AM To: 5:00 PM
 Days ☐ S ☒ M ☒ T ☒ W ☒ T ☒ F ☐ S

Connect Known, Forward Unknown, Block All Others

This strategy will only let known callers (action of Connect) ring your phone. Unknown callers will go straight to voice mail. Scammers will be blocked.

To use this strategy, set default action to Forward in the SJ Device Settings window:

SJ Device Settings

sj

Device Name: sj	Your timezone: PST
MAC Addr: 101010101010	Use Daylight Savings: Yes
Default Action: Forward	SJ is Active: Yes
Phone No: 2065551212	Master Device: *NONE*

Connect Known Callers, Block All Others

This is the most restrictive strategy and should be used with care. One would use this strategy when trying to protect an at-risk person from con artists / scammers. **Only known calls are allowed and the rest are blocked.**

The down-side to this strategy is **you must explicitly list EVERY telephone number** you want to allow to connect. This can be done by using one of the other strategies for a few weeks, then using the log to create rules for telephone numbers you wish to allow.

ALSO, you should take into account the fact that **emergency services CANNOT get through** either unless you explicitly allow them. Minimally you should determine the 911 call back number (if 911 calls you, the telephone number is NOT 911) and allow it through.

Note that emergency services will probably call back from a range of numbers (a PBX) and should be allowed with a partial match rule. For example the rule 21055510 would allow thru every telephone number starting with 210-555-10xx.

Further, it is a good idea to **monitor the log regularly** to see if any numbers should be added to the rules to connect.

To enable this strategy, set the Default action to block:

SJ Device Settings

sj

Device Name:	sj	Your timezone:	PST
MAC Addr:	101010101010	Use Daylight Savings:	Yes
Default Action:	Block	SJ is Active:	Yes
Phone No:	2065551212	Master Device	*NONE*

Bypassing Scammer Jammer by Redialing

If Scammer Jammer is setup to allow through **only** known callers, a known caller from an unknown telephone number cannot get through.

For example, say you setup Scammer Jammer to forward/block all calls except known callers and you have included your child's cell phone in the rules to Connect.

If the child loses his telephone and attempts to call from a pay phone, the pay phone's number is unknown and will not connect.

If this type of issue could be a problem for you, you can set Scammer Jammer's **Redial Connects** setting.

When turned On, Redial Connects will allow any caller to **Connect** by redialing Scammer Jammer within 60 seconds of it blocking or forwarding the call.

LCD Display	Press Button	Notes
Scammer Jammer On	Next / Settings	The Settings button take you into the Main menu.
Settings>	Select	Pressing select here goes into the Settings Menu, and the first setting will be Forward to VMail.
Forward to VMail: ON	Next	Go to next menu Item
Redial Connects: OFF	Select	This is the menu item we wish to modify, so press Select.
Redial Connects? OFF	Next	Press Next to change OFF to On.
Redial Connects? On	Select	Press Select to Save the On setting.
Redial Connects: On	Goback	Exit settings.

Blocking Local Exchange Spoofed Calls

Recently, scammers have started spoofing local exchange telephone numbers to trick people into answering the telephone.

Say your telephone number is 210-555-1212. The scammer will call you from another caller that starts with 210-555 such as 210-555-2121. You see the call is local and assume it is safe to answer.

Blocking local numbers presents a bit of a challenge. There is no way to know which number may be spoofed, and you don't want to blindly block them all because there is a good chance you will receive legitimate calls from nearby callers.

Note: This method requires you have voice mail or an external answering machine to which you can forward calls.

The method to block local exchange spoofed numbers is:

- Go thru your list of contacts and make sure each legit telephone number in your local exchange has a rule set up that allows it to connect.

For example, the example local exchange is 210-555. If 210-555-2222 is someone known in the local exchange, a rule is setup with the Connect action.

- Create a rule for your exchange that **Forwards** all other calls. The example local exchange is 210-555 so you would setup 210555 to Forward.

It is important that you FORWARD and not BLOCK. It is likely there will be legitimate calls from your local exchange and you don't want to just block them. If a scammer calls and goes to voice mail, chances are good he will not leave a message.

Forwarding rather than Blocking Scammers

The scammer list is not 100% accurate. It is possible for callers to be listed as scammers when they probably shouldn't be. This means a non-scammers might incorrectly get blocked.

In certain situations, the possibility of blocking a non-scammer is unacceptable. For example, a small business that gets regular customer calls would not want to risk blocking a customer.

In this case, rather than block scammers, they can be sent to voice mail. Then when a rare mistake occurs, the customer goes to voice mail, rather than gets blocked. His telephone number can then be added to the rules to make sure future calls aren't blocked.

Forwarding Scammers rather than blocking them is controlled in the SJ Device Settings window. Just change Block to Forward and click on Save:

SJ Device Settings			
<div>sj</div>			
Device Name:	<div>sj</div>	Your timezone:	<div>PST</div>
MAC Addr:	<div>101010101010</div>	Daylight Savings:	<div>Yes</div>
Default Action:	<div>Connect</div>	SJ is Active:	<div>Yes</div>
Phone No:	<div>2065551212</div>	Master Device:	<div>*NONE*</div>
<div><input type="checkbox"/> Except <div>Connect</div> From: <div>8:00 AM</div> To: <div>5:00 PM</div></div>			
Use Scammer Detection:	<div>Yes</div>	Detector Sensitivity:	<div>High</div>
Scammer Action:	<div>Block</div>	Reject Call if Score >=	<div>1</div>
		and age in days <	<div>360</div>

When Voice Mail nor an External Answering Machine is Feasible

There may be situations where the user cannot provide Voice Mail nor an External Answering machine. For example, the user may ONLY want to use a telephone's built-in answering machine OR Scammer Jammer is being used with a small PBX.

Using a Built-In Answering Machine

In the case of a built-in answering machine, Scammer Jammer must NOT forward calls because there is no where for the calls to be forwarded. In this situation, you can ONLY use CONNECT or BLOCK actions.

In this scenario, one would most likely just use Scammer Jammer to block Scammers and/or block specific numbers using rules. All other calls will go to the telephone handset / answering machine combo.

To use Scammer Jammer in this situation, first, make sure that the default action is Connect, there should be no Except action defined, and Scammer Action is Block:

SJ Device Settings

sj

Device Name: sj Your timezone: PST

MAC Addr: 101010101010 Daylight Savings: Yes

Default Action: Connect SJ is Active: Yes

Phone No: 2065551212 Master Device: *NONE*

☒ **Except** Connect From: 8:00 AM To: 5:00 PM

Use Scammer Detection: Yes Detector Sensitivity: High

Scammer Action: Block Reject Call if Score >= 1

and age in days < 360

When creating rules, their actions can ONLY be Connect or Block!

To prevent Scammer Jammer from processing the Forward action, should a rule incorrectly specify the Forward action, you should set Scammer Jammer's mode to *Connect Forwards* (see [Modes - Alter the Processing of Actions](#)):

```
Scammer Jammer
Connect Forwards
```

Using a PBX with Integrated Voice Mail

It is possible to use Scammer Jammer on a small analog telephone line PBX. To do so, a Scammer Jammer must be connected between each incoming line and the corresponding PBX port. Typically one of the Scammer Jammers would be the master for the rest so only one set of private rules must be maintained. (See [Master Scammer Jammer Units](#)).

You would then setup the Scammer Jammer[s] as was done above for a built-in answering machine. As with the built-in answering machine, calls cannot be forwarded in this setup.

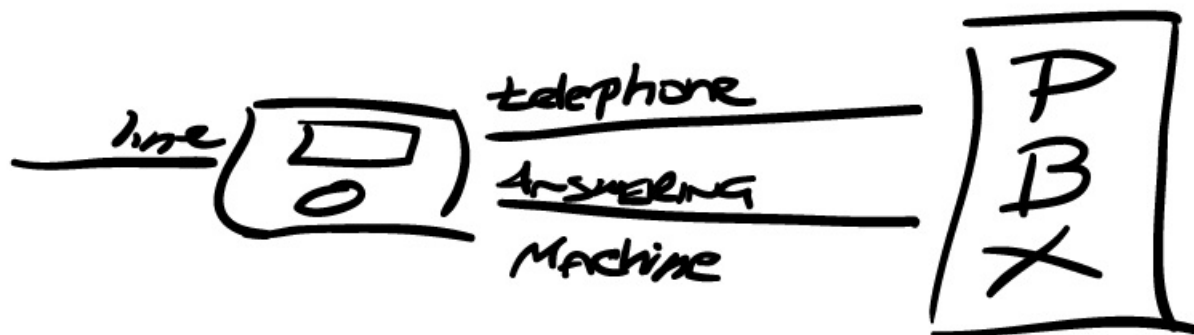
Using a PBX and Forwarding to Integrated Voice Mail

Depending on the PBX and voice mail equipment, it may be possible to use the Forward action.

Generally, when a call is Forwarded by Scammer Jammer, it simply doesn't answer the call. The call rings until voice mail or the external answering machine picks up. However, the call can be redirected to the Scammer Jammer's Answering Machine port if the setting Forward to VMail is **OFF**:

```
Forward to VMail:
OFF
```

The forwarded call can then be sent to a different port on the PBX that has been setup to direct the call to the user's voice mail account.

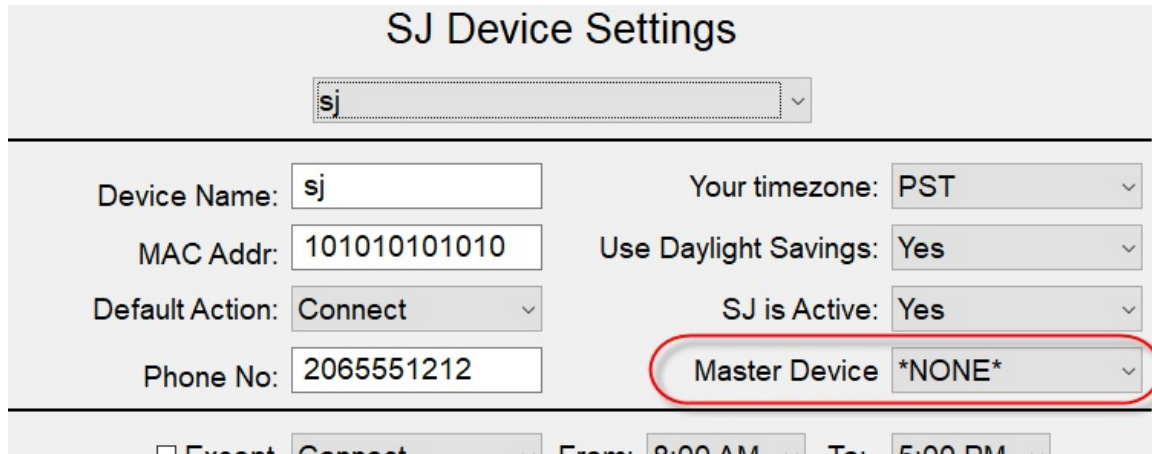


To determine if Scammer Jammer can be used in this manner will require working with your PBX vendor.

