≡scannexIII

Scannex Collector Manual

Thursday, 28th August 2008

Issue 3

Document History

Issue	Date	Comments
01	08-Oct-2004	Initial Release.
02	19-Nov-2004	General update.
03	28-Aug-2008	Update for ip.buffer

Scannex Electronics Ltd, UK
t: +44(0)8707 48 65 65
f: +44(0)8707 48 67 67

http://www.scannex.co.uk
info@scannex.co.uk

Scannex LLC, USA
t: 1-866-4BUFFER
(1-866-428-3337)

http://www.scannex.com
info@scannex.com

Table of contents

Overview

The Scannex Collector application provides a convenient way to collect data from the Scannex ip.buffer, NetBuffer and ModemBuffer products. Some of the major features are as follows:

- Supports encrypted and plain text data transfers

- Supports the ip.buffer zlib decompression

- Outputs the collected files using simple file locking (to provide compatibility with most external applications)

- Allows scheduled collection using FTP to both ModemBuffers and NetBuffers

- Includes an SMTP server so that emails can be received from the buffers

- Includes a proxy service to allow TCP/IP management applications to connect through the Scannex Collector and use an encrypted and authenticated TCP/IP session to the remote buffer

- Sends logs and events to disk and to the SysLog service

- Stores the past 7 days data and emails (configurable)

- Fully multithreaded 32-bit Windows application

- Capable of handling hundreds of sites

Installation and Configuration

Installation

Use the setup_secollector.exe application, and follow the on-screen prompts.

Requirements

- Windows 98, 2000, XP

- An installed and configured modem (if using ip.buffer PPP and/or ModemBuffers)

Installation Directory

When choosing an installation directory, consider the following points:

- The list of sites is stored in the same directory as the application (this is not optional)

- The default queue and archive directories are underneath the application directory (though these can be changed after installation, within the program options)

- There are no DLLs or other additions – the application is self contained.

Configuration

The global options for the Collector are available from the menu "File | Options".

NOTE:

You will need to enter at least one site for the Collector to work.

Dial Up Connection

If using ModemBuffers, you will need to create a dial up connection for the Collector. The "File | Options" menu item includes a button on the "Collection" tab page that will start the Windows new connection wizard for you.

You need to create a "Dial up to a private network" (Windows XP terminology), with any phone number (just enter "123" – the Collector will override the number entered here).

When asked to name the connection, call it "SECollector", or "ModemBuffer" – something to associate it with this application.

It is best to preset the IP addressing for this connection. In XP:

- Explore the dial up connections (Start | Settings | Network Connections, right click and select "Explore").

- Right click on the newly created connection, and select "Properties"

- Select the "Networking" tab page

- Double click on "Internet Protocol (TCP/IP)" that appears in the list underneath "This connection uses the following items:"

