Untangle Instruction Manual

Untangle NG Firewall is a hardware solution for small to medium businesses. The Untangle Device is installed in a network environment between the ISP modem and your internal network and will filter any device connected to the network. It is a subscription-based service, and offers the following solutions as listed by Untangle:

- **Web Filter** – Premium web content filtering. (over 140 Categories based on Zvelo)
- **HTTPS Inspector** – Decrypt HTTPS to allow other apps to process the datastream.
- **Live Support** – For easy resolution of any technical issues. Includes Configuration Backup!
- **Policy Manager** – Create web usage restrictions, such as teacher vs student.
- **Branding Manager** – Customize “block” screens with your own messages and logo.
- **WAN Failover** – Keep yourself online with multiple ISP”s.
- **WAN Balancer** – Leverage multiple ISP”s for better bandwidth utilization.
- **IPsec VPN** – Securely connect your network to others.
- **Application Control** – Control any application or protocol with a checkbox or use the Integrated Rules Engine to leverage other Untangle apps for complex rules.
- **Web Cache** – Save time and money by caching frequently accessed items.
- **Bandwidth Control** – Prioritize traffic as you see fit.
- **Virus Blocker** – Prevent infections from reaching your network.
- **Spam Blocker** – Stop spam before it hits your mail server.
- **Directory Connector** – Enforce restrictions and view reports by Active Directory user name.
- **Phish Blocker**
- **Intrusion Prevention**
- **Firewall**
- **OpenVPN**
- **Reports**
Note: After testing, Untangle has been approved as an acceptable category-based content filter if configured to meet the requirements set forth in the Weaverland Conference Electronic Technology Usage Guidelines. Please remember that no filter can be guaranteed to filter out all objectionable content; therefore the Weatec Accountability Software must be installed on all devices in order to be in compliance with Weaverland Conference guidelines. The accountability software logs all web traffic, thus fostering brotherhood accountability. So even if objectionable content is missed by Untangle, the content will still trigger a flag on the accountability server. Use the following configuration as a minimum; there is nothing preventing you from choosing stricter settings.

As of June 2015, the annual price for the Complete Package (covering up to 10 devices) costs $540.00. Find more information at https://www.untangle.com/shop/NG-Firewall-Complete.

How to Acquire

1. Go to www.untangle.com/partners/find-a-partner for a list of partners in your area.

The following documentation will guide you through the configuration process. We recommend that the Untangle configuration is performed by someone who is familiar with Networking/Network Security to ensure proper setup and accessibility. Prior installation of the Untangle Device on the network should have been done already by your company’s technician. This document only covers the Web Filter section of the Untangle Device. (the following configuration was Untangle Version 11.0.0) A sample image of network structure including the Untangle Device is shown below.

**Router Mode**
Untangle serves as the router and the firewall
1. Open your web browser and enter the Untangle Device’s IP address to get started. This should take you to the Untangle Administrator Login Page (see image at right). Enter your Username and Password as previously setup during the installation process.

1. You will be directed to the Untangle Home Page.

3. Web Filter – click on the Settings button below the Web Filter Icon. The Block Categories tab will open. You will see the option to Block or Flag each category. We will only be using the Block option because the Flag option is only for reports and logging purposes (if setup) within Untangle.

The Untangle Categories are listed below.

The “Non-Acceptable Use Categories” are listed in Red and must be checked to block.
The “Limited Use Categories” are listed in Amber and should be checked to block.
The “Acceptable Use Categories” are listed in Green and can be blocked/unblocked according to the needs of Users.
Philanthropic Organizations
Phishing/Fraud
Photo Sharing
Physical Security
Pornography
Portal Sites
Piracy & Copyright Theft
Private IP Addresses
Product Reviews & Price Comparisons
Profanity
Professional Networking
Real Estate
Redirect
Remote Access
Reference & Research
Reference Materials & Maps
Religions
Retirement Homes & Assisted Living
R-Rated
School Cheating
Search Engines
Self-Help & Addiction
Sex & Erotic
Sex Education & Pregnancy
Shipping & Logistics
Social and Affiliation Organizations
Social Networking
Software, Hardware & Electronics
Spam
Sport Fighting
Sport Hunting
Sports
Spyware & Questionable Software
Streaming & Downloadable Audio
Streaming & Downloadable Video
Supplements & Compounds
Swimsuits
Technology (General)
Television & Movies
Text Messaging & SMS
Tobacco
Torrent Repository
Toys
Translator
Travel
Unreachable
Violence
Weapons
Web Hosting, ISP & Telco
Web-based Email
Web-based Greeting Cards
Wikis

(If you find that blocking categories under Limited Use causes websites to be blocked that are needed by your business you may need to change these settings. Another option would be to list specific sites under the Pass Sites Tab in the Web Filter Menu)

4. After checking the appropriate categories to block click Apply in the lower right hand corner and click OK to return to the main menu.
5. When a website is blocked you will see a page similar to the one shown here. You do have the option to Unblock for Now or Unblock Permanently. These options are only accessible with the administrator password.

Your Untangle Configuration is now complete.

How to Get Help

1. Contact the WeaTec Helpdesk:
   Phone: (717) 723-8978
   Email: helpdesk@weatec.com

2. You can find additional support articles for Untangle at https://support.untangle.com/hc/en-us.