Master Scammer Jammer Units

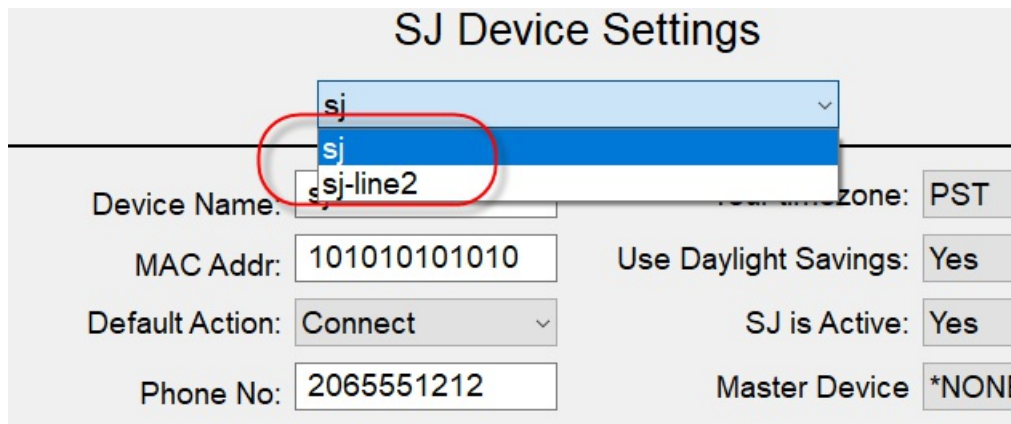
If you need to protect multiple telephone lines, you can connect a Scammer Jammer to each telephone line. But doing so requires setting up rules and standard rules for each Scammer Jammer.

Typically, a location with multiple Scammer Jammers just needs a single rule list which applies to all Scammer Jammers. That is the function of the Master Device option found in the SJ Device Settings:



The screenshot shows the 'SJ Device Settings' form. At the top, there is a dropdown menu with 'sj' selected. Below this, the form contains several fields: 'Device Name' (sj), 'MAC Addr' (101010101010), 'Default Action' (Connect), 'Phone No' (2065551212), 'Your timezone' (PST), 'Use Daylight Savings' (Yes), 'SJ is Active' (Yes), and 'Master Device' (*NONE*). The 'Master Device' dropdown is circled in red.

In this example, let's assume we have two Scammer Jammers, one called SJ and the other called SJ-Line2:



The screenshot shows the 'SJ Device Settings' form with the 'Device Name' dropdown menu open. The dropdown list shows three options: 'sj', 'sj', and 'sj-line2'. The 'sj-line2' option is circled in red. The other fields in the form are the same as in the previous screenshot.

If you go to the Rules List window, you will see you can select either Scammer Jammer to add rules:

Rules List

sj

sj

sj-line2

Rule	Name	Action	Active	Comment
20655534	XYX, Inc	Connect	Yes	
8005551212		Block	Yes	

SJ-LINE2 will show up in Log, Rules, and Standard Rules because it is a *stand-alone* unit.

We want SJ-LINE2 to follow all of the same rules that were defined for device SJ. This is done by going to the SJ Device Settings window, selecting the SJ-LINE2 device, and then setting Master Device to SJ:

SJ Device Settings

sj-line2

Device Name:

sj-line2

MAC Addr:

FFFFFFFFFFFF

Default Action:

Connect

Phone No:

Your timezone:

PST

Use Daylight Savings:

Yes

SJ is Active:

Yes

Master Device

sj

☐ Except

Connect

 From:

8:00 AM

 To:

5:00 PM

Once you save that setting, SJ-LINE2 will share the same rules defined for the SJ unit AND the same log as well.

Here, in the Rules List window you see that SJ-LINE2 is no longer available. This is because it shares SJ's rules:

Rules List

sj

sj

Rule	Name Override	Action	Active	Comment
20655534	XYX, Inc	Connect	Yes	
8005551212		Block	Yes	

Further, all calls to SJ-LINE2 will show up in SJ's log:

Call History Log				
sj				
Date	Phone No	Name	Action	Actual SJ
05/02/2018 08:00:00	8005551212	Test	Connect	sj-line2
03/21/2018 19:02:05	2105551212	WIRELESS	Connect	sj

Even though calls for both Scammer Jammers show up in the log for the device SJ, you can look at the **Actual SJ** column to see which Scammer Jammer actually received the call.

To stop using a Master Scammer Jammer, just change the Master Device back to *NONE*:

SJ Device Settings	
sj-line2	
Device Name: sj-line2	Your timezone: PST
MAC Addr: FFFFFFFF	Use Daylight Savings: Yes
Default Action: Connect	SJ is Active: Yes
Phone No:	Master Device *NONE*

If you set the Master Device to *NONE*, that Scammer Jammer will no longer use the Master Scammer Jammer's rules and if any rules had been set prior to using a Master Device, those rules will be restored.

Subscribing to Emailed Status Reports

You can receive several SJ reports via email. These reports will be emailed to the primary Email account specified in the account settings.

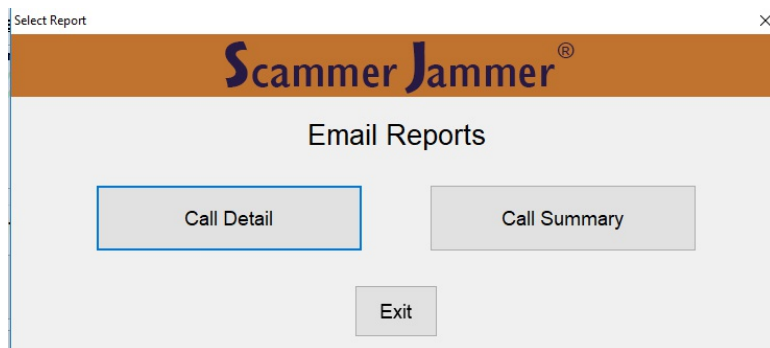
The program that produces the email runs once a day at about 12:00AM Pacific Time. Reports will show up shortly after that.

To enable, disable, or change settings for a report, click on the Reports button:



The image shows the 'Account Settings' form in the Scammer Jammer application. The form has a header with the 'Scammer Jammer' logo. Below the header, there are several input fields: 'Login Id' (containing 'johnnyj'), 'Enter Password', 'Re-enter password', 'Primary Email' (containing 'jj1234@gmail.com'), 'Backup Email', 'First Name' (containing 'Johnny'), and 'Last Name' (containing 'James'). At the bottom of the form are four buttons: 'Save', 'Cancel', 'Delete', and 'Reports'. The 'Primary Email' field and the 'Reports' button are circled in red.

When you do, the available reports will be displayed:



The image shows the 'Email Reports' dialog box in the Scammer Jammer application. The dialog has a title bar that says 'Select Report'. Inside the dialog, there are three buttons: 'Call Detail', 'Call Summary', and 'Exit'. The 'Call Detail' button is highlighted with a blue border.

- Call Detail Report: Reports every call.
- Call Summary: Summarizes all calls by telephone number and action.

Setting either of these reports is similar, so only Call Summary will be discussed. Call Detail works in the same manner.

To enable, disable, or change settings for the Call Summary report, click on the Call Summary button and you will see:

Call Summary Email Report Setup

Scammer Jammer®

Call Summary Email Report Setup

Report Enabled:

Frequency: ☐ Daily ☒ Weekly ☐ Monthly

Reverse Sort on Action:

Sample Report:

SJ Weekly Call Summary

--Action--	---Phone No---	-Count-	-----CID Name-----	---Name Override---
Block	2065021260	1	seattle, wa	
Block	5092034803	1	us air	
Forward	5093892055	1	millwood, wa	

- Settings:
 - **Report Enabled:** Set to **YES** to receive the report, **NO** to stop receiving it.
 - **Frequency:** Reports can be run daily, weekly, and / or monthly. Select the frequency you desire. The weekly report is run early on Mondays. The monthly report is run early on the first of the month.
 - **Reverse Sort Action:** The normal sort order for action is Connect, Forward, and finally Block. If you wish for the order to be Block, Forward, Connect, select this box.
 - **Save:** Click on this button to save your changes.

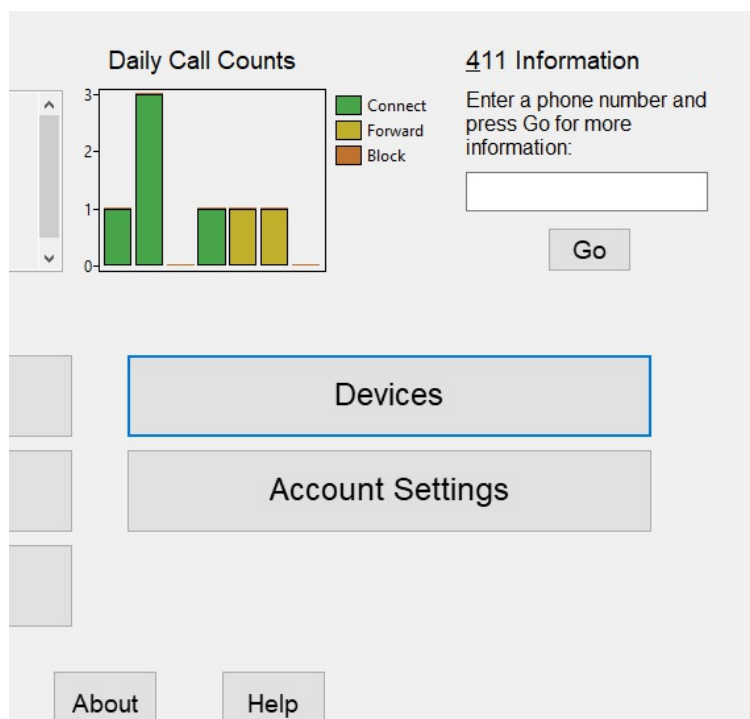
Store / Restore of Scammer Jammer Settings

Starting with version 1.04 of Scammer Jammer firmware, the Scammer Jammer will automatically store its settings to the server at start up and when the settings are changed. Version 1.04 of sjsconfig will allow you to store, restore, view, and change these settings.

While enabled by default, the SJ setting ***Send Status Reqs*** must be enabled. If you are not seeing backups of the SJ settings in sjsconfig, verify this setting is enabled.

You can request a store or restore of settings in sjsconfig. Your Scammer Jammer looks for such a request once every 10 minutes, so it can take a while before the request is processed. You can speed up the process by pressing the GO BACK button on the SJ. If you are in a remote location, you can speed up the process by calling the SJ and letting the phone ring once.

