

Kiwi Secure Tunnel

A Freeware Secure Syslog Tunnel for Windows

© 2003 - 2009 SolarWinds, Inc. All rights reserved.

Kiwi Secure Tunnel enables the secure sending of syslog data across the internet.

Kiwi Secure Tunnel is made up of a client and a server. The Tunnel Client gathers messages from one or more devices on a network and forwards the messages across a secure link to the Tunnel Server. The Server then forwards the messages on to one or more Syslog Servers

Table of Contents

Foreword	0
Part I Kiwi Secure Tunnel	3
Part II Introduction	3
1 Welcome to Kiwi Tunnel	3
2 Product Features	5
Part III Getting Started	5
1 Client Setup	5
2 Server Setup	6
Part IV Tunnel Client	7
1 Overview	7
2 Manager	7
Statistics	7
Status	8
Connections	9
Log	10
Menus	11
File	11
View	11
Manage	11
Help	11
Properties	11
3 Service	13
Service	13
4 File Monitoring	14
Overview	14
Ini File	14
Usage	15
Part V Tunnel Server	15
1 Overview	15
2 Manager	16
Statistics	16
Status	17
Connections	18
Log	18
Menus	19
File	19
View	19
Manage	19
Help	20
Properties	20

Clients	21
3 Service	22
Service	22
Part VI Advanced Information	22
1 Registry Settings	22
Client Pacing Interval	22
Server Pacing Interval	23
Index	24

1 Kiwi Secure Tunnel



Kiwi Secure Tunnel

[A Freeware Secure Tunnel Service for the Kiwi Syslog Server \(or compatible\)](#)

Program copyright 2003 - 2009 SolarWinds, Inc. All rights reserved.

Latest version available from: www.kiwisyslog.com

Online support available from: www.kiwisyslog.com/support

Kiwi Secure Tunnel receives, compresses, and securely transports, syslog messages from distributed network devices to the Kiwi Syslog Server (or compatible).

Kiwi Secure Tunnel is provided only as a Service Edition for Windows 2000 and above.

The Service Edition runs as an automatic Windows service. It does not require a user to be logged on to operate.

The Kiwi Secure Tunnel Manager program provides the interface to configure and manage the Windows service.

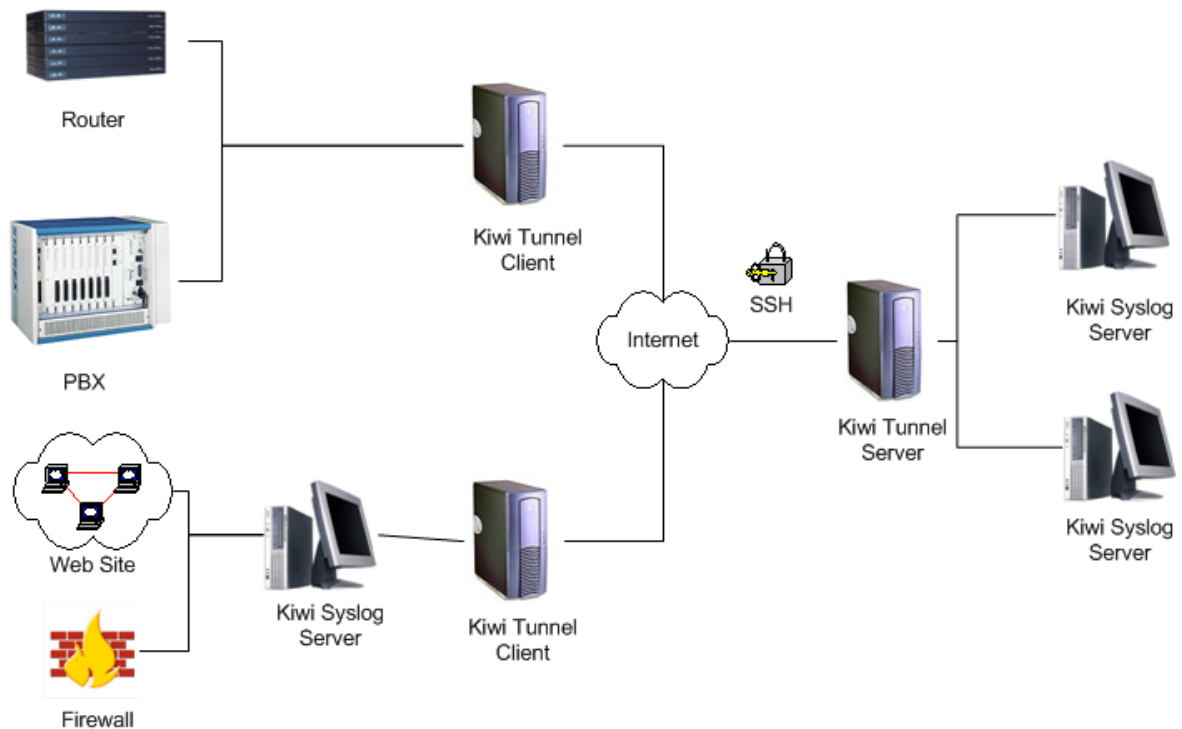
2 Introduction

2.1 Welcome to Kiwi Tunnel

Kiwi Tunnel enables the secure sending of syslog data across the internet or unreliable or untrusted networks.

Kiwi Tunnel is made up of a client and a server. The Tunnel Client gathers messages from one or more devices on a network and forwards the messages across a secure link to the Tunnel Server. The Server then forwards the messages on to one or more Syslog Servers.

Both the Client and the Server have a small footprint and are easily and quickly configured.



Overview

The purpose of the Kiwi Secure Tunnel is to gather data from multiple devices and files on a network and send the data securely from a single point (the Tunnel Client) across a public network like the internet, to a Tunnel Server. The Tunnel Server in turn forwards the data on to a Syslog Server for processing.