- Select the radio button "Use the following IP address:"
    - Enter an IP address that is **not** on your LAN. E.g. 192.168.234.1
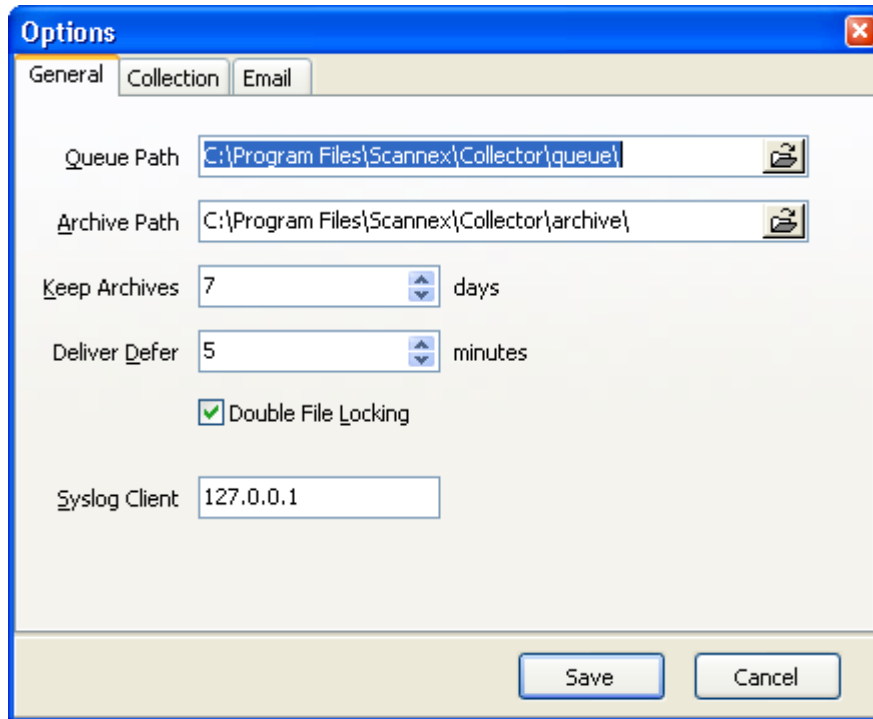   - (The DNS server entries can be left blank)
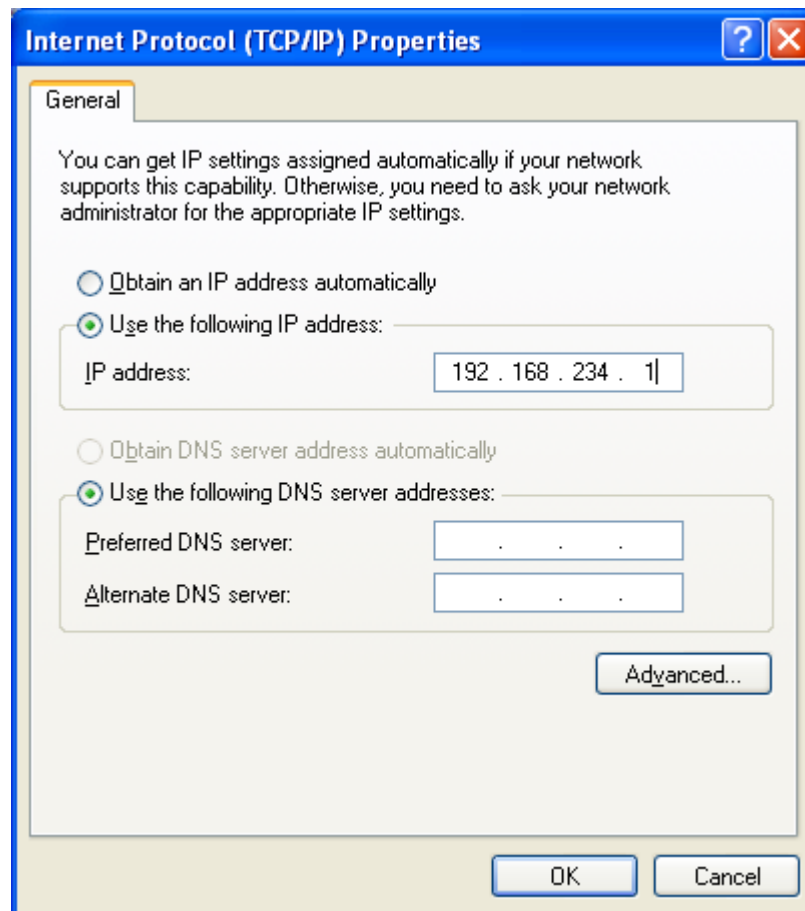
- OK all the dialog boxes

Even if these steps are not followed, the Collector will detect the IP address of the ModemBuffer.

Global Options

These are accessed via File | Options.

General

Queue Path

The Queue contains files that are pending output. Files stored in this directory will be appended to their appropriate output files as and when those pre-existing output files disappear (see the section on "File Locking" above).

WARNING! You should NEVER access the files within this Queue directory. The files are private to SECollector! Your application should always access the individual file outputs (as set in the Site parameters).

Archive Path

The Archive stores all data files that have already been output. It also holds all emails that arrive, and all the log files.

Files within the archive are deleted when they are older than the "Keep Archives Days" value.

Keep Archives Days

Sets the number of days to keep emails, logs, and data files that are contained in the "Archive Path".

Deliver Defer Time

If a queued file cannot be output (because the output file is in use, or there is a problem creating the file) the queue manager will leave the particular site alone for this time. Because the queue outputs in a sequential fashion (ie one site at a time), 'problem' sites must be deferred to allow the other sites a chance.