To view the list of settings backups, first click on the Devices button in the main window:



If you have more than one Scammer Jammer, make sure you select the one you wish to review:

Scammer Jammer®

SJ Server Settings

breadboardSJ

Device Name: breadboardSJ

MAC Addr: test SJ

Default Action: Connect

Phone No:

one: PST

ings: Yes

SJ is Active: Yes

Master Device: *NONE*

From: 8:00 AM To: 5:00 PM

Days: ☒ S ☒ M ☒ T ☒ W ☒ T ☒ F ☒ S

then click on the SJ Settings button:

Connect

SJ is Active: Yes

Master Device: *NONE*

Connect

From: 8:00 AM To: 5:00 PM

Days: ☒ S ☒ M ☒ T ☒ W ☒ T ☒ F ☒ S

Yes

Detector Sensitivity: Custom

Block

Reject Call if Score >= 2

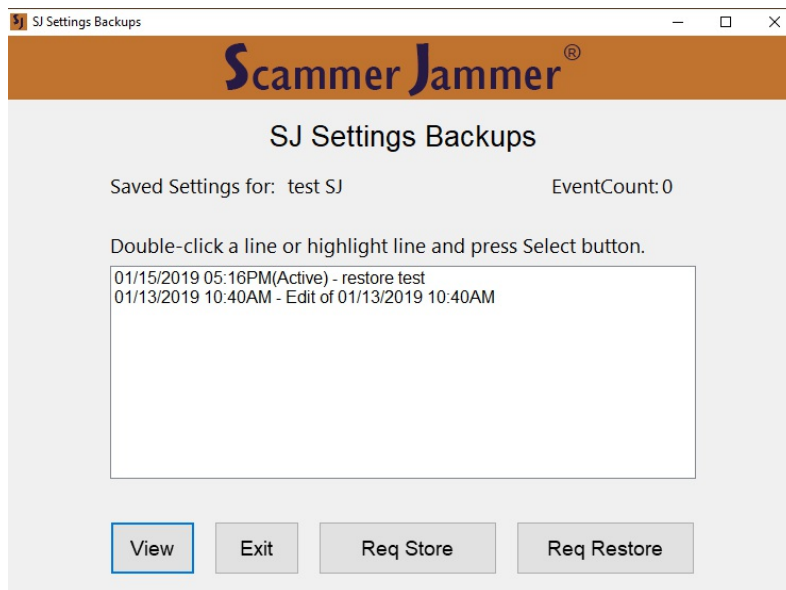
365

and age in days < 360

Full

Cancel Delete New SJ Settings

This brings up the list of settings backups on the server:



The SJ Settings Backup window lists all of the settings backups stored on the server, the date&time the backup occurred and if the backup is the **active** backup.

If there **are no records** listed, make sure your Scammer has the proper firmware version AND the Send Status Reqs setting is enabled.

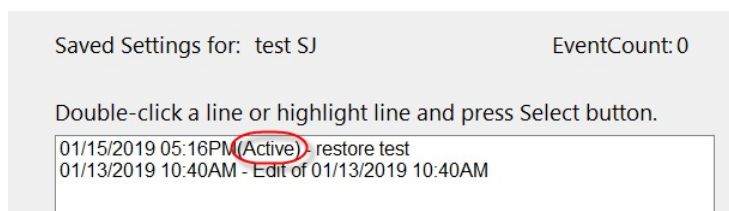
Restarting the Scammer Jammer should create a settings backup if everything is configured properly.

From inside the SJ Settings Backups window you can

- View - examine and edit a settings backup.
- Req(uest) a Store of Settings - the Scammer Jammer will send its current settings to the server.
- Req(uest) a Restore of the selected settings - the Scammer Jammer will restore the selected settings into its memory.
- Delete - selecting a record and pressing the delete key will delete the selected settings backup.
- Refresh - Pressing F5 will refresh the list immediately; otherwise, it automatically refreshes occasionally.

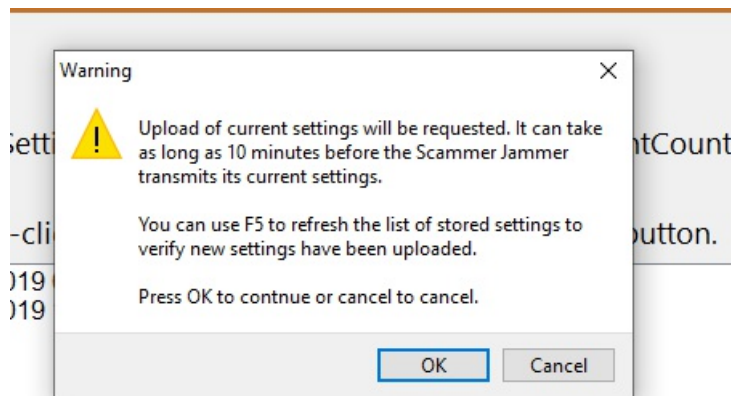
Request SJ Settings be Stored

You typically will want to work with the current SJ settings. The **active** settings are displayed:

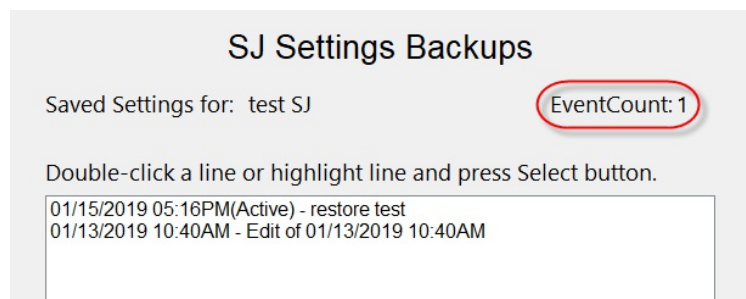


If the date of the store is not recent, it is suggested that you request settings be stored again so you are sure the settings on the server match the actual settings. This is done by clicking on the Req Store button.

When you click on the Req Store button you will see:



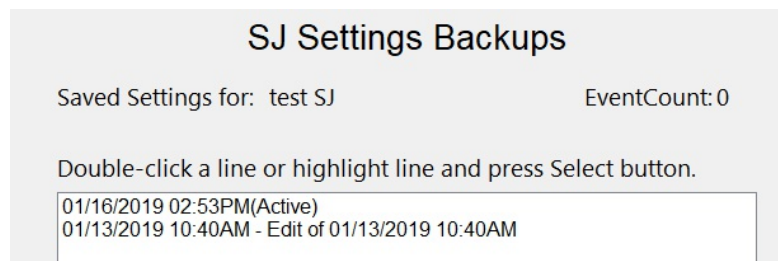
Click on OK to request the store. After you do you will see:



Note the EventCount is no longer 0. This indicates there is a store request waiting to be processed by the Scammer Jammer.

You can now wait for the Scammer Jammer to do the Store. If you have access to the Scammer Jammer, just press the Go Back button on the unit, and the store will occur immediately. Alternatively, you can call the SJ unit and let the phone ring 1 time.

Once the store is complete, the EventCount returns to 0 and the current settings are on the server:

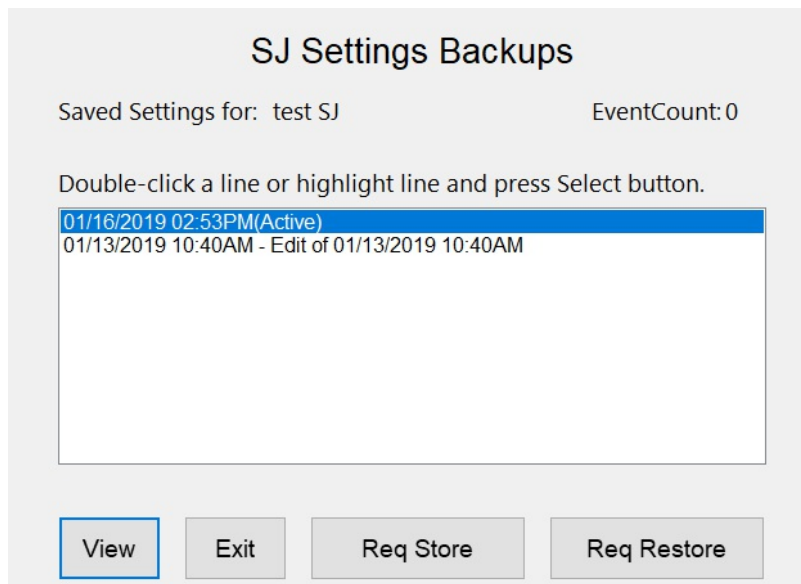


Note in this example that a new record isn't created - the old active record was replaced with the new one. This occurs if the settings being backed up match the active settings on the server.

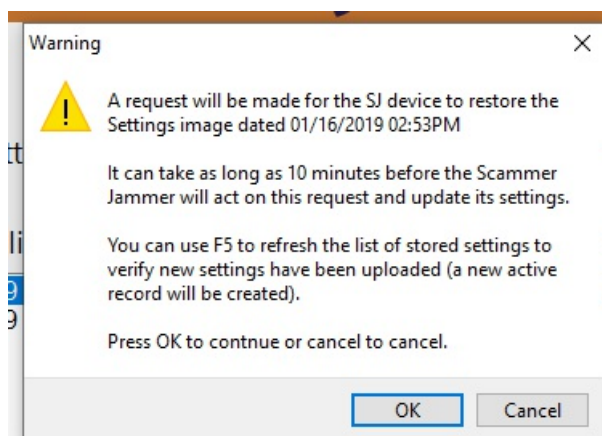
Request SJ Settings be Restored

Warning: It is possible to cause your Scammer Jammer to completely stop functioning if you restore bad settings. This is discussed more in Advanced Settings further below.

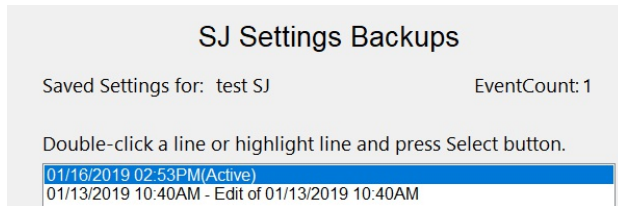
You can restore settings from the server to the Scammer Jammer as easily. To do so, select the settings to restore:



When you click on the Req Restore button you will see:



As with store, restore can take as long as 10 minutes to occur. When you click on OK, you will then see:



Note the EventCount is 1 again. When it returns to 0, the Scammer Jammer has restarted.

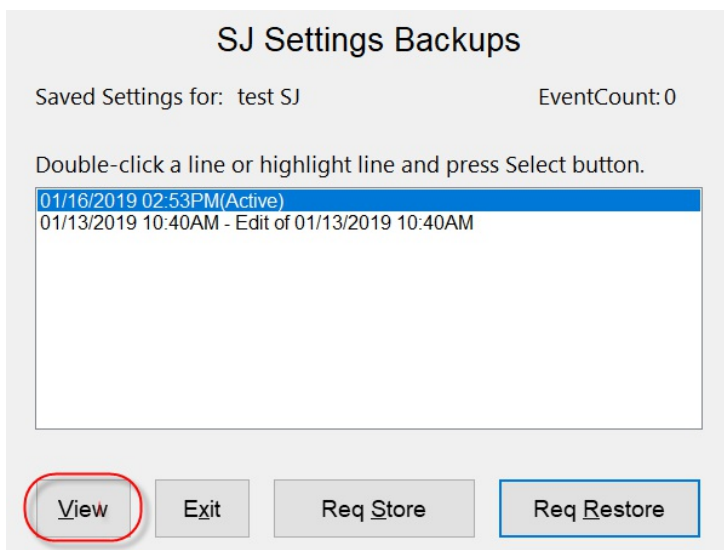
In this example, it didn't really restart. **Tip:** if you restore the same settings that are in the SJ unit, it will not actually restart since there is no reason to do so.

When different settings are restored, the SJ will restart and will also store those new settings so the date and time of the store will change.

Viewing Settings

sjsconfig allows you to examine a settings backup so you can see each of the settings. This is done with the View button.