The Tunnel Server may act as a collection point for multiple Tunnel Clients, allowing it to act like a data funnel.

Imagine a corporate network spread across 3 physically separate sites, all linked via the internet. Sites A, B, and C are all in different locations of the city, joined by a broadband IP link. However, the network is administered from site C. Sites A and B need to send their syslog data to site C in a timely manner, but as the data is in plain text and may describe the nodes of the network, sending it across the internet is a high security risk. The Kiwi Secure Tunnel provides a secure and simple facility to do just that.

Tunnel Clients would be set up on sites A and B and would connect to a Tunnel Server at site C. This Tunnel Server would forward the data on to a Kiwi Syslog Server running in network C, which would already be receiving data from network devices on network C. This allows the whole corporate network to be securely monitored from a single physical point.

Another scenario could involve a network administration services company, remotely managing the networks for companies A, B, and C. The network company would run a Tunnel Server on their network, and run Tunnel Clients at each of their client sites. The syslog data from each company can then be collected securely from each client site to a single point. However, there might be separate administrators assigned to monitor each

client company. The Kiwi Secure Tunnel Server would then send a parallel data stream to each administrator's computer running Kiwi Syslog Server. Each Kiwi Syslog can filter the incoming data so that only the records from their client site are logged on their machine.

Most network devices send syslog messages via the UDP protocol. This protocol is very unreliable when sent across the internet or slow WAN links. Kiwi Secure Tunnel can take these UDP syslog messages and transport them over a reliable and secure SSH layer across the internet.

2.2 Product Features

Kiwi Secure Tunnel includes the following features:

Client Features

- Accepts UDP syslog messages from any number of network devices
- Accepts TCP syslog messages from up to 50 network devices at once
- Listens on up to 10 different UDP ports
- Listens on up to 10 different TCP ports
- Supports standard SSH type data compression across the secure link
- Supports a number of different encryptions across the secure link (AES, 3DES, DES, Blowfish)
- Supports buffering of messages for performance via a memory buffer
- Supports data caching to disk if the input traffic rate exceeds the specified output rate, or if the tunnel link goes down
- A unique identifier string can be added to each message
- Can monitor multiple text based log files and forward their contents as syslog messages
- Can send a keep alive message at a specified interval to help mark a syslog data file

Server Features

- Send UDP syslog messages to as many as 10 destinations
- Send TCP syslog messages to as many as 10 destinations
- Accepts up to 50 client connections at once
- Supports buffering of messages for performance via a memory buffer
- Supports data caching to disk if the tunnel input traffic rate exceeds the specified output rate, or if the output link goes down
- Can monitor clients for disconnection and send an alert message to the Syslog Server

3 Getting Started

3.1 Client Setup

Perform the following steps to get the Tunnel Client set up for the first time after installation. If you chose to install and start the service during the installation, you should not have to perform steps 6 or 7.

1. Run the Manager
2. Select Manage / Properties menu item
3. Set the Target Properties for the Tunnel Server you are going to connect to.
Fill in a Target Host Address
Fill in a Client Login name
Fill in a Client Password
The standard Port for the Tunnel Server is 22
Choose an encryption method
4. Add an Incoming Port
Click the Add button to add a new incoming port
Leave the default parameters for now - UDP on port 514
Leave the Client Properties at the defaults for now
5. Click the Ok button to save the settings
6. Select Manage / Service Install menu item
You should receive a message indicating the install was successful
7. Select Manage / Service Start menu item
The Service should start running
8. Check the various panels of the Manager to ensure they reflect your settings and that no errors have occurred.

You can now set up the Tunnel Server.

3.2 Server Setup

Perform the following steps to get the Tunnel Server set up for the first time after installation. If you chose to install and start the service during the installation, you should not have to perform steps 7 or 8.

1. Run the Manager
2. Select Manage / Properties menu item
3. Set the Service Properties for the Tunnel Server Service
They should match your Target Properties setup for the Tunnel Client
The standard Port for the Tunnel Server is 22
Leave the other Service Properties for now
4. Add an Outgoing Port
Click the Add button to add a new outgoing port
Set the parameters to point to a Kiwi Syslog you want to send the data to
5. Click the Ok button to save the settings
6. Select Manage / Clients menu item

Add a Login and Password for an incoming client connection. These should match what was set for the Tunnel Client that is to connect with this Tunnel Server.

Click the Ok button to save the settings

7. Select Manage / Service Install menu item
You should receive a message indicating the install was successful
8. Select Manage / Service Start menu item
The Service should start running
9. Check the various panels of the Manager to ensure they reflect your settings and that no errors have occurred

If the Tunnel Client has been set up and run previously, there should now be a connection with the Tunnel Server.

4 Tunnel Client

4.1 Overview

The Tunnel Client is designed to be the focal point for Syslog data from any number of devices. It is designed to concentrate the data being sent to it into a single encrypted data stream that is sent to the Tunnel Server.

The Client can accept connections by devices using UDP and TCP protocols. It can listen on up to 10 ports for UDP and 10 ports for TCP. Further, multiple connections are supported on the TCP ports, so that up to 50 simultaneous connections are possible using TCP.

The Tunnel Client is made up of 2 separate components, the Manager and the Service.