Double File Locking

When checked the output mechanism of SECollector will only copy queued data to the output if the destination file *does not exist*.

When unchecked, the output mechanism of SECollector will use Windows file-locking techniques and will append to the destination file. However, the application that is reading the destination file must be able to cope with SECollector appending while it itself is reading.

Please see page 18 for more information.

Syslog client

Set the IP address of the machine that should receive the Syslog messages. By default this is 255.255.255.255 – i.e. broadcast to all addresses.
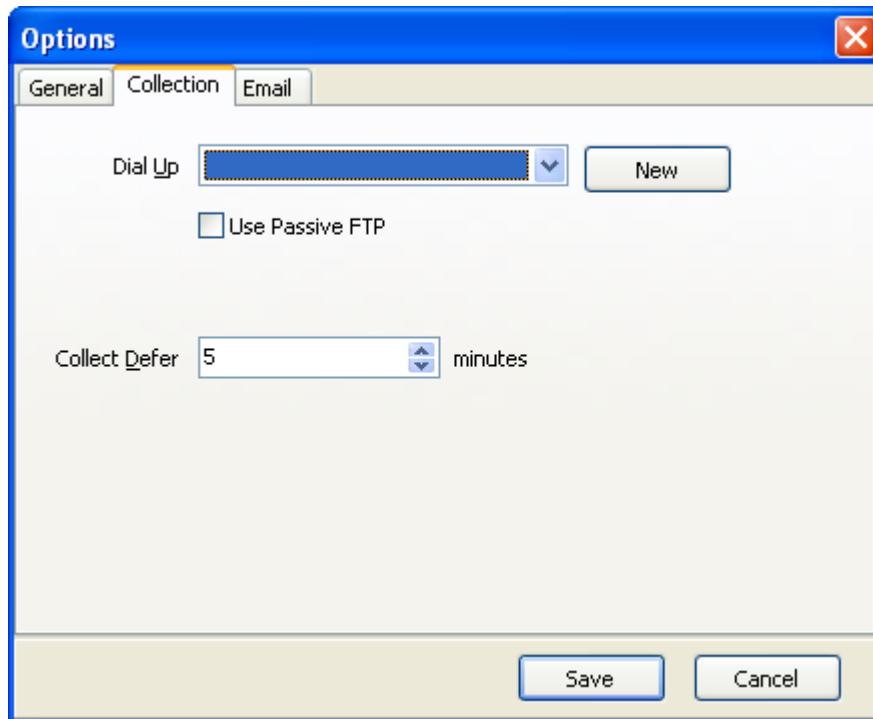
Dial Up

Sets the dial up connection to use for all *outbound* accesses. The Collector requires only one dial up connection, irrespective of the number of sites programmed.

If you have inbound, dial-in, access for email collection you need to configure the dial-in connections too (depending on the number of modems connected).

Use Passive FTP

Usually this option should be left unchecked. If there are firewall issues (specifically the PC running the Collector is itself behind a firewall), check the box.

This is a global setting, and cannot be applied on a per-site basis.

Collect Defer Time

If there is a problem connecting to the remote NetBuffer or ModemBuffer, the site is deferred so that other sites can use the dial-up connection. The default is 5 minutes.