To view a settings backup, select it and then press the View button:



When you do so, you will see:

Scammer Jammer®

SJ Device Settings

test SJ

Date Settings Stored: 01/16/2019 02:53PM eeprom Version: 16

Active: Yes

Comment:

Edit Advanced Save Save Copy Delete Clip Cancel

Crash Diagnostics

Last Abort Code: 28 State Queue: 108

Basic Settings

Forward to VMail: On	Redial Connects: Off
AnsMach Always On: Off	Use Distinct Ring: Off
Mode: On	Lock Mode: Off

Network Settings

SJS Server Name: LABDUDE.HALLOCK.NET	Server Port: 11183
Use Static IP Addr: Off	IP Address: 192.8.50.0

The SJ Device Settings window is very long and can be scrolled using the scroll bar, mouse wheel, or pgUp/pgDown.

Editing Settings

To change the settings (which will only change the version of settings backed up and being viewed), click on the Edit button. When you do this, the fields that are always safe to change will become available:

SJ Device Settings

test SJ

Date Settings Stored:
Active:
Comment:

eeprom Version:

Crash Diagnostics

Last Abort Code:

State Queue:

Basic Settings

Forward to VMail:
AnsMach Always On:
Mode:

Redial Connects:
Use Distinct Ring:
Lock Mode:

Network Settings

Saving Settings

If you make changes to the settings, you save them back to the server using the Save button.

After clicking on save, you will return to the SJ Settings Backups window:

SJ Settings Backups

Saved Settings for: test SJ

EventCount: 0

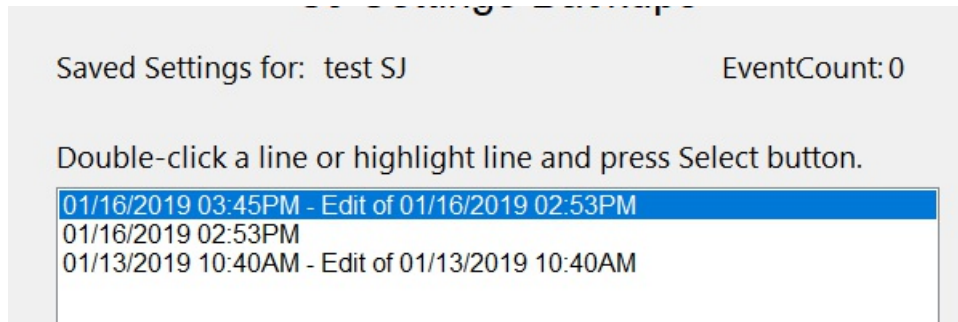
Double-click a line or highlight line and press Select button.

01/16/2019 02:53PM - Edit of 01/16/2019 02:53PM
01/13/2019 10:40AM - Edit of 01/13/2019 10:40AM

Note that the backup is no longer the active backup. Also, the comment is added automatically unless you specify your own comment.

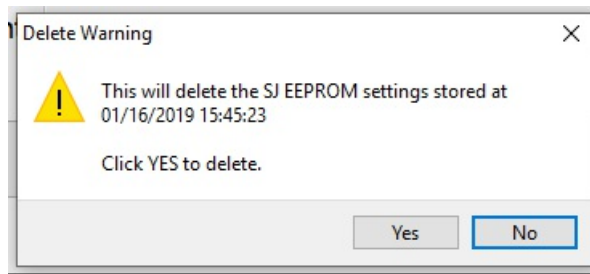
Save Copy of Settings

If you use the Save Copy button rather than the Save button, the settings are saved to a new backup:



Deleting Settings

Inside the SJ Device Setting window, press the delete key. You will be asked to confirm the deletion:



If you click on Yes, the settings backup is deleted.

You may also delete settings in the SJ Settings Backups window by selecting a settings backup and pressing the delete key.

Copying Settings to the Clipboard

You can copy the settings to the clipboard and then paste them into an editor to view or print them:

```
SJ DEVICE SETTINGS FOR: test SJ (deviceId: 1)

Date Settings Stored: 01/16/2019 03:45PM
eeprom Version: 16
Active: No
Comment: Edit of 01/16/2019 02:53PM

CRASH DIAGNOSTICS
Last Abort Code: 28
State Queue: 108 3 2 1 103 2 107 2 1 103 2 1 2 1 2 1 103 2 107 2

BASIC SETTINGS
Forward to VMail: Off
Redial Connects: Off
AnsMach Always On: Off
Use Distinct Ring: Off
Mode: On
```

Lock Mode: Off

NETWORK SETTINGS

SJS Server Name: LABDUDE
Server Port: 11183
Use Static IP Addr: Off
IP Address: 192.8.50.0
Subnet Mask: 255.255.255.0
Gateway IP Addr: 192.8.50.1
DNS Server IP Addr: 192.8.50.15

ADVANCED SETTINGS

LCD Light Timeout: 60
Must Ring On: 2
Test for Dial Tone: On
Netfail to AnsMachine: Off
Cache Enabled: Off
Send Status Req's: On
Pass CID to handset: Off
ADC Threshold: 50

TIMING

Redial Timeout(mins): 60
DNS Cache Timeout(mins): 30
Net Initialize Timeout(secs): 30
Net Start Timeout(secs): 10
Ping Timeout(secs): 15
CID Timeout(ms): 500
Watch Dog Timeout(secs): 30
DHCP Timeout(secs): 10
DHCP Resp Timeout(secs): 4
Connection Timeout(secs): 30
Status Req Std Timeout(mins): 10
Status Req Fast Timeout(secs): 30
Ringback Time(secs): 11
Max Flash Time(ms): 1000

MISCELLANEOUS

Keypad Lock: Off
Lock PIN: 0
Syslog Server Name: SJS.XYFYX.COM
Syslog Port Number: 11184
Syslog Priority Filter: 6
CID Wave Height: 2047
CID Wave Start: 0
Modem Baud Rate: 2400
Modem Country Code: B5

Advanced Settings

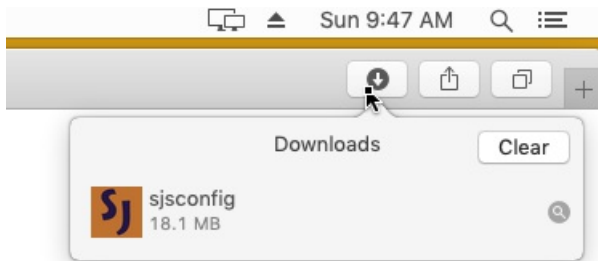
You can change nearly any of the SJ settings by clicking on the Advanced button.

Warning: It is possible to cause your Scammer Jammer to stop functioning if you restore bad settings into it. For this reason it is recommended you only make Advanced changes when directed by SJ support staff.

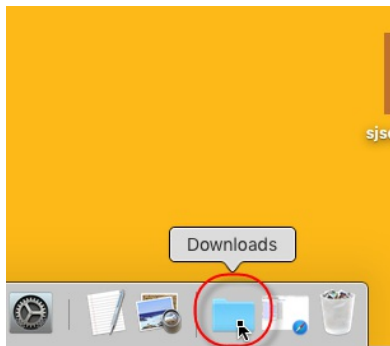
Installing the Native Mac Version of sjsconfig

These instructions assume you have been given a web link to the sjsconfig setup file.

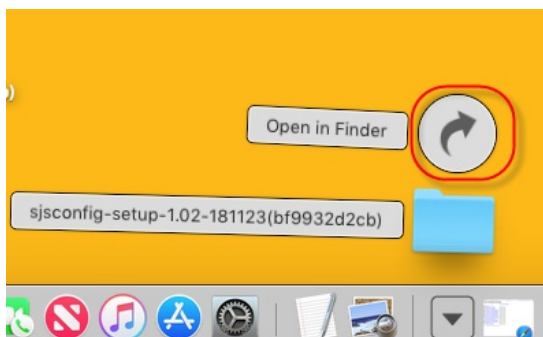
- Clicking on the link should start safari (or your preferred web browser), and it will automatically download the file:



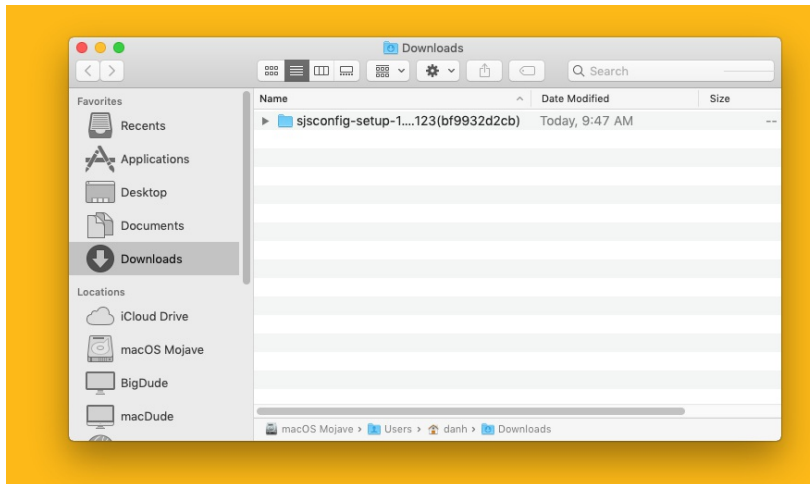
- Locate your downloads folder:



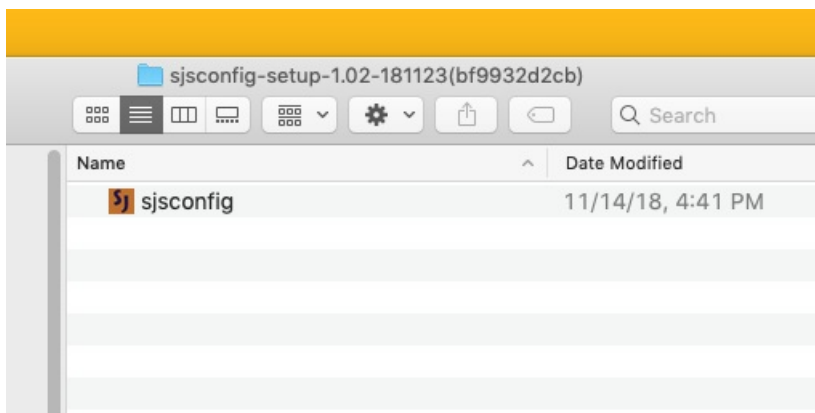
- Click on the downloads folder and you will see a list of files:



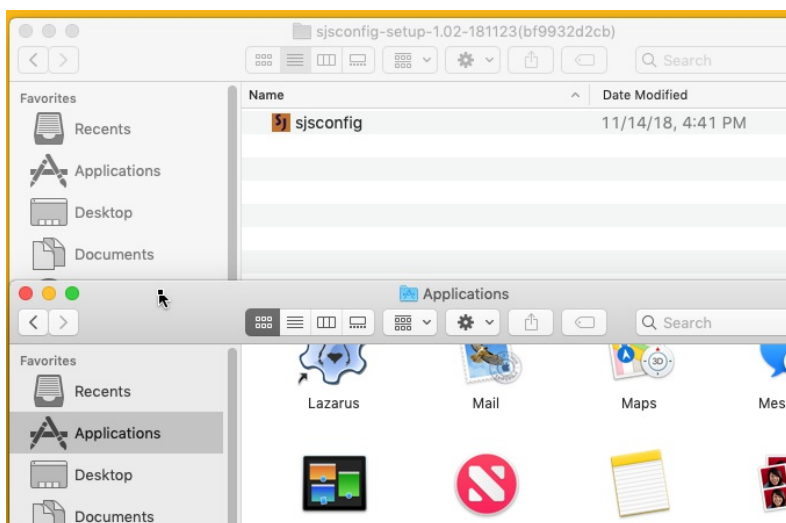
- Click on the Open in Finder Icon (circled in red above) and this opens the download folder:



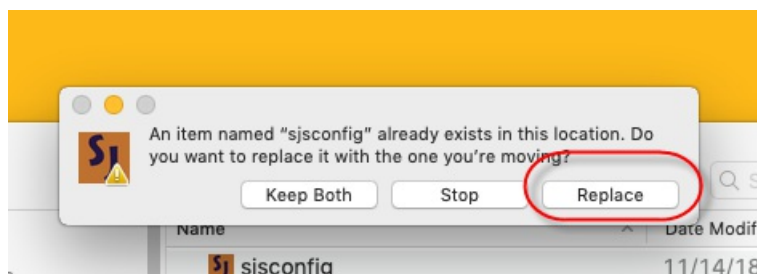
- Now open the sjsconfig-setup... folder:



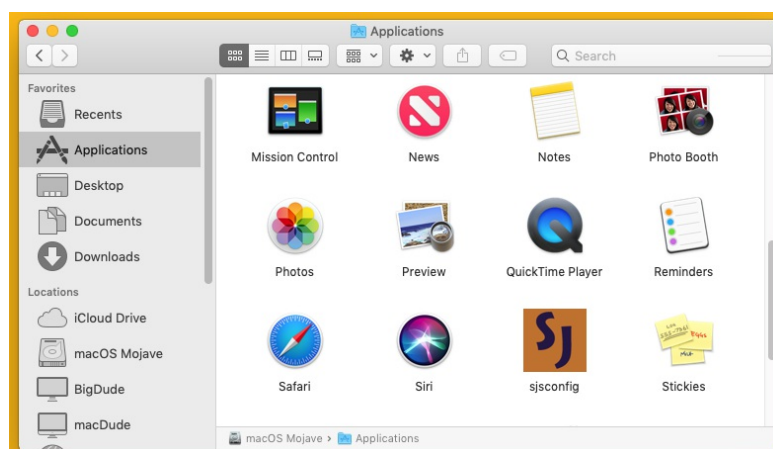
- In File Finder, type command-N to open a new file finder window and go to the applications folder within it:



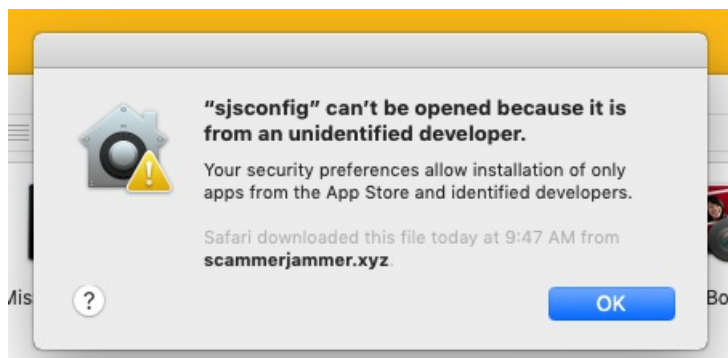
- Finally, drag the sjsconfig application from the setup folder into the applications folder.
- If you already have sjsconfig installed, click on replace:



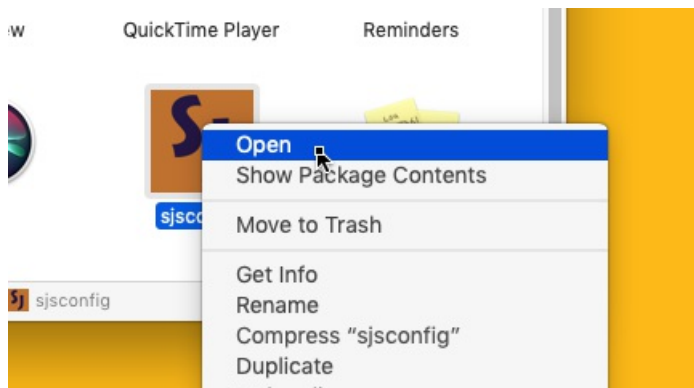
- sjsconfig is now installed:



- Double click on the sjsconfig icon to start the program. Quite likely you will see this warning:



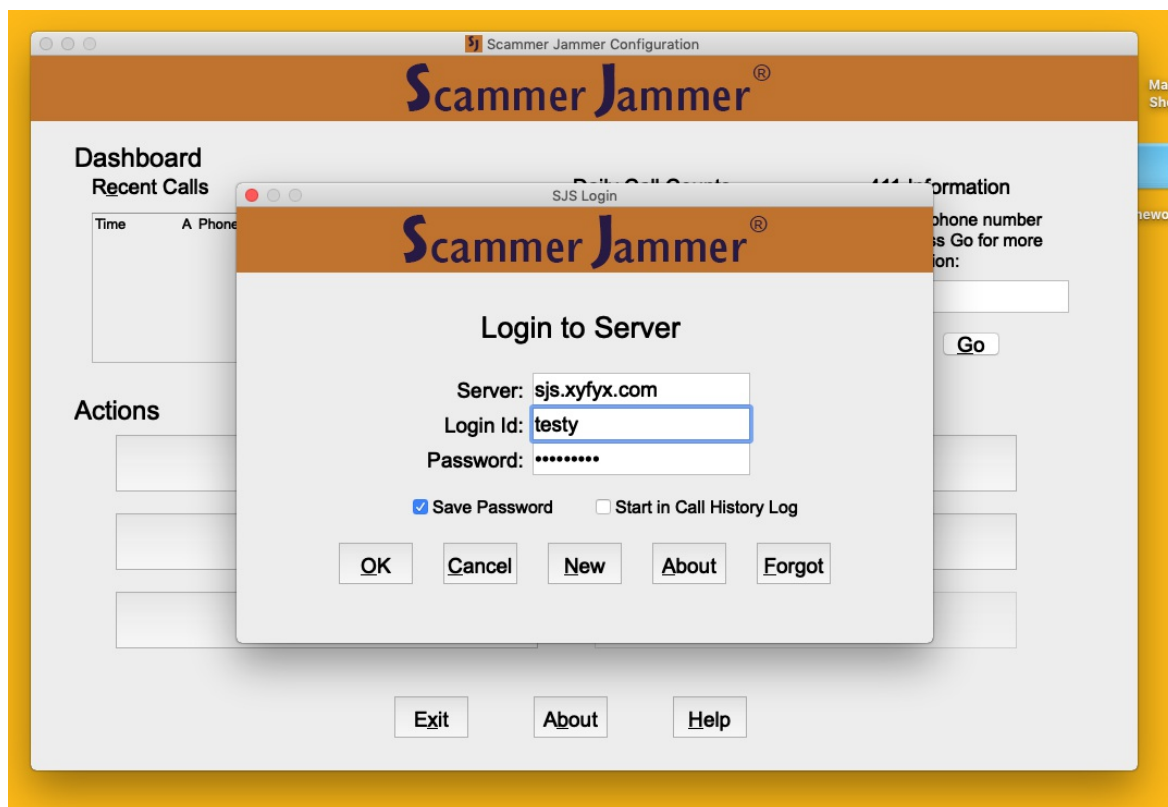
- If you do get this message, click on OK. Then right click on the sjsconfig icon and click on open:



- You will then see this box. Click on open:



- sjsconfig will start and in the future will start without the warning dialog boxes:



Notes for Using Native Mac Version of sjsconfig

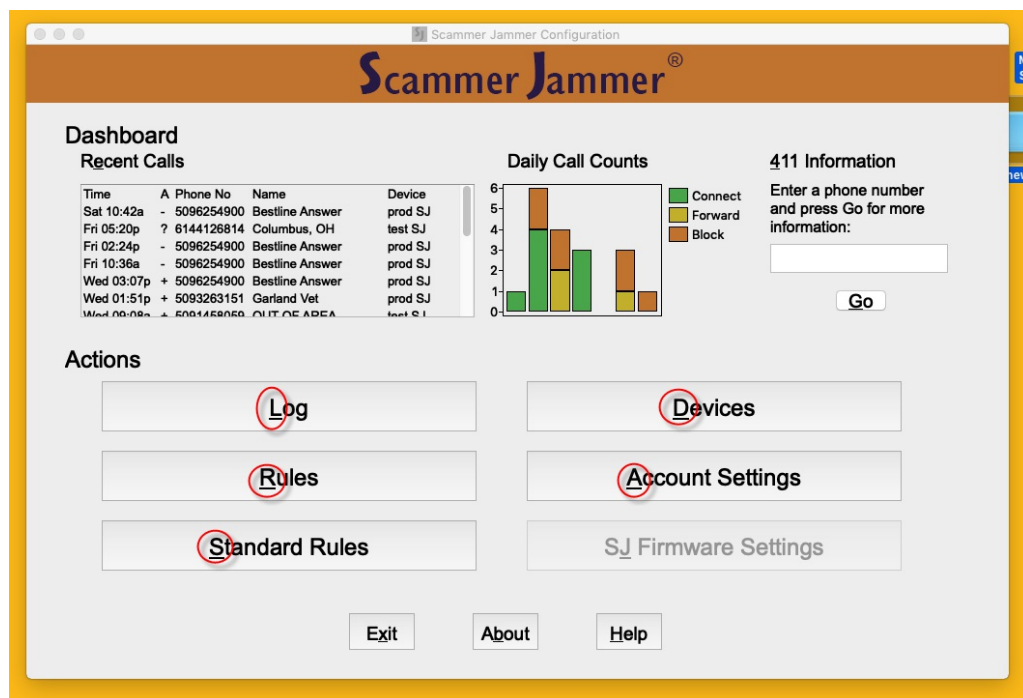
There are differences in the graphical user interface (GUI) between Windows and MacIntosh. Some of those differences can impact sjsconfig usage.

The current version of sjsconfig uses the QT framework GUI rather than Apple's built-in GUI. This was done due to issues between the compiler and the Apple GUI.

The QT GUI works much like windows, but not exactly.

Accelerator Keys

Apple does not support accelerator keys. QT does. For example, in windows, you can type alt-X to press the exit key. Using QT you must use command-X. In the example below, pressing command-L would bring up the log window, command-R the Rules window, etc.



Tab Key Differences

In Windows, the tab key will cycle thru all controls in the window. In Mac, the tab key will only cycle thru text entry boxes. You must use the mouse to click on buttons or combo boxes.

In QT for Mac, the tab key works as it does for windows and allows you to tab through all of the controls in the window.

Interesting Note:

You can change this behavior on the Mac by going into the keyboard settings, going to short cuts and selecting *Full Keyboard Access: All Controls*. BUT this is a global setting and will impact all programs permanently.

You can temporarily enable tabbing into all controls by pressing control-f7.