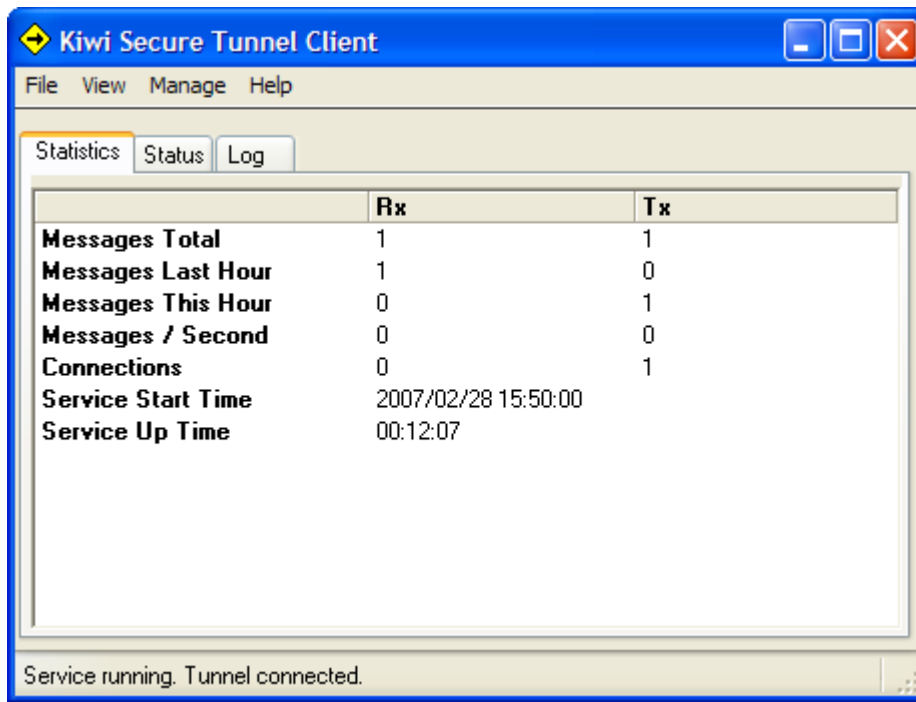
The Manager provides the user interface of the Client. It shows statistics and status. It also allows you to manage the configuration of the Client.

The Service is the data engine of the Tunnel Client. It runs as an operating system service. Once it is installed, it is started automatically by the operating system when the system boots up.

4.2 Manager

4.2.1 Statistics

This is the Manager statistics display.



	Rx	Tx
Messages Total	1	1
Messages Last Hour	1	0
Messages This Hour	0	1
Messages / Second	0	0
Connections	0	1
Service Start Time	2007/02/28 15:50:00	
Service Up Time	00:12:07	

Service running. Tunnel connected.

This shows message and connection statistics for inwards connections, which are all the devices sending messages to the Client, and the outwards connection, which is the Tunnel connection.

The Total Messages shows the total number of messages processed since the Service started.

The Messages Last hour shows the number of messages processed in the preceding hour.

The Messages This hour shows the total messages processed during the current hour.

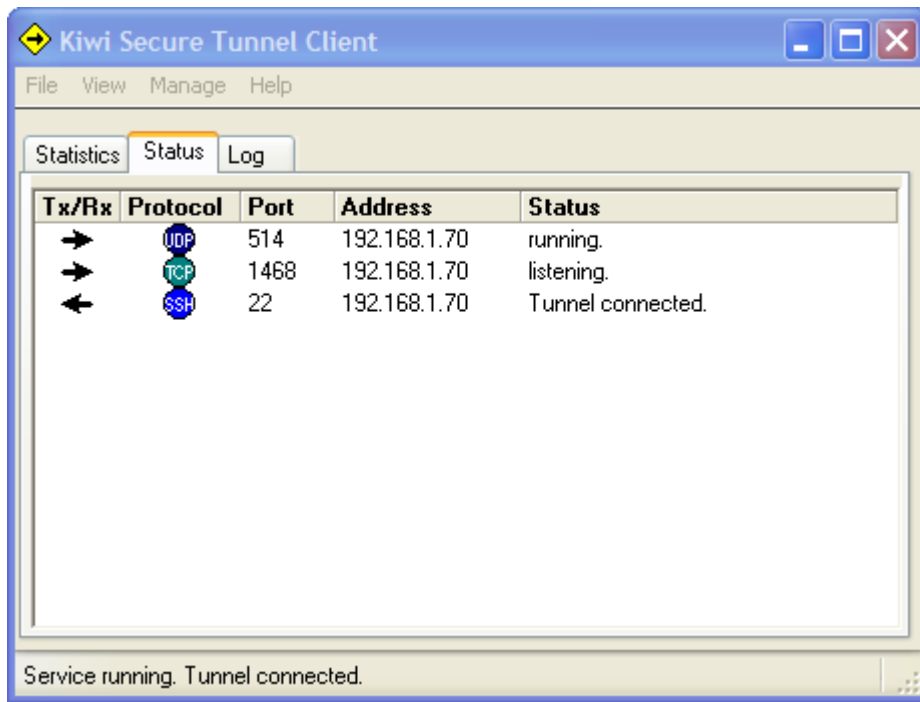
The Messages per Second shows a dynamic rate of messages processed based on the messages processed during the last statistics sampling interval.

The Connections show the number of active connections, including all individual TCP connections.

The times are self explanatory.

4.2.2 Status

This is the Status display.



This shows the status and details of the connections.