Deferred collections can be manually overridden using the "Site | Collect Now" menu.
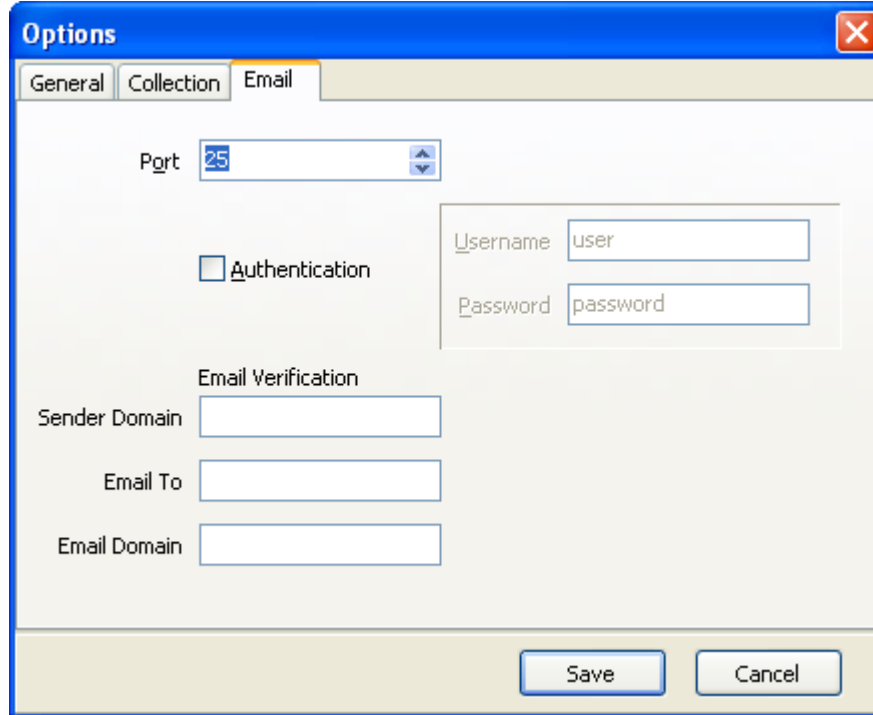
Email

The Collector includes a fully functional SMTP server. If remote buffers connect across the internet, or another public network, there are various options to validate the email sender. All other senders, for example people trying to use the server to send spam, are rejected.

Port

The default port for SMTP traffic is 25. However, if the remote buffer send emails via an ISP (Internet Service Provider), it is advisable to use a different port (such as 20025). More and more ISPs intercept the SMTP traffic on port 25 to check the outbound emails for viruses or spam.

It is advantageous to use a point-to-point connection (ie. remote buffer connecting directly to the Collector). This minimises any risks of data loss or out-of-sequence delivery.

Authentication

If the remote buffers are delivering directly to the SMTP server, then you can enable Authentication. If enabled, all emails must be authenticated.

HINT: When setting up SECollector, leave all the authentication fields BLANK first. When the system is running you can then "lock down" the system by filling in the appropriate values.

NOTE: If you are using the public DNS MX entries to nominate this server, or if you expect other SMTP servers to relay the traffic onto the Collector, you cannot

use Authentication. However, because of the risk of out-of-sequence delivery it is strongly suggested that you use a point-to-point delivery rather than relaying through other SMTP servers.

Username & Password

Enter the username and password for authentication. This same username and password must be also entered into every remote buffer that connects to this Collector.

Sender Domain

The Collector SMTP server can validate emails based on the sender's domain.

The default is blank – accept all sender domains.

To restrict emails, enter a domain (fictitious or real) and enter this as the SMTP Domain in all the remote buffers.

Email To

The Collector SMTP server can validate emails based on the destination email address.

The default is blank – accept all email addresses.

To restrict emails, enter a name (e.g. secollector) and enter this as the first part of the "Email To" within all the remote buffers.

Email Domain

The Collector SMTP server can validate emails based on the destination email domain.

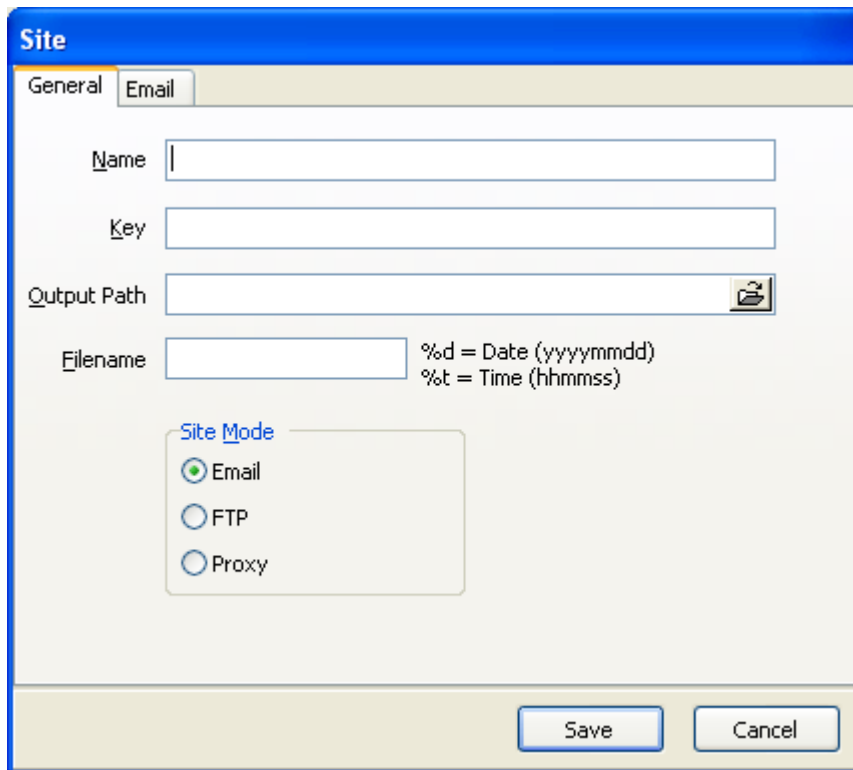The default is blank – accept all destination email domains.