Escape Key Differences

In the Windows version, the escape key will always exit the current form, returning you to the prior form. For the Mac, sometimes it exits, sometimes it brings up autocompletion, sometimes it does nothing.

In QT for Mac, the exit key works as it does for windows - the current window will be closed and you will be returned to the prior window.

Intersting Note: In the Mac version, if the focus is in a text box, pressing the escape key will first bring up an autocompletion from the built-in spell checker. IF you press **escape again**, the form will be closed.

You can permanently get rid of this autocompletion by typing the following command into terminal:

```
defaults write -g NSUseSpellCheckerForCompletions -bool false
```

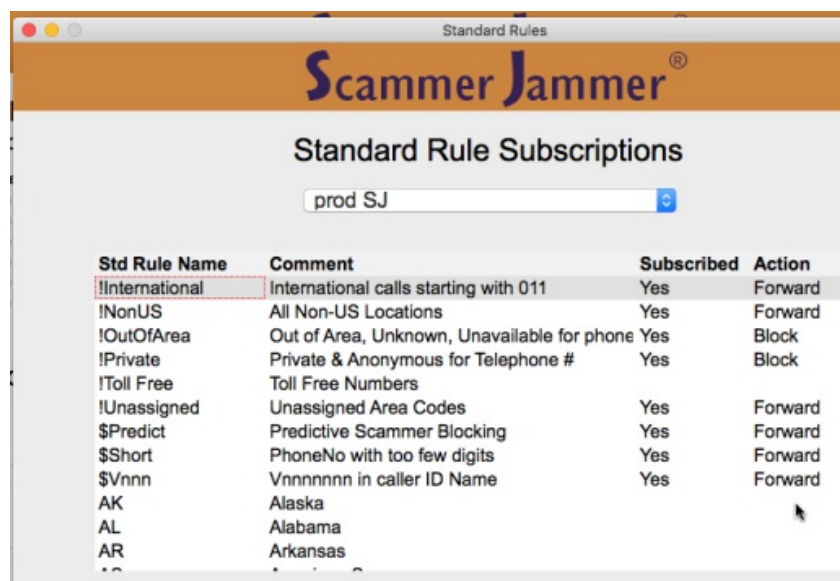
This is a system-wide setting!!

To return autocompletion, type this

```
defaults write -g NSUseSpellCheckerForCompletions -bool true
```

Right Click in Grid Control

There are various grid controls in sjsconfig, such as the one shown here in the Standard Rules Subscriptions form:



Std Rule Name	Comment	Subscribed	Action
!International	International calls starting with 011	Yes	Forward
!NonUS	All Non-US Locations	Yes	Forward
!OutOfArea	Out of Area, Unknown, Unavailable for phone	Yes	Block
!Private	Private & Anonymous for Telephone #	Yes	Block
!Toll Free	Toll Free Numbers		
!Unassigned	Unassigned Area Codes	Yes	Forward
\$Predict	Predictive Scammer Blocking	Yes	Forward
\$Short	PhoneNo with too few digits	Yes	Forward
\$Vnnn	Vnnnnnn in caller ID Name	Yes	Forward
AK	Alaska		
AL	Alabama		
AR	Arkansas		

In Windows, if you right click, the cell under the mouse will be selected, then a popup menu related to that cell is displayed.

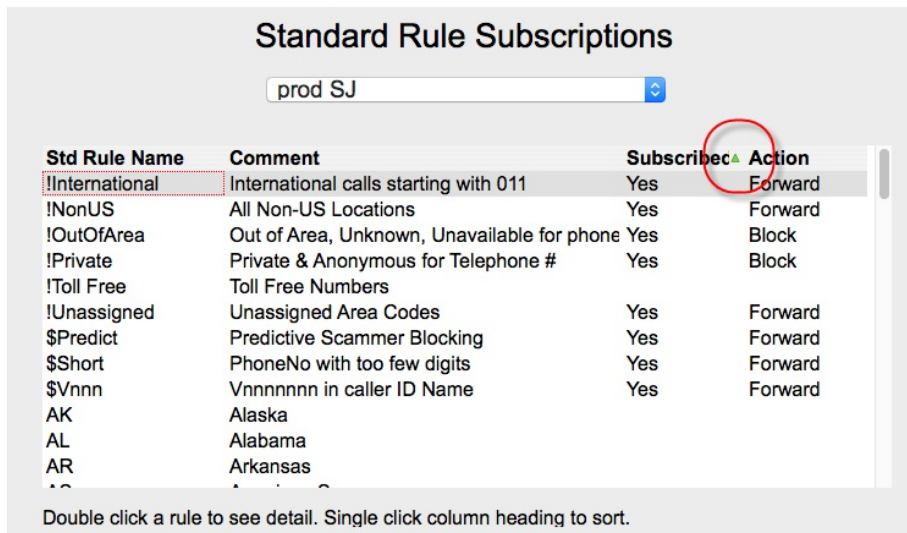
In Mac, if you right click, the cell under the mouse is NOT selected. Instead the current cell (which has a red border around it) is used and the popup menu for that cell is displayed. *The same applies to QT for Mac!*

Column Sort Indicator Never Goes Away

In Windows, when you first enter a window with a gridcontrol in it, it is always sorted by the first column, and the sort indicator is not present. When you click on a column to change the sort, then the indicator is displayed. Exit and re-enter the window and the indicator is no longer there.

On the Mac, when you first enter a window with a gridcontrol, it will be sorted properly and the indicator is not there. If you click on a column to sort, it will sort properly and the sort indicator shows up correctly.

BUT if you sort on a column, exit the window, and re-enter the window it will be properly sorted by the first column, but the sort indicator will be where-ever it was when you exited the window last.



prod SJ			
Std Rule Name	Comment	Subscribed	Action
!International	International calls starting with 011	Yes	Forward
!NonUS	All Non-US Locations	Yes	Forward
!OutOfArea	Out of Area, Unknown, Unavailable for phone	Yes	Block
!Private	Private & Anonymous for Telephone #	Yes	Block
!Toll Free	Toll Free Numbers		
!Unassigned	Unassigned Area Codes	Yes	Forward
\$Predict	Predictive Scammer Blocking	Yes	Forward
\$Short	PhoneNo with too few digits	Yes	Forward
\$Vnnn	Vnnnnnnn in caller ID Name	Yes	Forward
AK	Alaska		
AL	Alabama		
AR	Arkansas		

Double click a rule to see detail. Single click column heading to sort.

When to Use Static IP Addressing

It is most convenient to use the default DHCP-based IP addressing. When used, DHCP will provide all networking parameters to your Scammer Jammer. Typically this is the best choice.

DHCP-based IP addressing has one disadvantage - it must periodically poll the router (DHCP server) to make sure it can continue to use the assigned IP address. As long as the DHCP server is available, this is not a problem.

If the DHCP server is inaccessible, then the SJ's poll process will take about 12 seconds waiting for the server but never getting a response. Should an inbound call occur during this process, the call will not be seen by the SJ. Minimally, you will not get any CID information, and worst case, the phone call may not be seen at all.

If your local network is unreliable or the DHCP Server/router is unreliable, it is better to use static IP addressing. When static IP addressing is used, the DHCP poll never occurs and so the SJ will not get stuck waiting for a poll to fail.

Appendices

Telephone Compatibility List

The following telephone handsets have been tested with Scammer Jammer and are known to display the enhanced caller ID properly.

Manufacturer	Model	Notes
AT&T	CL2909	
AT&T	CL2940	
AT&T	CL4940	
AT&T	CL80101	
AT&T	TR1909	
AT&T	TL96456	
GE/Thomson	29281FE1-A	
Motorola	L601M	
Panasonic	KXTA-624 / TVS-50	This is a key system and vmail processor. Because the voice mail is internal using vmail requires special programming.
Panasonic	KX-TGS110	
Panasonic	KX-TGD220N	CID circuitry is more sensitive than most
Panasonic	KX-TDG223N	
Panasonic	KX-TGF383M	
RCA	25413RE3-A	
VTech	CS6829	
VTech	CS6114	Very Rarely loses power
VTech	CS6919-16	Occasionally loses power
VTech	LS-6225	CID circuitry is more sensitive than most

Tested Handsets without Caller Id

Manufacturer	Model	Notes
Western Elec	Rotary Dial	Rotary Dial
Western Elec	CS500DM	Rotary Dial
Northern Tel	NE228A4	Rotary Dial

Telephone Carrier Compatibility List

Scammer Jammer is known to work with the following Telephone Service Providers:

Telco	Notes
CenturyLink	POTS
CenturyLink	VoIP
Comcast	VoIP
GoogleVoice/Obihai	VoIP

Recommended Answering Machines

If you wish to use a stand-alone answering machine instead of voice mail, these answering machines have been tested with Scammer Jammer.

AT&T 1739 Digital Answering System

This is a standard answering machine that works well. Ringing can be disabled and the minimum number of rings before pickup are 2. The only downside is you cannot turn off call screening if the user leaves a message.

No longer manufactured, but the AT&T 1740 is nearly identical.

AT&T 1740 Digital Answering System

This is a standard answering machine that works quite well. Ringing can be disabled and the minimum # of rings before pickup are 2. The only downside is you cannot turn off call screening if the user leaves a message.

Current cost is \$15.

AT&T CL4940 Corded Standard Phone with Answering System

This is a combo phone/answering machine - the phone features can't be used when it is connected to Scammer Jammer. While twice the cost of AT&T 1740 (\$32), it has the added ability to NOT screen incoming calls.

Menu Tree

This section illustrates the full Scammer Jammer menu tree.

In general the tree is negotiated using these keys:

Previous: Goes Up the tree at the same level. Pressing previous for Redial connects goes to Forward to Vmail.

Next: Goes Down the tree at the same level. Pressing next for Forward to Vmail goes to Redial Connects.

Select: Goes to the next level in the tree when pressed on a menu item that ends with '>' such as Network Settings. Pressing select for Settings> goes to Forward to Vmail.

Goback: Goes to the previous level in the tree. Pressing goback for Server Name will goback to Network Settings. There is an exception to this rule: if you are in the first level of Settings (Forward to Vmail, Redial Connects,...) then goback will goback to the main menu.

```
Settings>
  Forward to Vmail:
  Redial connects:
  AnsMach always on:
  Use distinct ring:
  Network Settings>
    Server Name:
    Server port:
    Use Static IP Addr:
    Static IP Settings:
      IP Addr:
      Subnet mask:
      Gateway Addr:
      DNS Addr:
  Advanced Settings>
    TimeOut settings>
      Redial timeout:
      DNS cache timeout:
      Net init timeout:
      Net start timeout:
      Ping Timeout:
      CID timeout:
      WDT timeout:
      DHCP Timeout:
      DHCP resp. timeout:
      Stat req std time:
      Stat req fast time:
    Modem settings>
      Modem baud rate:
      Modem country code:
    Mode settings>
      Lock mode:
    CID settings>
      Pass CID to phone:
      CID wave height:
      CID wave start:
```

```

Logging settings>
  syslog settings>
    syslog Port:
    syslog Pri Filter:
    syslog Server Name:
Lock settings>
  Lock PIN:
  Keypad lock:
Misc settings>
  Must ring on:
  LCD light timeout:
  Net fail to ansMach:
  Cache enabled:
  Send status req's:
  ADC threshold:
  Test for dial tone:
Factory RESET
Information>
  MAC address:
  IP address:
  NetMask:
  Gateway Addr:
  DNS addr:
  Server addr:
  syslog addr:
  Program version:
  Build date:
  Modem FW version:
  Uptime:
  EEPROM Version:
Diagnostics>
  Self tests>
    LCD tests>
      Tst Quick Brown Fox?
      Test Back light?
    Key test?
    Modem tests>
      Test simple AT?
      Test modem reset?
      Test Dial tone?
      Monitor line state?
      Monitor voltage?
      Test hang up?
    Handset tests>
      Monitor ADC value?
      Test Xfer SSR?
      Test Ans mach SSR?
    CID tests>
      Test inbound CID?
      Test outbound CID?
      Generate FSK tone?
    Network tests>
      DHCP Request?
      DNS Lookup?
      Ping local gateway?
      Ping SJS server?
    EEPROM test?
Free memory:

```

ADC Lo/Hi values:
Last abort code:
Last reboot reason:
StateQ at reboot>
Modem monitor:
Clear abort code
Force WDT timeout
CID ACK Testing:
Call Log>
Restart

Settings Menu

Forward to VMail (ON/OFF, Default: ON)

If your telephone company provides voice mail service OR your Scammer Jammer is connected through an external answering machine, you should turn this option ON.