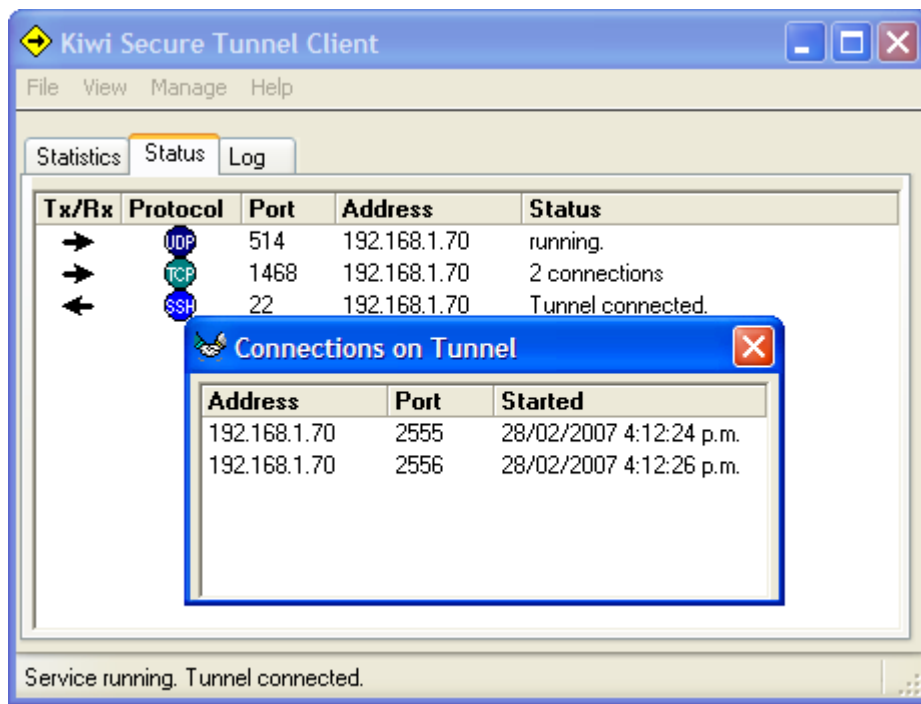
In this example it shows a UDP port defined on port 514, a TCP port on port 1468, and the Tunnel connected on port 22.

The address column for TCP and UDP shows the IP address of the Network Interface Card (NIC) bound to the ports used.

The address of the Tunnel is the IP address of the system the Kiwi Tunnel Server is running on.

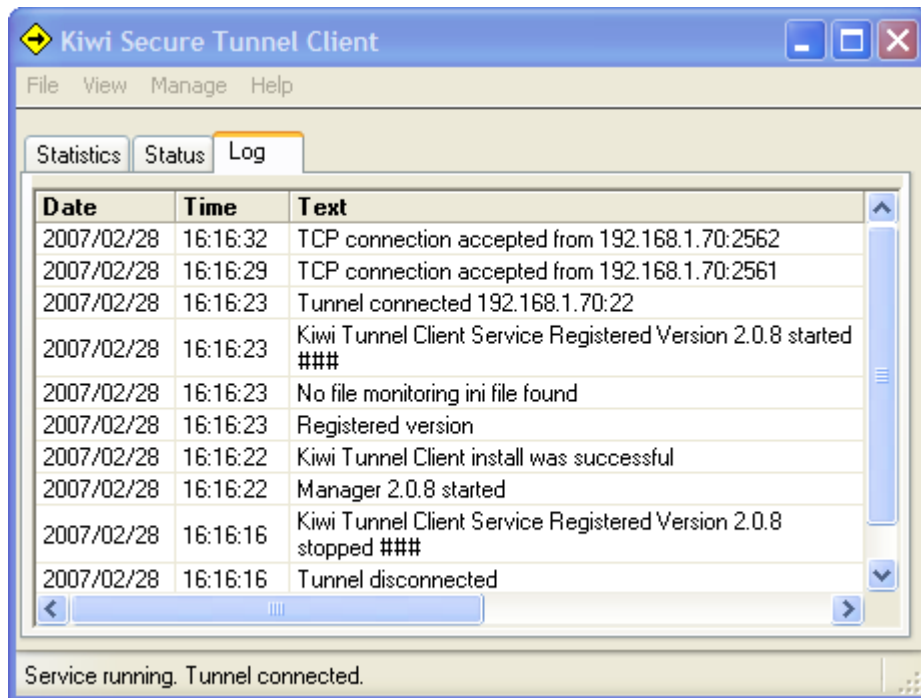
4.2.2.1 Connections

Double clicking on a TCP port entry that is showing one or more connections brings up a detail window that lists the individual connections on that port.



4.2.3 Log

The Log tab shows the latest messages from the Service log file.



4.2.4 Menus

4.2.4.1 File

The File menu:

- Allows you to export the settings to an ini file ***
- Allows you to purge the log file
- Has an Exit item to close the Manager

***** This option is used for SolarWinds support purposes only**

4.2.4.2 View

The View menu:

- Lets you view the log file created by the Service

4.2.4.3 Manage

You manage the Service configuration and its state from the Manage menu. You can:

- Set all the Service properties from the properties screen
- Start and stop the Service
- Install and uninstall the Service from this menu. This registers the Service with the operating system service manager, or unregisters it as the case may be.

The Service must be installed before it can be started. Once installed, it will be started automatically every time the operating system starts up.

4.2.4.4 Help

The Help menu item:

- Allows you to view the Kiwi Secure Tunnel help
- Allows you to view the About form showing general version information about the Tunnel

4.2.5 Properties

This shows the Service property display.

Tunnel Client Properties

Connection to Tunnel Server

Server Address: localhost Port: 22 Login: KiwiTunnelClient Password: *****

Encryption Method: BlowFish Transmit Pacing: 64Kbps

Incoming Ports

On	Protocol	Port	Bind To Address
<input checked="" type="checkbox"/>	UDP	514	

Add Remove

Misc Options

Use Tunnel Client ID: KiwiTunnelClient Stats Update Interval: 1 second

Client ID Position: Add to end of message Log Service Events

Add original address if missing

Keep Alive Message

Send Message: %ClientID is alive Interval: 10 Minutes

Facility: User Level: Information Priority: 14

OK Cancel

The properties screen configures the Client connection to the Tunnel Server. You need to tell the Client the IP address or known name of the system the Tunnel Server is running on, and on which port. Port 22 is the standard for an SSH server port but may be any port you choose. You should supply a Login and Password that the Tunnel Server can recognise the valid Client by.