To restrict emails, enter a domain (fictitious or real) and enter this as the second part of the "Email To" within all the remote buffers (ie the part after the @ symbol in the email address).

Note: Incoming emails must be *from* a remote buffer that has already been entered into the site list. If the remote site name cannot be matched to a name in the Site List, the SMTP server will reject the email.

Entering Sites

Use the menu option "Site | New Site" to begin entering the site details.

General

Name

Enter the name of the site. If this is to be a site that will receive emails the name entered here *must* match the Box Name entered in the remote buffer.

The Name cannot be amended once the site is created, but instead incorrectly named sites will need to be deleted from the site list and set up again.

Key

This is the encryption key for the site. If encryption is not enabled in the remote buffer, leave this field blank.

The key is a hexadecimal number, and ideally should be unique to each remote buffer. That way, if a key is compromised you only have one key to change (analogous to have one key for your house, car, garage, work etc. If you lose the key or someone else obtains it, you risk access to all places!)

Output Path

The output path for the data, works along with the Filename. If the Output folder set doesn't exist, the appropriate folder will be created.

Filename

The filename for the output data. If the Filename is left blank then the files will be queued and appear as "Output Unavailable" until updated.

The Filename can be set to include the current date and/or current time by using the variables %d and %t respectively (for example, a Filename set as NetBuffer%d-%t will create Netbuffer20041117-163246). In this case, the external application needs to process a directory, rather than a single file.

Site Mode

A choice of Email, FTP, or Proxy.

Email is for situations where the remote buffer elects to send the data (either on a timed, or triggered basis). Additionally, if using ModemBuffers, the sender pays for the call.

FTP is where you need to schedule the collection from the central Collector (and all modem accesses are paid for by the central site).

Proxy is for situations where you need a local TCP/IP-to-device connection. For security it is strongly suggested you enable encryption on the remote device. That way any would-be attackers need the private secret, the key, to gain read/write access to the managed device. (For example where a ModemBuffer is connected to the management port of a PBX.)

Trigger Phone

The ModemBuffers (as of firmware 1.13) include the ability to ring the buffer and hangup within 10 seconds to trigger an email delivery.

At the moment this field is for information only – you must manually call the remote ModemBuffer, listen for the first ring and hangup immediately. The ModemBuffer will then reply by dialling out and sending an email (with data attached if programmed to deliver data by email).

Connect

Choose a connection method to the remote site: either networked or modem.

If networked, enter the remote buffer's IP address or name.

If using a modem, enter the phone number, and the dial-up username/password (e.g. as entered in the ModemBuffer r130 and r131 registers).

Port

Enter the port for FTP access. The default is port 21, however this may be changed in the NetBuffer or ModemBuffer (r300).

Username & Password

Enter the FTP username and password, as entered in the remote buffer. The defaults for the devices are "user" and "password", but may be changed through the NetBuffer's web-interface, or the ModemBuffer's r301 & r302 registers.

FTP Schedule

- Check the days of the week you require FTP collection.

- Choose between "Once daily" and "Interval"
    - If Once daily, enter the start time
    - If Interval, enter the start and end times, as well as the hours:minutes interval to collect

If you choose "Interval" for Zone A, you can also decide how often to collect when *outside* the day and time limits for Zone A. Zone B specifies the option for all time periods "outside Zone A".

