Firmware Release Notes for the NetPilot and SohoBlue Product Range

Document version: 6.1.16 v2

Date: 22nd Apr 2014

This document applies to the following models:-

- NetPilot Guardsman S2025
- NetPilot Vanguard S2100
- NetPilot Vanguard R2100
- NetPilot Globemaster R2250
- NetPilot Globemaster R2500
- NetPilot Globemaster R21000
- SohoBlue
- SohoBlue 25
- SohoBlue 50
- SohoBlue 100

NetPilot Internet Security Ltd., Wellington Gallery, Tunbridge Road, Chew Magna, Bristol, BS40 8SP.
Website: http://www.netpilot.com Email: info@netpilot.com Tel: 01275 333608

v6.1.16

Release dates: 22nd Apr 2014 (upgrade)

23rd Jan 2014 (manufacturing)

New features in this release

1. WiFi

Added support for 802.11b/g/n wireless network interface in supported hardware models.

Enhancements in this release

1. Web virus scanning

Compatibility with iPlayer live radio streams and CCTV video streams.

v6.1.15

Released 4th Dec 2013.

Enhancements in this release

1. Microsoft Windows Activation

Compatibility with the latest Microsoft activation servers, so that Microsoft products can be successfully activated when proxy authentication is enabled.

2. Web Virus Scanning

Stale web virus scanning temporary files are periodically deleted to reclaim disc space.

Bugs fixed in this release

- Fix for virus scanning updates intermittently not being reloaded.
- Fix for PPPoE default route issue.

v6.1.14

Released 29th Nov 2013.

Enhancements in this release

1. New hardware support

Hardware support for SohoBlue 25 v2 and external USB-ethernet adapter.

2. Virus scanning engine

The virus engine has been further optimised for robustness and scalability. The number of threads is automatically scaled depending on the hardware model, to optimise performance.

3. Web proxy

Web proxy performance has been tuned on all hardware models.

Responsiveness of Youtube and Google Video streaming sites is improved.

The layout and content of the progress page for large downloads has been enhanced.

4. DNS nameserver

The built-in nameserver now responds to the product name, i.e. netpilot or sohoblue, even if the hostname has been modified from the default. The product name resolves to the LAN1 IP address. This allows you in most common configurations to connect to the admin interface from the LAN by typing “netpilot” or “sohoblue” even if you aren't sure what the hostname or IP address are set to.

5. IPsec

The formatting of the IPsec “recommended settings for a 3rd party device” screen has been improved.

The wording on the static routes screen for IPsec Advanced profiles has been improved to clarify the distinction between source and destination addresses.

6. Enhanced security in the default Trusted/Internet firewall settings

Security in the default Trusted/Internet firewall settings has been enhanced. In this version of firmware, filtered HTTP and ICMP are allowed, and all other outbound connections are rejected by default. This applies to new installations only. The firewall settings of upgraded units will remain unchanged, although we recommend that you disable unneeded outgoing services, especially SMTP, to increase security and prevent the spread of malware.

7. Support for custom Web Proxy Auto-Detect configuration

Support has been added for serving a custom PAC file for Web Proxy Auto-Detect. This file should be named wpad.dat and placed at the root of the webadmin share. If present it will be served to clients in place of the built-in file. which configures clients to use the local proxy on port 8000. You can use the following as a template for creating your own wpad.dat file:-

```
function FindProxyForURL(url, host)
{
        return "PROXY 10.0.0.1:8000"
}
```

8. Licensing changes

Web Content Filtering now comes free with a UTM Pack (LN) or UTM Premium Pack (UN), whereas previously Web Content Filtering came free with Smartfilter (NN).

The Advanced Firewall licence (code FN) has been retired, since this feature is now permanently enabled as standard.

9. Technical support access

New support IP address block “NetPilot Support E” has been added.

v6.1.13 (preview release)

Released 13th July 2013.

New features in this release

1. Major improvements to web virus scanning

This release contains a major update to the HTTP virus scanning engine. Multi-threading has been greatly enhanced, leading to greater throughtput when under heavy load. A download progress indicator has been added, which appears automatically when downloading large files, to give the user feedback that their download is progressing, and an estimate of time remaining. In addition, the virus scanning engine has been optimised to reduce the incidence of timeouts and failures when running updater clients such as Windows Update and Anti-Virus updaters.