The Secure Tunnel link supports a number of different encryption methods, and you may chose a specific one if you wish. Choosing "Any" lets the Tunnel decide the best one to use.

The Tunnel also supports standard SSH style compression. This may help reduce network traffic, especially where the messages being transmitted are very similar.

You can control the rate of data being sent to the Tunnel Server by selecting values from

the Transmit Pacing drop-down list. The selections are in K bits per second. You can use the settings to regulate the flow of syslog data over the network to prevent flooding it if data traffic becomes heavy. The default setting is 64K.

There is a list of all the ports the Client can listen on that devices can connect to. You may add or delete ports at any stage. You may turn a port off or on. Be aware that any change to the port list will interrupt traffic very briefly while the Service reconfigures the ports.

The Client Options box allows you to set a unique Client ID, the interval that the statistics are updated on, and whether you wish standard events to be logged into the log file. Error events are always logged no matter what the setting.

The purpose of the Client ID is to positively identify messages a Secure Tunnel Client is sending in a case where several Clients on different networks are all sending messages that the same Syslog Server collects. The Clients may be on internal networks where the devices sending Syslog messages have the same IP address. The Tunnel Client can add its own unique ID to each message it sends on so that messages can be positively identified as to where they originate. The ID is added to each message either at the front of the message after the priority or at the end, and is in the format "KiwiClientID=" plus the actual Client ID.

The Client ID is also sent to the Tunnel Server when the Client logs onto the Server, and is kept there to help identify Clients when they disconnect. The Client ID may be changed at any time, and any messages sent after changing the Client ID reflect the new ID. However, until the Client logs on to the Server again, the Server does not know that the ID has changed. If the Client disconnects after the ID is changed, the Server may send a disconnection message reflecting the old ID.

You may choose to have the Client add an "OriginalAddress=" tag to the message if one is not present. This adds the IP address of the device sending the message to the Client and enables the Syslog server to derive where the message originated.

In times of high data traffic load, turning the logging off may help the Client cope with a higher flow.

A keep alive message may be sent from the Client at a specific interval that can help mark syslog data files. You can build your own message, add standard variable values to it, and set the priority as you see fit. The priority is set from the Facility and Level drop down lists.

Saving the changes causes the Service to read the configuration data and make any changes specified. It may take a second or so for the Service to do this.

4.3 Service

4.3.1 Service

The Client Service normally has no interaction with the system desktop. It is normally installed to start automatically at system start time.

It can be viewed by the **Administration / Services** facility. It is called Kiwi_Tunnel Client.

4.4 File Monitoring

4.4.1 Overview

The File Monitoring feature of the Tunnel Client allows the Client to monitor the contents of selected files and send data from the files as syslog messages to the Syslog Server using the Secure Tunnel.

Options read by the Client from an ini file control the way the file is monitored, and also allows the source of the data to be identified in a manner compatible with other syslog enabled devices.

The ini file is looked for at Client startup time. If it is not found, no file monitoring is enabled. If it is found, the contents define the files to be monitored. The ini file name is: `KiwiTCFM.ini` and is expected to be found in the same folder as the Client application.

4.4.2 Ini File

A sample ini file is provided with the installation.

```
[Properties]
Tic=300
```

the timer interval in milliseconds for checking the files

```
[File0]
FileName=c:\program files\syslogd\logs\syslogcatchall.txt
```

the name of the file to monitor

```
FileNumber=0
```

internal use only

```
FilePosition=1
```

the current byte position within the file - normally set by the program

```
BigChange=1024
```

where to start monitoring the file if a big change in file size is detected

-1 = start monitoring at the end of the file

0 = start monitoring at the start of the file

>0 = start monitoring this many bytes from the end of the file - default is 1024

```
BigChangeValue=409600
```

the number of bytes the file has grown by that indicates a big change has occurred

```
CurrentSize=0
```

current size n bytes of the file - normally set by the programs

```
MaxBytesPer=30720
```

maximum bytes to send per second

```
StartPosition=0
```

where to start monitoring the file the first time it finds the file

-1 = start monitoring at the end of the file

0 = start monitoring at the start of the file - default value

>0 = start monitoring this many bytes from the end of the file

OriginIP=192.168.1.1

a way of identifying the machine the file resides on - added as Original Address in the message if one does not exist

Facility=16

the facility part of the priority to stamp the messages with

FileDate=15/07/2003 12:41:27

date the file was created - normally set by the program for internal purposes

4.4.3 Usage

To get started with file monitoring, you can set up your own ini file. The only entries required to start with are the Tic entry in the [Properties] section, and the FileName entry in the [File0] section. The file should be set up in the same folder as the Tunnel Client application, `KiwiTCS.exe`. You can also rename the supplied sample ini file and enter the name of the file you wish to monitor.

If the Client successfully finds and reads the ini file, it monitors the files defined in it, using the default values for the other entries if nothing but the file name is set. At shutdown time the Client program writes out the values of all the entries as it knows them.

If the file to be monitored does not exist at the time the Client starts up, it will keep looking for it, so when it is created the Client opens it and starts to monitor it.

The Client keeps track of where it is monitoring in the file, so that when it is restarted it can continue from where it left off. The FilePosition entry holds this location.

If a file being monitored is refreshed or recreated while the Tunnel Client is running, it tries to detect that the file is not what it used to be, and should restart monitoring the file from the position indicated in the StartPosition entry.

If you wish to reset the monitoring position in the file manually, for instance if the file has been refreshed by archiving or similar process, you may set the FilePosition entry to 1 and the Client will monitor the file from the start when it starts up again.

Note that the file monitoring ini file should be changed only while the Tunnel Client Service is not active. The Service continuously refreshes the ini file with the latest settings while it is running, so any changes made manually to the ini file are lost when the ini file is refreshed.