For example, you may wish to collect every 5 minutes during working hours from a NetBuffer, and every 4 hours outside of working time. Tick the working days, select "Interval" for Zone A, and enter the start and end times. Select 00:05 for the Zone A interval. Now select "Interval" for Zone B and enter 04:00 for the Zone B interval (as shown in the figure above).
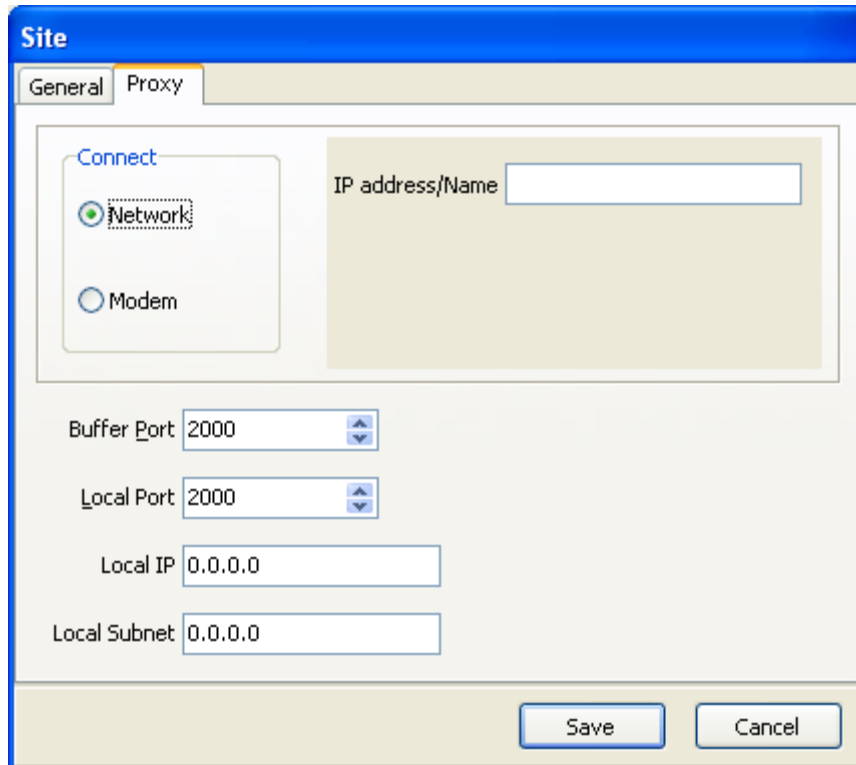
Proxy

The proxy allows a bridge between an unencrypted TCP/IP local connection and a remote, encrypted NetBuffer or ModemBuffer. The remote buffer should be configured for Serial->TCP2, TCP1->TCP2 (for the NetBuffer), or r210="T" (ModemBuffer).

Connect

Choose between Network and Modem. If Network, enter the remote buffer's IP address or name. If Modem, enter the ModemBuffer's telephone number and dial-in username and password.

Buffer Port

The buffer port is the port entered in the remote buffer for the TCP connection. For the NetBuffer this is the TCP2 port (leave the NetBuffer's TCP2 address blank, or enter a # followed by the Collector's IP address to restrict access). For the ModemBuffer this is the value entered in r221 "TCP2 Port".

Local Port

Choose a port the Collector should listen on. Do not use 80, 21, 25, or the SMTP port (if other than 25). The application you use to connect should be programmed with the same port.

Local IP & Local Subnet

By default these are both "0.0.0.0" implying that any local device can connect to the Collector. To provide software restrictions enter appropriate values.

For example, to restrict local access to the 192.168.0.x range, enter "192.168.0.0" and "255.255.255.0" respectively.

Note: It is better to use a hardware or software firewall to restrict inbound access. Additionally, if a firewall is in place, make sure that inbound port access is allowed for all machines that need to have access to the proxy functions of the Collector.

Saving

The site list is held in memory and must be saved to disk. The disk file is written to whenever you exit the Collector.

However, if you have made significant additions or changes to the list, use the menu option "Site | Save Sites" to perform an immediate save.

The site list is saved in the file "Sites.csv" within the application subdirectory.