2. Web filtering by IP address group

A new management screen “Web > Filtering > IP address groups” has been introduced, which allows client IP addresses or address blocks to be mapped directly to NetPilot user groups. This allows web access controls to be applied in scenarios where user authentication is undesirable or impossible, for example “bring your own device” type deployments, and networks containing a mix of operating systems.

3. Web authentication exceptions

While the NetPilot's web proxy has full support for Active Directory integration, NTLM and Basic Authentication, we sometimes find that client support for proxy authentication is missing. To cater for applications which don't support proxy authentication, we have added a new management screen “Web > Filtering > Auth Exceptions”. This management screen allows you to enter a list of web site domains for which the NetPilot will not require proxy authentication. Note: Requests for web sites on this list are treated as anonymous queries, and are filtered via the “Global rules” and “Filters for anonymous user” groups. Sites in the auth exceptions lists are still subject to URL and content filtering.

4. NTLM authentication passthrough

Support has been added for accessing web sites which use the NTLM protocol for authentication and access control. This includes some IIS-based sites.

5. Support for pushing DNS/WINS servers to MobileVPN clients

The 'Advanced' section of the MobileVPN profile page allows up to two DNS and two WINS servers to be entered. These addresses are pushed to the roaming clients, allowing the clients to use hostnames when accessing resources over the VPN. The NetPilot's own LAN1 address can be entered as a DNS server, or alternatively, a server on the LAN can be specified, for

example an Active Directory server. The NetPilot's domain name is pushed to VPN clients as the default DNS suffix for the case where the user enters an unqualified hostname.

Bugs fixed in this release

- Fixed a problem with the CMOS clock drifting out of time and then causing a serious disk error when the system next restarts.
- Reduced the length of time certain hardware models take to initialise network ports during system startup.
- Fixed a mail loop issue which could occur in certain circumstances when auto-reply is enabled. This also fixes the issue of auto-replies being erroneously sent to the administrator.
- The email virus scanning time limit has been increased to allow for complex documents to be scanned and delivered.
- Google Safesearch has been updated to prevent users from bypassing the filter by using HTTPS.

v6.1.12

Released 4th April 2013.

New features in this release

1. MobileVPN default profile

A MobileVPN profile named “Remote Access” has been added to the factory default settings, to further simplify the process of setting up VPN access on mobile devices.

The factory default profile applies to new installations only. On upgraded units, MobileVPN can be configured by following the instructions in the MobileVPN Quick Start Guide.

v6.1.11 (preview release)

Released 20th Mar 2013.

New features in this release

1. MobileVPN – VPN connectivity for iPhone/iPad/Android and PCs

MobileVPN provides VPN connectivity for iPhone/iPad/Android devices as well as simplified VPN deployment on Windows XP/Vista/7/8. See the MobileVPN Quick Start Guide for further information.

v6.1.10

Released 28th Nov 2012.

New features in this release

1. Ethernet speed/duplex configuration on PPPoE profiles

Allow the manual configuration of ethernet speed and duplex mode in PPPoE profiles.
Please note, this is required only in special circumstances; auto-negotiation is the best option in most cases.

2. Web filtering by IP address

Added support for web filtering by IP address.

To use this feature, create a NetPilot user with the username matching the IP address of the iPad/iPhone/PC device you would like to control. The web access rules applied to this user will apply to the nominated IP address.

To save time when setting up a large number of clients, the NetPilot user accounts can be created in bulk via the CSV user list import facility.

If you wish to avoid creating individual user accounts for a large number of IP addresses, it is possible to configure a set of default filtering rules in the 'Filters for the anonymous user' group which apply to any device which has an unknown IP address. Then create dedicated IP address users (as above) in a separate user group for devices which are to be granted elevated web access rights.

Enhancements in this release

- Compatibility with Trend Micro automatic updates when Active Directory authentication is enabled.

Bugs fixed in this release

- Fix for certain downloads being blocked by the web proxy if web content filtering was enabled and the user group's default setting was 'block all other sites'.
- Fix for ClamAV blocking certain types of genuine attachment as a “PUA”.
- Fix for importing large CSV user list files.

v6.1.9

Released 13th August 2012.

- Fix an issue with the auto-generated SSL certificate which caused it to have an expiry date in the past.

v6.1.8

Released 28th June 2012.

New features in this release

1. Email autoreply

Added support for sending out-of-office autoreplies. This is configured via a new admin screen: Email > To local users > Autoreply.

Bugs fixed in this release

- Fix the memory and system load graphs in Health Check > Performance.

v6.1.7

Released 9th June 2012.