5 Tunnel Server

5.1 Overview

The Tunnel Server is designed to be the secure focal point for Syslog data from any

number of Tunnel Clients. Its purpose is to concentrate the data being sent to it and forward the data stream to one or more Syslog Servers.

The Server can accept multiple connections over the secure Tunnel. It can forward data on up to 10 ports for UDP and 10 ports for TCP.

The Tunnel Server is made up of 2 separate components, the Manager and the Service.

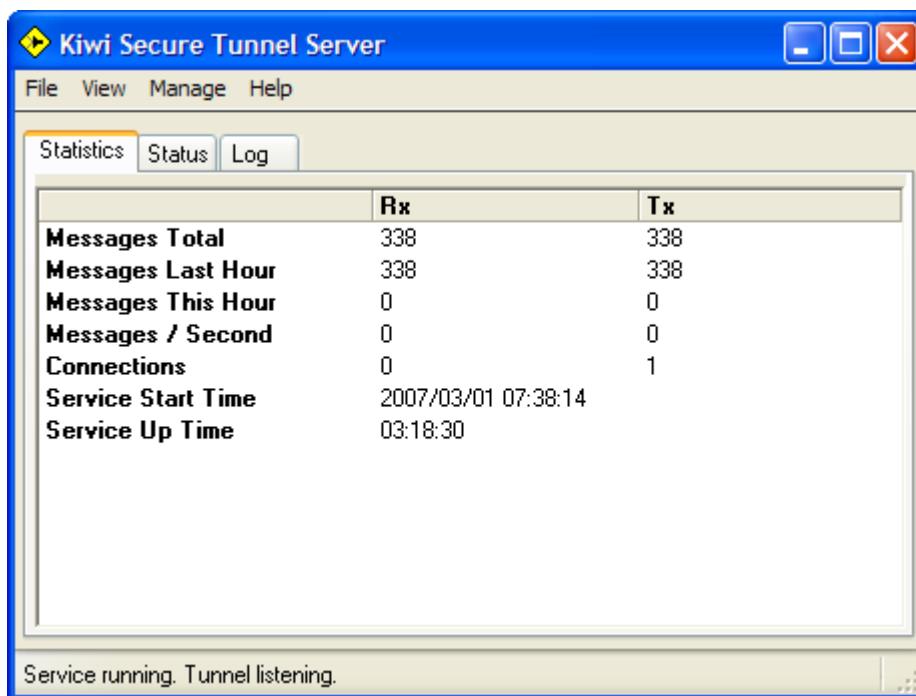
The Manager provides the user interface of the Server. It shows statistics and status. It also allows you to manage the configuration of the Server.

The Service is the data engine of the Tunnel Server. It runs as an operating system service. Once it is installed, it is started automatically by the operating system when the system boots up.

5.2 Manager

5.2.1 Statistics

This is the Manager statistics display.



	Rx	Tx
Messages Total	338	338
Messages Last Hour	338	338
Messages This Hour	0	0
Messages / Second	0	0
Connections	0	1
Service Start Time	2007/03/01 07:38:14	
Service Up Time	03:18:30	

Service running. Tunnel listening.

This shows message and connection statistics for inwards connections, which are across the secure Tunnel, and the outwards connections to Syslog Servers. It shows that the Service has 2 connections from Tunnel Clients and can forward messages to 1 Syslog Server.

The Total Messages shows the total number of messages processed since the Service

started.

The Messages Last hour shows the number of messages processed in the preceding hour.

The Messages This hour shows the total messages processed during the current hour.

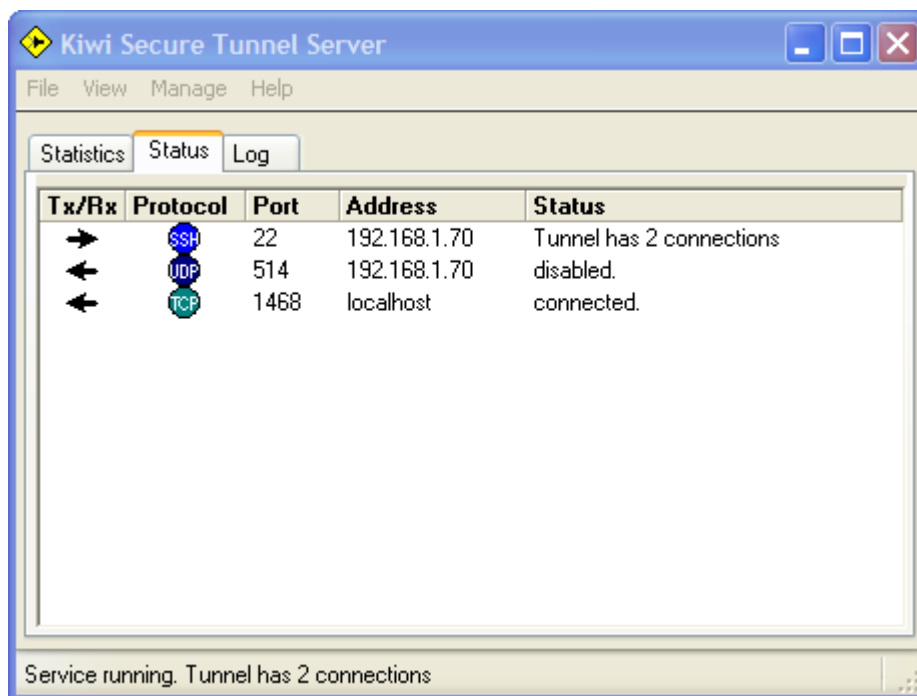
The Messages per Second shows a dynamic rate of messages processed based on the messages processed during the last statistics sampling interval.

The Connections show the number of active connections, including all individual Tunnel connections.

The times are self explanatory.

5.2.2 Status

This is the Status display.