If opening or amending the Sites.csv file directly for any reason, this needs to be done with care since some editors (eg Microsoft Excel) may reformat the file when it is saved, thus causing incorrect site information.

User Interface

The main form of the Collector can be hidden to the system task-tray. Just press the minimise or the "X" in the top right of the window.

NOTE: Pressing the "X" will not close SECollector – merely hide it! To close SECollector use either the "File / Exit" option, or right click on the SECollector task tray icon and select close.

To restore the main form, double click the Collector icon in the system task tray, or right-click the system task tray icon and select "Restore".

Site List

The site list shows the sites in memory. You may:

- Click on a column heading to sort

- Click on a column heading again to reverse the sort order

- Edit a site by double clicking (or pressing Enter)

- Select a site and right click to gain a context menu (for deleting or collecting now)

- Filter the site list with the "Filter" option

    o **All** shows all sites.

    o **Active** shows all sites that have connections.

    o **Idle** shows all sites that do not currently have connections.

    o **Queued** shows the sites that have data in the queue directory.

    o **Error** shows sites that have temporary, or permanent, errors.

    o **Pending** shows the FTP sites that are in the queue awaiting collection.

Selecting a site will show the site's log and information in the lower panels.
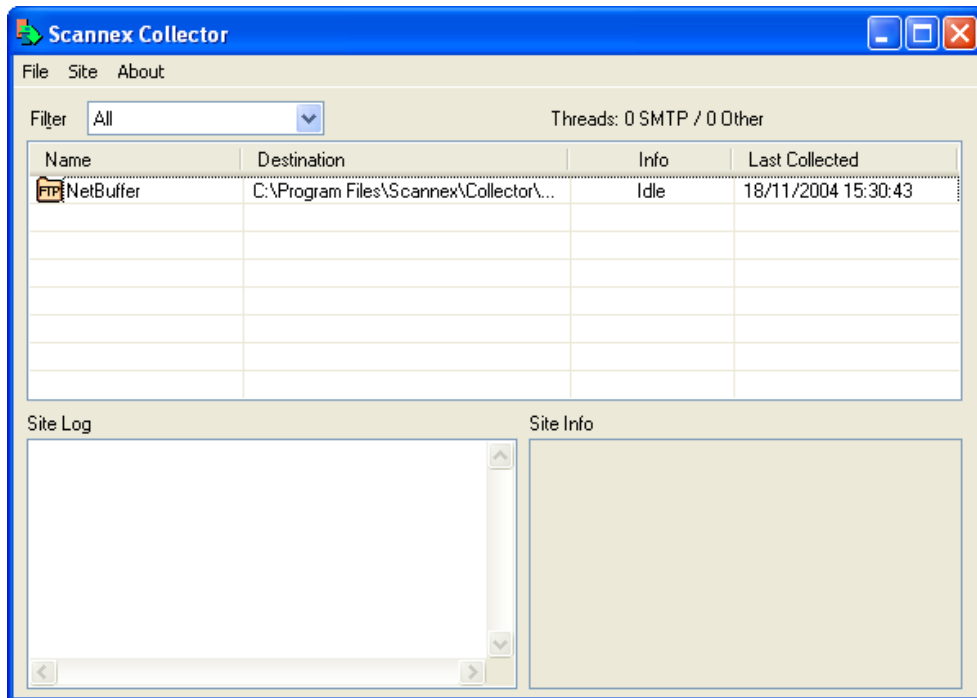
Collect Now

When collecting by FTP, you can force an individual site to collect, by highlighting the site and selecting Site | Collect Now.

Deliver Now

If the output file is unavailable for any reason, the Collector will continue to attempt to deliver at intervals (as set in the Global Options, Deliver Defer Time). However, you can force an individual site to reattempt delivery by highlighting the site and selecting Site | Deliver Now.

Abort

When collecting by FTP it is possible to Abort a current collection by highlighting the site and selecting Site | Abort. The collection will then be postponed for the interval set in the Global Options, Collect Defer Time.

Closing the Collector

To close the application, use the "File | Exit" menu option. Alternatively, you can right click on the system tray icon and select "Exit".

A confirmation dialog appears before actually closing the Collector.