Enhancements in this release

- Add support for ethernet speed/duplex setting in DHCP-based network profiles.
- Update the web authentication bypass list for compatibility with Windows updates, Java updates, Adobe updates and Google apps.

Bugs fixed in this release

- Fix for URL filtering test page when Web Content Filtering is enabled.

Miscellaneous changes

- Implement new licence expiry policy - The grace period for licence renewal is now 3 days.

v6.1.6

Released 27th June 2012

Enhancements in this release

- Kernel update to provide support for the latest hardware revisions.
- IPsec update.

v6.1.5

Released 28th March 2012

Bugs fixed in this release

- NIC ordering fix for Globemaster units.

v6.1.4

Released 13th March 2012

Enhancements in this release

- Technical support IP address update.
- NIC driver update.

v6.1.3

Released 25th Nov 2011

Enhancements in this release

1. Asymmetric Routing

Add support for asymmetric routing setups, i.e. network layouts in which the NetPilot does not see all the traffic in both directions but is expected to handle one half of a connection. Previously the NetPilot would log “state_invalid” and drop any packets which were not part of a known connection. The behaviour has been changed so that the NetPilot allows asymmetric traffic, while still logging “state_invalid”. This changes incorporate a previously released firewall update for asymmetric routing [nub 1000096].

2. Web phrase filtering

Phrase filtering now matches on whole words rather than subwords. As an example, it is now possible to block pages containing the word 'sex' without causing 'essex', 'middlesex' etc. to be blocked.

3. Web Proxy

Cache performance tuning for Vanguard and Globemaster models.

v6.1.2

Released 2nd Nov 2011

Enhancements in this release

- Updated NIC drivers for SohoBlue, Guardsman and Vanguard models.

v6.1.1

Released 18th Oct 2011

New features in this release

1. PPP over Ethernet (PPPoE)

PPPoE support is added for compatibility with ISPs which provide a broadband service using this connection method. To use PPPoE, select the PPPoE profile on the LAN2 connector, and edit the profile to enter the username and password supplied by your ISP.

v6.1.0

Released 14th Sept 2011

New features in this release

Web keyword filtering
New feature which provides the facility for blocking web pages if they contain particular words or phrases, configurable by the administrator. The list of phrases is entered under "banned phrases" on the site blacklist pages, e.g. *global forbidden sites*.

Note: This feature is available when a Smartfilter URL filtering licence is installed, and "web content filtering" is activated via the licence screen.

Google/Bing Safesearch Enforcement
New feature which provides safe access to the Google and Bing search engines, by enforcing use of the "safe search" feature of these search engines. This feature is configured within the "urlmanip" section of the site greylist pages, eg. *Global manipulated sites*. When enabled, search queries are manipulated to ensure that a safe search is performed. If you have disabled access to search engines via a blacklist (e.g. *global forbidden sites*), and you wish to allow safe access to Google and Bing, you need to apply the following settings:-

a. Tick the Bing Safesearch / Google Safesearch options on the *global manipulated sites* page.
b. Add the following hosts to the "site list" section of the *global manipulated sites* page:-
*.google.co.uk
*.google.com
*.googleusercontent.com
*.bing.co.uk
*.bing.com
*.bing.net

Note: This feature is available when a Smartfilter URL filtering licence is installed, and "web content filtering" is activated via the licence screen.

IPsec extended configuration options
v6.1.0 adds a new IPsec profile type, "IPsec Advanced", which offers enhanced interoperability with 3rd party VPN devices. IPsec Advanced profiles allow the following Phase 1 and Phase 2 parameters to be configured manually:-

- Hash algorithm
- Encryption algorithm
- Diffie Hellman group
- Key lifetime

In addition, static routes attached to IPsec Advanced profiles accept a source address and mask as well as a destination. Each static route initiates a single IPsec connection. This is in

contrast to a regular IPsec profile which automatically sets up IPsec connections from all local networks.

Ethernet speed and duplex configuration options
In v6.1.0, Ethernet speed and duplex mode can be manually configured. On the *Network Profiles* page, tick “show advanced options” to display and edit the Ethernet speed and duplex settings. The currently negotiated speed and duplex mode for each network interface are displayed on the *interface list* page under the *Network* menu.

New defaults in the Trusted/Internet firewall
The default firewall settings for LAN devices accessing the internet are more permissive than in previous versions of software.
-Outgoing traffic is allowed by default
-Web traffic is transparently proxied and filtered
These settings can be adjusted via the Trusted/Internet firewall.