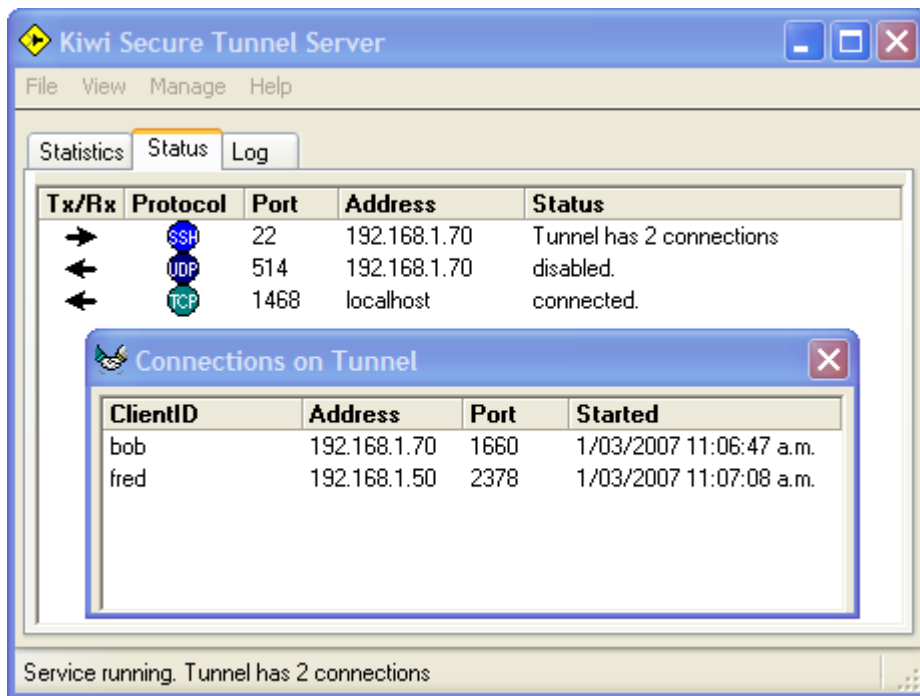
This shows the status and details of the connections.

This shows that the Service has 2 connections from Tunnel Clients and that data can be forwarded to a Syslog Server on TCP port 1468. Another port is defined to send via UDP to port 514 on the local PC but is turned off.

The address column shows the IP address of the machine the Syslog Server is running on.

5.2.2.1 Connections

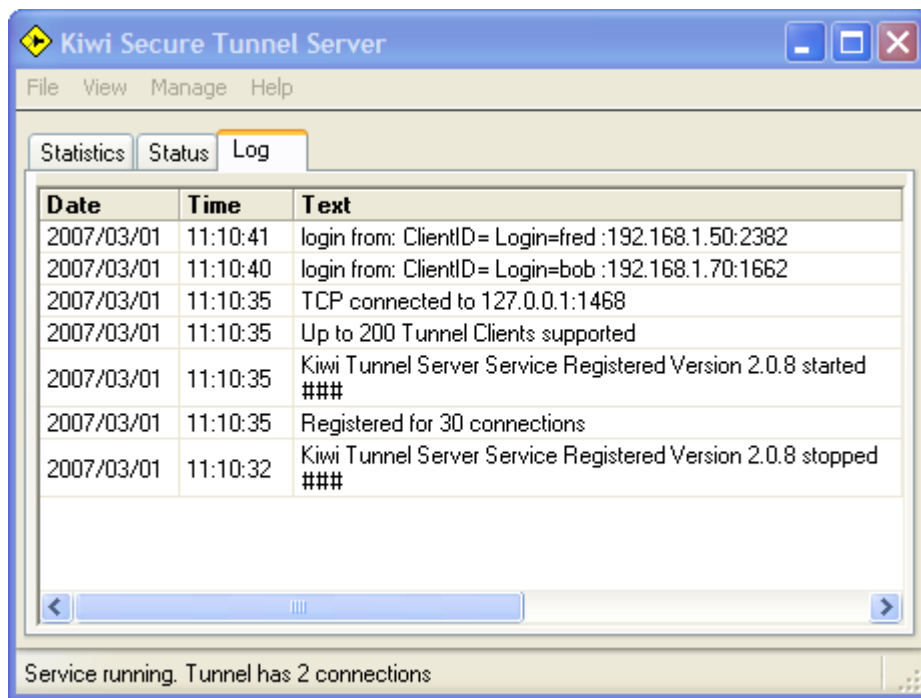
Double clicking on a port entry that is showing one or more connections brings up a detail window that lists the individual connections on that port.



In this case the Tunnel has one connection from a Client whose Login ID is "bob" on a machine with IP address 192.168.1.70 using port 1660, and another from Client "fred" at IP address 192.168.1.50 on port 2378.

5.2.3 Log

The Log tab shows the latest messages from the Service log file.



5.2.4 Menus

5.2.4.1 File

The File menu:

- Allows you to export the settings to an ini file ***
- Allows you to purge the log file
- Has an Exit item to close the Manager

***** This option is used for SolarWinds support purposes only**

5.2.4.2 View

The View menu:

- Lets you view the log file created by the Service

5.2.4.3 Manage

You manage the Service configuration and its state from the Manage menu. You can:

- Set all the Service properties from the properties screen
- Define the IDs of the Clients that are allowed to use the Tunnel
- Start and stop the Service
- Install and uninstall the Service from this menu. This registers the Service with the operating system service manager, or unregisters it as the case may be.

The Service must be installed before it can be started. Once installed, it will be started automatically every time the operating system starts up.

5.2.4.4 Help

The Help menu item:

- Allows you to view the Kiwi Secure Tunnel help
- Allows you to view the About form showing general version information about the Tunnel

5.2.5 Properties

This shows the Service property display.