When this option is ON, Scammer Jammer will **Forward** calls by letting the incoming call ring until voice mail or an answering machine answers.

If you have an external answering machine connected to the Scammer Jammer's AnsMach port, this setting should be OFF.

When this option is off, Scammer Jammer will **Foward** calls by connecting the call to the AnsMach jack.

Default changed to ON in version 1.02 of firmware.

Redial connects (ON/OFF, Default: OFF)

Redial connects allows callers to skip Scammer Jammer's call screening entirely by redialing.

When enabled, if a caller is forwarded or blocked they can call back within 60 seconds and Scammer Jammer will connect them to the telephone handset.

This feature can be useful to allow family/friends/coworkers the ability to still contact you when Scammer Jammer would normally forward or block their calls.

AnsMach always on (ON/OFF, Default: OFF)

When enabled, the ANSMACH port is ALWAYS connected to the line. If the answering machine is set to pickup on ring 4, it will still pickup on ring 4.

When disabled, the external answering machine is only connected to the line after Scammer Jammer determines a call must be forwarded to it.

Rather than turning this option on, it is recommended that the telephone line connect to the external answering machine, and Scammer Jammer then connect to the answering machine.

Use Distinctive Ring (ON/OFF; Default: OFF)

This setting must be enabled when the telephone company sends distinctive ring.

Distinctive Ring is used when you have two phone numbers assigned to a single phone line. Each number will play a different ring cadence.

The standard ring cadence used in the United States is a 2 second ring followed by a 4 second silence.

Any non-standard ring cadence must fit into the first 2 seconds. The second 4 seconds must always be silent for Scammer Jammer to operate correctly.

Network Settings

Server Name (Default: SJS.XYFYX.COM)

The name or IP address of the Scammer Jammer server.

Server port (Default: 11183)

The port number of the SJS service.

Use Static IP Addr (Default: OFF)

ON - Use Static IP addressing.

OFF - Use DHCP (Dynamic) IP addressing.

Static IP Settings

NOTE: Static IP Settings will be set to the last DHCP settings negotiated. Thus, if the DHCP subnet mask were 255.255.255.0, the static subnet mask will be set to the same.

The static IP address is also initialized in this manner except the last byte will always be ".0".

IP Addr

Subnet Mask

Gateway Addr

DNS Addr

Advanced Settings

TimeOut settings

These settings should only be changed when advised. Poor choices for these settings can cause Scammer Jammer to fail.

Redial timeout (Range: 15-240 secs; Default: 60)

If *Redial connects* is enabled, this is the amount of time the caller has to place another call to bypass Scammer Jammer's call screening.

DNS cache timeout (Range: 1-1440 mins; Default: 30)

Time between updates of the SJS server's IP address.

Net init timeout (Range: 15-240 secs; Default: 30)

If the local network is down, this is the time to wait between attempts to reinitialize the network hardware.

Net start timeout (Range: 5-60 secs; Default: 10)

If the local network is down, this is the time to wait between attempts to reinitialize the network software.

Ping Timeout (Range: 15-240 secs; Default: 15)

Time between ping attempts to determine source of network failure and if issue has been corrected.

Ignored after version 1.0 of Scammer Jammer firmware.

CID timeout (Range: 250-5000 ms; Default: 500)

Time to wait for CID transmission from modem.

WDT timeout (Range: 30-3600 secs; Default: 30)

Time to wait before assuming a software hang/loop and rebooting the unit.

DHCP timeout (Range: 1-255 secs; Default: 10)

Under normal circumstances, 10 seconds should be fine. If there is an issue with the DHCP server being intermittent, you may wish to reduce the timeout so Scammer Jammer realizes sooner there is a network issue.

5 second timeout has been tested and appears to not cause issues during normal operations.

This setting should only be changed when advised. Poor value choice can make Scammer Jammer fail to work.

DHCP Response Timeout (Range: 1-255 secs; Default: 4)

This setting should only be changed when advised. Poor value choice can make Scammer Jammer fail to work.

Stat req std time (Range: 2-60 minutes; Default: 10)

The interval between standard status requests.

Stat req fast time (Range: 10-120 seconds; Default: 30)

The interval between fast status requests.

When a status request gets a response, or a key is pressed, the Status Request interval changes from the standard time to the fast time.

Modem settings

These settings should only be changed when advised. Poor value choice can make Scammer Jammer fail to work.

Modem baud rate(Range: 1200-9600; Default 2400)

This should always be set to 2400. One would change it only if there were issues communicating with the modem.

Modem country code (Default: B5)

Scammer Jammer only operates in the United States and so the country code should always be B5. This setting allows the country code to be changed should it become wrong.

Mode settings

Lock mode (ON/OFF; Default: OFF)

If set to ON, changing the Mode is locked and it cannot be changed.

CID settings

Pass CID to phone (ON/OFF; Default: ON)

Under normal conditions, this option is set to ON and caller ID is generated and sent to the handset.

If, for some reason, the Scammer Jammer generated caller ID signal reacts badly with the handset, you can disable generation of the caller ID signal.

Caller ID information is always visible on the Scammer Jammer LCD display.

CID Wave Height (511, 1023, 2047, 4095; Default: 2047)

Controls the CID AFSK wave's maximum value output to the D/A converter.

Change this value ONLY if instructed to do so.

CID Wave Start (0, 270; Default: 0)

Controls the CID AFSK wave's start angle. Scammer Jammer can begin wave generation at 270 degrees (-Vpeak) or at 0 degrees (0V).

Change this value ONLY if instructed to do so.

Logging settings

syslog settings

syslog port number (Default: 11184)

This is the port number of the remote syslog server. Change this value only if instructed to do so.

syslog priority filter (Default: 5)

This determines which events to transmit. Events with a priority \leq the priority filter will be transmitted. Most of Scammer Jammer's events are assigned to the following priorities:

- 0 Crash/Reboot
- 1 Restart
- 5 Important events
- 6 Debug information
- 7 Very verbose information

Change this value only if instructed to do so. A value > 5 can sometimes cause slow network responses. Values < 5 greatly reduce the ability to resolve possible problems.

syslog server name (Default: SJS.XYFYX.COM)

Change this value only if instructed to do so.

Lock settings

Lock PIN (Range: 0-9999, Default: 0)

Value of PIN used to unlock keypad.

Keypad Lock (ON/OFF, Default: OFF)

Enable/disable keypad lock. When enabled, it is not possible to change/view any Scammer Jammer settings until the correct lock PIN is entered.

Misc settings

Must ring on(Range: 2-10, Default: 2)

Ring number on which Scammer Jammer MUST allow phone to start ringing if server hasn't yet responded with an action.

The Scammer Jammer server can almost always return the action to take (Connect, Forward, Block) before ring #2 starts. But occasionally there may be network or server slowness so the action is not known before ring #2 starts.

This setting instructs Scammer Jammer how to proceed if the action isn't returned before ring #2 starts. Using this setting, you can tell Scammer Jammer it must start ringing the phone on the requested ring number even if it doesn't have the action.

If the handset is connected because Must Ring On has been reached, Scammer Jammer continues to wait for a response from the server. If, while ringing, a response from the receiver is received from the server indicating the call should be forwarded or blocked, Scammer Jammer will go ahead and forward or block the call. If, however, the phone has been picked up, Scammer Jammer will ignore any further response from the server.

If Scammer Jammer connects handset to let it ring AND the incoming telephone # is in cache, it will use information from the cache. See [Cache Enabled](#).

If Scammer Jammer doesn't have cache information for the call, it will transmit the telephone company's caller ID information with a call indicator of '*'.

Using *Must Ring On* with Voice Mail

Voice mail typically picks up on ring 5. This limits the number of silent rings you should allow. A value higher than 3 is not recommended.

If Max Silent Rings is 3, the handset can only ring 2 full times and just a bit of ring 5 before voice mail picks it up. That isn't much time to answer the phone before vmail picks up.

If Max Silent Rings were set to 5, you would never hear the phone ring before voice mail picks up.

LCD Light Timeout (Range: 0-255 seconds; Default: 60 seconds)

When a message is displayed on the LCD screen, the backlight is turned on for the amount of time specified by this setting.

If a value of 0 is selected, the backlight is never turned on.

Net fail to ansMach (ON/OFF; Default: OFF)

If the network fails, Scammer Jammer's normal operation is to then connect all incoming calls to the handset since it cannot receive directions from Scammer Jammer server as how to direct inbound calls.

If Net fail to ansMach is set to ON, the rather than connect all calls to the handset, all inbound calls are connected to the answering machine when the network is down.

If a phone number is cached, it will be processed in the same manner as it was the last time a call was received from that number.

Cache enabled (ON/OFF; Default: ON)

Occasionally, Scammer Jammer will not receive information from the Scammer Jammer server. This can be due to the network being down or due to *Must Ring On* being exceeded.

If Scammer Jammer does not receive an action from the server, it will look in its **call cache** to see if it has processed the same telephone number before. If it has, it will follow the same action as it did before.

If you use the EXCEPT option to change when calls may be connected or forwarded, Scammer Jammer will follow the LAST action for a number which may not be the same as it would be during the current time period.

If you use the EXCEPT option, you may wish to turn Cache enabled OFF so calls that should Connect aren't incorrectly forwarded.

The cache is not stored if power to Scammer Jammer is removed. Upon restarting Scammer Jammer, the cache will be empty.

Disabling then enabling cache will also clear it.

Send status req's (ON/OFF; Default ON)

Enable transmission of status requests.

This setting should only be changed when advised.

ADC threshold (Range: 5-500; Default: 50)

If set too low, Scammer Jammer will sense the handset off hook when it is not. If set too high, it will not see the handset go off hook.

This setting should only be changed when advised.

Test for dial tone (ON/OFF; Default: ON)

Allows Scammer Jammer to test the line for dial tone to determine if it is up.

The ability of Scammer Jammer to reliably report No Dial Tone depends on the telephone service provider. In some cases, Scammer Jammer may not detect absence of dial tone or it may incorrectly report absence of dial tone when it is present.