NTP servers
By, default v6.1.0 uses NTP time servers from pool.ntp.org.

Product Activation
In v6.1.0 and onwards, please note that it is necessary to activate your NetPilot or SohoBlue unit by installing a UTM Pack or Firmware Licence to enable full product functionality.

CIPE end-of-life
CIPE has been removed and is superceded by OpenVPN which provides identical functionality. When restoring a backup containing CIPE profiles it is necessary to manually migrate these VPNs to OpenVPN.

Important note for users of Neoaccel SSL VPN-Plus
Neoaccel SSL VPN-Plus is not included in v6.1.0 software. For users of SSL VPN-Plus, please continue using v6.0.5 / v6.0.x.

v6.0.5

Released 20th April 2011

Bugs fixed in this release

- Fix for issue with default route in the Ethernet Cable/ADSL profile.

v6.0.4

Released 15th April 2011

Where a nub number is given in square brackets, this refers to an update which has previously been released as a standalone nub.

New features in this release

1. Multiple WAN IP addresses

Added support for binding multiple IP addresses to a NIC port. Each external IP address is assigned its own firewall, allowing for independent port forwarding rules to be applied. See the Multiple WAN IP Quick Start Guide for more information.

Enhancements in this release

- Improve compatibility with web sites which use chunked transfer encoding in HTTP/1.0 [also in nub 1000066].

v6.0.3

Released 21st January 2011

Where a nub number is given in square brackets, this refers to an update which has previously been released as a standalone nub.

1) SSL VPN-Plus changes:
    a. Added support for VNC screen resolutions up to 1920x1200. [1000064]
2) Optimize file size of system backup. [1000064]
3) Optimize disk partition sizes on Soho Blue hardware.

v6.0.2

Released 10th January 2011

Where a nub number is given in square brackets, this refers to an update which has previously been released as a standalone nub.

1) Fixed a DNS nameserver reliability issue. (Upgrade to bind-9.6-ESV-R1.) [nub 1000049]
2) Fixed an Active Directory authentication compatibility issue with Windows 2008 Server.
3) Fixed a mail relay vulnerability caused by the lynx user. [nub 1000047]
4) Fixed the network start-up sequence to prevent the names of non-existent network interfaces from being displayed on the VGA console at boot time.
5) Spam Assessment rule updates for mishandling of 201x dates, open-whois.org blackhole list, and FORGED_MUA_OUTLOOK false positives. [nubs 1000026, 1000038, 1000046]
6) Updated the port number (8443) in the Spam reclassify link and the X-Spam-Reclassify header. [nubs 1000035 and 1000037]
7) Future updates now require a Firmware Upgrade Licence or UTM Pack. A message is displayed on the login screen confirming that the unit has a valid licence to receive firmware updates and technical support.
8) Central Management System now allows changes to be made when the original settings differ among a group.
9) Enabled support for NTLMv2 in the web proxy.
10) NeoAccel SSL VPN-Plus updates:-
    a. Added “SSL VPN-Plus” firewall service. This service is automatically updated with the full list of SSL VPN gateway ports configured via the Neoaccel Management Console. Use this service instead of “Secure Web” if you need to use a port other than 443 for SSL VPN-Plus.
    b. Added support for multiple screen resolutions in the RDP thin client. [nub 1000043]
    c. Neoaccel SSL VPN-Plus licence is now included in a System Backup and hence no longer needs to be manually re-applied after a System Restore.
11) Added support for NetPilot Soho Blue hardware.

NetPilot Internet Security

SoHoBlue internet security

v6.0.1

Released 14th Dec 2009

1) NeoAccel Management Console fixes:-
    a. Certificate Revocation List screen fixed.
    b. Logs screen fixed.
    c. Total amount of system RAM is now displayed correctly.
    d. Custom layouts and logos are now backed up and restored.
2) Fixed neoweb error message on shutdown.
3) Restoring a backup from v5.2.0 no longer causes the VPN “Add” button to disappear.
4) The dropped packet count for LAN1 on the Guardsman and Vanguard is fixed.
5) The mail posting server is fixed. [Already fixed by nub 1000017 for v6.0.0.]

v6.0.0

Released 19th Nov 2009

First release for new NetPilot Guardsman, Vanguard and Globemaster hardware models.

New features in this release

- SSL VPN-Plus powered by NeoAccel