File Locking Mechanisms

Double-File Locking

Double File Locking should work with all applications. The method used ensures that SECollector will not be writing to a file while it is in use by the application.

- SECollector collects and buffers internally all received data

- If the destination file is not present, then SECollector will join together all buffered files for that destination and write the file.

- If the destination file exists, then SECollector continues to buffer the data internally.

This approach has the following implications:

- The application needs to move/rename/delete the file when it has processed the data. SECollector will then regenerate the file with all received data.

- In the case where the application is polling the file (say once a day), the application will be up to that period behind. This is true especially when the buffers are delivering very frequently – the first collected block of data will recreate the file, and all subsequent data will be buffered in SECollector. Only when the application renames the file (which would have the first collected block) will SECollector then make "visible" the rest of that day's data. Increasing the frequency of polling at the application will help, but it will still be up to the interval behind.

File Access Locking Mode

When the "Double-File Locking" option is unticked, then SECollector uses File Access locking.

Where an application wishes to process data daily, or where the application wants to process data in real time, SECollector allows you to turn off "Double File Locking" and use a file access locking mode.

NOTE: This mode absolutely requires cooperation between SECollector and the application that is processing the data!

In this mode, SECollector will append data to the destination file as it arrives. To do this it obtains an exclusive write lock – which denies any other application from gaining a write lock, but does allow concurrent reads.

Your application should be aware of the following points:

- SECollector always buffers internally first. If the file is arriving over a modem this process can take a while. However, the destination file is not locked during the actual collection process. It is only when the transfer has completed successfully that SECollector will move the data from the buffered file into the destination file. Consequently the locks on the file should be of very short duration.

- The easiest method is for the application to obtain an exclusive read/write lock on the file (it may do this already), and not just a read lock. If the application has an

exclusive read/write lock on the file when data arrives (and SECollector wishes to append to the file), then SECollector will defer the writing and buffer the data internally.

- o As soon as the application released the lock, then SECollector will append new data (or recreate the file if it was deleted).

● Be aware that there is a very, very small possibility that SECollector will append more data between the application releasing the lock and deleting (or renaming) the file (meaning that you could lose data).

- o Consequently, it is safer to rename the file before working on it.

- o However, the rename may fail if SECollector is currently writing to the file. So the application should have logic to do one of the following:

  - ■ Defer the processing for a couple of minutes

  - ■ Wait a second or two and try the rename again. However, the failure could be for other reasons, e.g. security locks applied to the file by a user. It would be prudent to limit the number of retry attempts before raising some kind of alert (so the application doesn't hang waiting for something that will never happen!)

● If the application is designed to read the file while allowing SECollector to concurrently write, then you should be very careful about the loop.

- o Since the file may grow while reading, do not grab the file length at the beginning of the process and only read that amount! You should either read until nothing is read, or keep reassessing the file size through the loop.

- o Again, there is a very slim chance that in between finishing with the read loop and deleting the file that SECollector will have obtained a write lock. In this case, the delete will fail – indicating there is more data to process. This logic should be coded into the exit part of the loop and allow for re-entry into the loop.

Log File Format

SECollector outputs its daily logs in a simple CSV (Comma Separated Value) text file.

Each log file includes a header to aid understanding:

`"Date"`

The PC local date and time in the form "yyyy-mm-dd hh:mm:ss"

`"Name"`

For messages that involve a file as source (for example, when removing a file from the Archive directory because it is too old), this will have the form "`File:filename`".

For message events where data is being collected from a buffer, this field will be the site name.

`"Error"`

If the message is informational then this will be blank, ie. "".

All error messages have the string "`*E`" as the value.

`"Origin"`

Which SECollector module originated the message.

"Q" - the queue output module. This module is responsible for shifting the data from the queue subdirectory out to the destination files.

"F" - the FTP collector module.

"E" - the SMTP email server module.

`"Device/Destination"`

For message events that involve collecting data from a buffer this will have the IP address or name of the device (in the case of an FTP pull), or blank (in the case of email collection).

For message events that involve the Queue module, this is the destination file name.

`"Size"`

If applicable, this field will be an integer value showing the size of the file received, or the size of the file transferred to the destination file.

For error messages this value is "-1"

`"Message"`

A human readable message for the event. e.g. "`Removed from archive`", "`Copied`".