Tunnel Server Properties

Service Properties

Port: 22 Bind To Address: Transmit Pacing: 1024Kbps

Options

Stats Update Interval: 1 second Log Service Events

Disconnected Message

Send Message: Interval: 10 Minutes

Facility: User Level: Information Priority: 14

Outgoing Ports

On	Target	Protocol	Port	Bind To Address
<input type="checkbox"/>	192.168.1.70	UDP	514	
<input checked="" type="checkbox"/>	localhost	TCP	1468	

Test Add Remove

OK Cancel

The Service properties box allows you to set the port that the Service listens for connections on, and the IP address of the Network Interface Card (NIC) to bind the port to if more than one exists on the PC.

The Options box allows you to set the interval that the statistics are updated on, and

whether you wish standard events to be logged into the log file. Error events are always logged no matter what this setting.

You can control the rate of data being sent on to the Kiwi Syslog Server by selecting values from the Pacing drop-down list. The selections are in K bits per second. You can use the settings to regulate the flow of syslog data over the network to prevent flooding if data traffic becomes heavy. The default setting is 64K.

In times of high input data traffic load, turning the logging off may help the Server cope with a higher loading.

A Client disconnection alert message may be sent from the server at a specific interval that can help mark syslog data files. You can build your own message, add standard variable values to it, and set the priority as you see fit. The priority is set from the Facility and Level drop down lists.

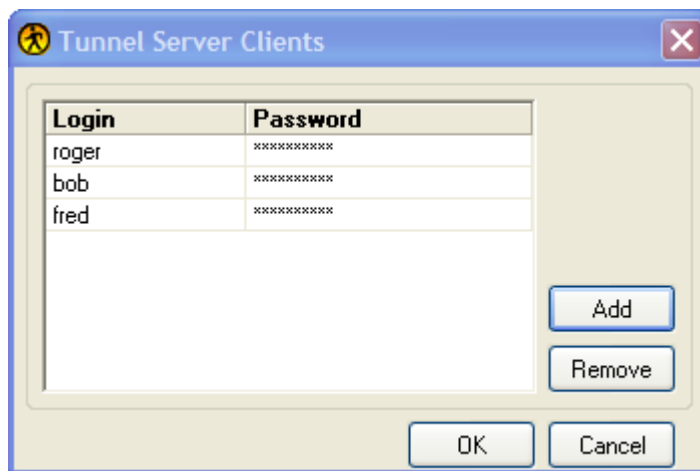
The Outgoing Ports list is a list of the network addresses of all the target Syslog Servers that the Server can forward data to. You may add or delete ports at any stage. You may turn a port off or on. Be aware that any change to the port list will interrupt traffic very briefly while the Service reconfigures the ports.

The Test button tells the Manager to send a test message to the currently selected entry in the list. If more than 1 entry is selected, only the first one is used. If the port is UDP, the message is sent to the target address. If the port is TCP, the Manager attempts to connect to the target before sending the message. If it cannot connect to the target within 10 seconds, it abandons the test.

Saving the changes causes the Service to read the configuration data and make any changes specified. It may take a second or so for the Service to do this.

5.2.6 Clients

Client identities must be set for each Tunnel Client that you want to be able to connect to the Tunnel Server.



You should set a Login ID and Password for each client.

These may be changed at any time and are in effect as soon as they are saved.

5.3 Service

5.3.1 Service

The Server Service normally has no interaction with the system desktop. It is normally installed to start automatically at system start time.

It can be viewed by the **Administration / Services** facility. It is called Kiwi_Tunnel Server.

6 Advanced Information

6.1 Registry Settings

The following registry values will affect the operation of Kiwi Secure Tunnel.

Ensure that Kiwi Secure Tunnel is not running before making changes to the registry.

Use RegEdit to access and modify the values. If a string value is not present then you will need to create it as Kiwi Secure Tunnel will use the defaults if no registry value is found.

Once changes have been made, Kiwi Secure Tunnel can be restarted and will read the new settings.

6.1.1 Client Pacing Interval

Adding the following key to the registry allows you to specify how often the timer controlling the pacing is fired.

Whenever this timer fires the Kiwi Tunnel Client will send up to the amount of data specified in the 'Transmit Pacing' section of the Tunnel Client Properties form.

Key Name: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Kiwi_TunnelClient

Name: Client Pacing Interval

Type: DWORD Value

Min value: 0x00000064 (100 milliseconds)

Max value: 0x00002710 (10 seconds)

If this key does not exist then the Kiwi Secure Tunnel Client will use the default value as it's pacing interval

Default value: 0x000000C8 (200 milliseconds)

6.1.2 Server Pacing Interval

Adding the following key to the registry allows you to specify how often the timer controlling the pacing is fired.

Whenever this timer fires the Kiwi Tunnel Server will send up to the amount of data specified in the 'Transmit Pacing' section of the Tunnel Server Properties form.

Key Name: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Kiwi_TunnelServer

Name: Server Pacing Interval

Type: DWORD Value

Min value: 0x00000064 (100 milliseconds)

Max value: 0x00002710 (10 seconds)

If this key does not exist then the Kiwi Secure Tunnel Server will use the default value as it's pacing interval

Default value: 0x000000C8 (200 milliseconds)

Index

- C -

Client Setup 5
Clients 21
Connections 9, 18

- F -

File 11, 19

- H -

Help 11, 20

- K -

Kiwi Secure Tunnel 3

- M -

Manage 11, 19

- P -

Product Features 5
Properties 11, 20

- S -

Server Setup 6
Service 13, 22
Statistics 7, 16
Status 8, 17

- T -

Tunnel Client Overview 7
Tunnel Server Overview 15
Tunnel Server Service 22

- V -

View 11, 19

- W -

Welcome to Kiwi Tunnel 3