If Scammer Jammer incorrectly reports No Dial Tone, then you can disable this testing by changing this setting to OFF.

Factory RESET

This option will reset ALL settings to the factory settings (defaults as shown).

Warning and Error Messages

Message	Meaning	Internal Name
Any key to continue	Press any key on the Scammer Jammer unit to continue processing.	sc_anyKey
Backing Up EEPROM	Displayed momentarily when EEPROM is copied to Scammer Jammer server.	sc_backupEp
EEPROM initialized	EEPROM has been initialized to factory defaults.	sc_eprInit
EEPROM updated	EEPROM updated to new version.	sc_eprUpd
Failed	The attempted self-test failed to function properly.	sc_failed
Inbound call...	A new incoming call has been detected. This message will shortly be replaced with caller ID information once available.	sc_inbound
Initializing...	This message is displayed when power is first applied and indicates Scammer Jammer is not yet ready to process calls.	sc_init
Initializing Modem...	Displayed during modem self-test.	sc_mdmlInit
Log Empty.	The call log is empty.	sc_logEmpty
Network Problem!	Scammer Jammer cannot access the Scammer Jammer server over the network.	sc_noNet
No Caller Id Avail.	No caller ID information was received from the Telco. This can occur if you don't subscribe to the caller ID service. It can also occur if a new call comes in just as an old call is hung up.	sc_noCid
No Dial Tone! Check Telco Jack.	Scammer Jammer is not receiving dial tone from the telephone line.	sc_noDT
Outbound call...	An outbound call is in progress.	sc_outbound
Restarting...	Scammer Jammer is in the process of restarting.	sc_restarting
Save Failed!	Scammer Jammer was unable to save new action to Scammer Jammer server.	sc_saveFailed
Scammer Jammer NEW	When the NEW message is displayed, call Log contains unreviewed entries.	sc_SJNew
SJS DNS Lookup Fail!	DNS Lookup of SJS Server has failed. DNS Server name in config may be wrong.	sc_badDNS
WDT timed out.	Watch Dog timer has expired. Scammer Jammer will automatically restart. This should be an infrequent occurrence, and Scammer Jammer will recover automatically.	sc_wdtPopped

Call Indicator

When Scammer Jammer receives a call, it will first display (on its LCD), the raw caller ID information such as

Joe Smith
101-555-1212

Once Scammer Jammer begins processing the call, it will put a single character prefix, the indicator, on the caller's name such as

+Joe Smith
101-555-1212


Further, this indicator will be transmitted to the handset if it rings.

Indicator	Meaning
+	Allowed caller - Connect Rule used
?	Unknown caller - Forward rule used
-	Blocked caller - Block rule used
\$	Telemarketer - Telephone number in Scammers database.
#	User called back - Redial Connects allowed caller to connect.
*	Must Ring On ring# has occurred.
!	Network Failure. Not displayed if calling telephone number is found in cache.
	Can't authenticate with Scammer Jammer server. Device or account has been inactivated.

Troubleshooting

Error	Solution
Scammer Jammer remains in Outbound Call state even when handset is placed on-hook.	<p>The telephone line connection may have been lost during a call.</p> <p>Scammer Jammer cannot detect circuit loss if the telephone is off-hook and it goes back on-hook while the connection is down.</p> <p>If you see the "Outbound Call..." message on Scammer Jammer's status screen and the telephone is hung up, pick it up and check for dial tone.</p> <p>Verify Scammer Jammer is properly connected to the telephone company jack and the jack is providing dial tone.</p> <p>You can connect the handset directly to the telco jack to verify dial tone is being received.</p> <p>If the telephone is hung up, you can cycle power on Scammer Jammer which will allow it to disconnect the handset from the telephone circuit and correctly report "No Dial Tone".</p>
Scammer Jammer remains in Outbound Call state even when handset is placed on-hook.	<p>First, verify you have dial tone going into Scammer Jammer's Telco jack.</p> <p>The ADC Threshold may be too small.</p> <p>Typically, when all handsets are on hook, the ADC value should be 0 to 1; however, if Scammer Jammer's handset jack is connected to multiple phones and house wiring, ADC may be in the 10-20 range.</p> <p>If ADC output is > threshold, Scammer Jammer assumes a telephone has been taken off-hook and initiates an outbound call.</p> <p>Try increasing ADC Threshold.</p>
When handset is taken off-hook, user does not get dial tone.	<p>First, verify you have dial tone going into Scammer Jammer's Telco jack.</p> <p>The ADC Threshold is most likely too large.</p> <p>Typically, when a handset is off-hook, the ADC should be greater than 200.</p> <p>If ADC output is less than the ADC Threshold setting, Scammer Jammer assumes all phones are on-hook and does nothing.</p> <p>Try increasing decreasing ADC Threshold.</p>

<i>Outbound...</i> message will occasionally show briefly on Scammer Jammer LCD display even though no one has picked up handset.	Some telephones have a feature to check voice mail. They do this by going off-hook and listening to the dial tone. If the stutter dial tone is heard, indicating waiting voice mail, then the phone will light some kind of indicator.
Scammer Jammer reports "No Dial Tone", but dial tone is present.	Scammer Jammer detects loss of dial tone by monitoring the telco line's voltage. Your telco's voltages may be outside what Scammer Jammer considers "normal". If this problem occurs, turn "Test for Dial Tone" off.
Scammer Jammer reports "No Caller ID / 000-000-0000" even though caller ID service is enabled.	There are two conditions that can cause this error. This should rarely happen, but there are several reasons Scammer Jammer might not be able to decode the caller ID. The most common reason for getting No Caller ID is due to call waiting. Usually, Scammer Jammer will properly handle call-waiting. But sometimes if you hang up on a call and a waiting call does a 'ring-back' to let you know it is still waiting, that might register as "No Caller Id". Another reason for No Caller Id is two successive calls. If caller #1 hangs up before ring #1 is complete (and thus no caller ID is transmitted), then caller #2 just happens to call within a few seconds afterwards this will appear to Scammer Jammer as a single call with no Caller ID. Finally, if the telephone is picked up before Scammer Jammer receives the caller ID signal it will generate this error. If a call just starts and you pick up the telephone to place an outbound call that will interrupt receiving caller ID.
SJ report "No Network"	This message appears anytime SJ can no longer reach the remote SJ server (sjs.xyfyx.com). SJ will 'ping' the remote server about every 10 minutes to make sure it can be accessed. If this 'ping' fails you will get the <i>No Network</i> message. You will also get the <i>No Network</i> error if SJ fails to access the SJ server during an inbound call. It is best to not turn the SJ off to attempt clear this message until all other troubleshooting fails. Doing so will clear its list of past incoming calls and it will not be able to block any calls without that list. <ul style="list-style-type: none"> ● Can any other PC on your local network reach the internet? For

	<p>example make sure you can reach www.google.com on your PC. If not, troubleshoot your network until your PC works. Once it works, the <i>No Network</i> error will clear itself.</p> <ul style="list-style-type: none"> ● If your PC can reach www.google.com fine, then try www.xyfyx.com. If that fails, the SJ server is down. Report the problem to SJ support. Once you can reach www.xyfyx.com, the <i>No Network</i> error will clear itself. ● If your PC can reach www.xyfyx.com, then the problem is probably with the SJ unit itself or the wiring. Examine the back of the SJ (again without removing power). The network jack should have a solid green LED light on the left with a blinking yellow light on the right:  <p>If there are no lights on, check wiring from the SJ to your network router or switch. If there are no lights, either there is a cabling issue or the router / switch has no power.</p> <ul style="list-style-type: none"> ● If both LED lights are on and SJ still doesn't work, try rebooting the router and waiting several minutes for the router to reboot and SJ to obtain an IP address. ● If SJ still doesn't work, debugging is more involved. Depending on your familiarity of network equipment, you may wish to obtain help with the rest of this procedure. <p>Examine the IP configuration of the SJ. See the Menu Tree appendix to help you locate the SJ information menu. Then examine the IP configuration values for your SJ:</p>

	<p>IP address: This should NOT contain 0.0.0.0. If it doesn't, then the SJ is NOT obtain a valid IP address from the DHCP server.</p> <p>NetMask: This should typically contain 255.255.255.0 though other values are possible. It should NOT contain 0.0.0.0.</p> <p>Gateway Addr: This should contain the IP address of your router.</p> <p>DNS addr: This should contain the IP address of your DNS server.</p> <p>Server addr: This should contain the IP address of the SJ server.</p> <ul style="list-style-type: none"> • If settings look proper, then the last step is to run the network diagnostic tests. Those tests are beyond the scope of this document. You should contact SJ support for further help.
Late in the evening, Scammer Jammer's LCD display lights up but there is no incoming call.	<p>For older copper voice lines, the telephone company will run tests. When this test occurs, Scammer Jammer will see the telephone circuit go down and then come back up.</p> <p>Scammer Jammer will actually report the circuit is down, but then it comes backup so fast it is unlikely the message will be seen. But the LCD back light stays on for 60 seconds or so and that you may see.</p> <p>To date, the testing that has been observed has occurred late in the evening after 10PM. That may not always be the case, though.</p>
No caller ID transmitted to telephone handset.	<ul style="list-style-type: none"> • Verify SJ receives Caller ID information by examining the device log or the call log in sjsconfig. • Make sure the "Pass CID to phone" setting is set to Yes. • In diagnostic self tests, run the Test outbound CID. • In diagnostic self tests, run the Generate FSK Tone. If there is no tone it is a hardware issue.

Resetting EEPROM

If Scammer Jammer hangs during start up, it is possible to externally reset EEPROM (typically this is done in the menu when Scammer Jammer is running).

You will lose all configuration settings when you reset EEPROM. Only do this as a last resort.

To Reset EEPROM, turn Scammer Jammer off. While pressing the center select button and the left arrow button, restore power to Scammer Jammer. After the copyright notification, you will be given a chance to Reset EEPROM.

Revision History

April 16, 2021

- Fixed references to "Answer Only" to "Forward Connects".
- Fixed references to "Block Only" to "Connect Forwards".

May 29, 2020

- Added section on Nuisance calls.

January 17, 2020

- Removed procedure for installing using Wine Bottler. Full Mac support makes this procedure unnecessary.
- Document new Default Action found in the Rules form.

September 13, 2019

- Added new section, "Caller ID Name Based Rules".

August 3, 2019

- Discuss DHCP vs Static IP addressing

Jun 14, 2019:

- Update for new “Next” column in Call History Log.

January 16, 2019

- Added section for SJ Settings

November 25, 2018

- Updates for Dogwood release.
- Added section on installing native Mac version of sjsconfig.
- Added section on sjsconfig’s usage for the Mac native version.

November 4, 2018

- Added section on installing sjsconfig into WineBottle for Mac OS.

September 14, 2018

- Updated order in which rule sources are executed.
- Added \$Predict standard (system) rule.
- Document troubleshooting of No Network error.

June 21, 2018

- Update manual for Birch-delta-1 release.

May 25, 2018

- Max Silent Ring is now Must Ring on.

May 18, 2018

- Added Call History Log Box and new Icon

May 8, 2018

- Version 2 of User's Guide

Sept 13, 2016:

- Version 1 of User's Guide