Untangle Administrator's Guide

By

Blitz Networking Systems
# Table of Contents

## Contents

Getting Started with Untangle .................................................................................................................. 4

Supported Configurations .......................................................................................................................... 5

- Untangle Server as a Router and Firewall .............................................................................................. 5
- Untangle Server as a Bridge .................................................................................................................... 6

The Basics .................................................................................................................................................. 8

- Logging On To Untangle Server ........................................................................................................... 8
- Restarting Untangle Server .................................................................................................................... 9
- To power off the Untangle Server ........................................................................................................ 9
- Resetting Untangle Server To Factory Defaults .................................................................................. 9

Applications ............................................................................................................................................... 12

- Filter Applications ................................................................................................................................. 12
- Spam Blocker ........................................................................................................................................ 13
- Phish Blocker ......................................................................................................................................... 24
- Spyware Blocker .................................................................................................................................... 32
- Web Filter ............................................................................................................................................... 38
- Web Cache ............................................................................................................................................ 44
- Bandwidth Control ................................................................................................................................. 48
- Kaspersky Virus Blocker ....................................................................................................................... 61
- Virus Blocker ......................................................................................................................................... 67
- Intrusion Prevention ............................................................................................................................... 73
- Protocol Control .................................................................................................................................... 77
- Firewall .................................................................................................................................................. 81
- Ad Blocker ............................................................................................................................................ 88

Service Applications .................................................................................................................................. 91

- Commtouch Spam Booster .................................................................................................................... 92
- IPsec VPN .............................................................................................................................................. 94
- Captive Portal ......................................................................................................................................... 99
- WAN Failover ......................................................................................................................................... 107
- WAN Balancer ...................................................................................................................................... 111
- Policy Manager ..................................................................................................................................... 114
- Directory Connector .............................................................................................................................. 124
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Blocker</td>
<td>135</td>
</tr>
<tr>
<td>OpenVPN</td>
<td>138</td>
</tr>
<tr>
<td>Configuration Backup</td>
<td>153</td>
</tr>
<tr>
<td>Report Tool</td>
<td>157</td>
</tr>
<tr>
<td>Setting Up Your Network</td>
<td>165</td>
</tr>
<tr>
<td>Network Configuration Modes</td>
<td>168</td>
</tr>
<tr>
<td>Networking Basics</td>
<td>170</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>172</td>
</tr>
<tr>
<td>Port Forwards</td>
<td>181</td>
</tr>
<tr>
<td>External Aliases</td>
<td>185</td>
</tr>
<tr>
<td>Configuring Untangle Server To Use Dynamic DNS</td>
<td>187</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>189</td>
</tr>
<tr>
<td>DNS Server</td>
<td>191</td>
</tr>
<tr>
<td>QoS Configuration</td>
<td>193</td>
</tr>
<tr>
<td>Multi-WAN</td>
<td>201</td>
</tr>
<tr>
<td>Packet Filter</td>
<td>205</td>
</tr>
<tr>
<td>Bypass Rules</td>
<td>207</td>
</tr>
<tr>
<td>Route Management</td>
<td>209</td>
</tr>
<tr>
<td>Static ARP Management</td>
<td>210</td>
</tr>
<tr>
<td>Admin Accounts</td>
<td>213</td>
</tr>
<tr>
<td>Public Address</td>
<td>216</td>
</tr>
<tr>
<td>Certificates</td>
<td>217</td>
</tr>
<tr>
<td>Configuring Monitoring</td>
<td>222</td>
</tr>
<tr>
<td>Email Settings</td>
<td>226</td>
</tr>
<tr>
<td>Quarantine Configuration</td>
<td>230</td>
</tr>
<tr>
<td>Local Directory</td>
<td>235</td>
</tr>
<tr>
<td>Support</td>
<td>237</td>
</tr>
<tr>
<td>Backups and Restores</td>
<td>239</td>
</tr>
<tr>
<td>Protocol Settings</td>
<td>241</td>
</tr>
<tr>
<td>Regional Settings</td>
<td>242</td>
</tr>
</tbody>
</table>
Getting Started with Untangle

The following links contain a wealth of information on how Untangle works, including racks, applications and policies. If you're new to Untangle, we highly recommend reading these pages to familiarize yourself with the platform:

**An Introduction to Untangle - the GUI and supported configurations.**

**About Untangle Server’s User Interface**

The Untangle GUI can be broken down into three major components: the Navigation Pane, Racks and Applications. On the left side of the GUI you can see the Navigation Pane, which contains two tabs: **Apps** and **Config**. After Applications have been downloaded from the Untangle Store, they will appear in the **Apps** tab and can be installed into a rack.

The **Config** tab contains administrative settings for the Untangle Server. To the right of the Navigation Pane is a virtual rack. The interface is similar to a physical network rack - a cabinet with a collection of hardware. All Untangle Servers will have a **Default Rack**, and you can create additional virtual racks as needed.

The Applications are divided into two sections:

- **Filter Applications**: All the Applications above the **Services** pane in the interface can have unique configurations, which you can apply to specific virtual racks. Virtual racks enable you to create different policies for different sets of users.

- **Service Applications**: All the Applications below the **Services** pane are services and are "global." Each has a configuration that applies to all virtual racks. As such, if you remove any service from any rack, you will remove that service from all racks.
Supported Configurations

Your Untangle Server will fit into one of three basic network configurations:

- Untangle Server as a Router and Firewall
- Untangle Server as a Bridge

Untangle Server as a Router and Firewall

If you do not have an existing router or you want to replace your existing router, use the Untangle Server as a router and firewall.

Basic

Untangle Server as a Router and Firewall
Advanced

Untangle Server as a Bridge

If you already have a router/firewall and want to keep it installed, simply install the Untangle Server between the firewall and the main internal switch. In this scenario, the Untangle Server will function as a bridge. You do not need to change your default route (gateway) on any computers behind the firewall, nor change the routes on your router.

You can also install the Untangle Server as a bridge between the firewall and the Internet device. This configuration is not recommended because Denial-of-Service protection within the Untangle Server (along with Reports) will not be able to differentiate between internal machines behind your firewall.
Basic

Untangle Server as a Bridge

Advanced

Untangle Server as a Bridge
The Basics

Logging On To Untangle Server

Once you set up and configure the Untangle Server using the Installation Wizard, you can administer the Untangle Server from the Untangle Client. You can log on to the Untangle Server using one of two methods:

- Connect directly using a monitor, keyboard, and mouse.
- Connect remotely using a browser.

To launch the Untangle Client when directly attached:

*Before You Begin:* Ensure that the Untangle Server is turned on.

1. Connect a monitor, keyboard, and mouse to the Untangle Server. Your monitor displays the Untangle logo and navigation bar.
2. In the Navigation bar, click the Untangle Client button. The Untangle Client will launch.
3. Type your username and password, and click the Login button.

To launch the Untangle Client from a browser:

Unless you have remote access enabled, you cannot log on from outside the protected network. You must first log on from within the protected network, then enable remote access.

*Before You Begin:* Ensure that the Untangle Server is turned on.

1. Do one of the following:
   - *(Remote Logon)* In your browser, type https:// followed by the External IP address of the Untangle Server, port number (default is 443). For example: https://72.14.207.1:443.
   - *(Local Logon)* In your browser, type http://localhost/webui or type http:// followed by the Internal IP address of your Untangle Server. For example: http://198.168.1.1

*Note:* You might receive a warning from your web browser regarding certificates.

2. If you receive a warning, dismiss it as you are safe connecting to the Untangle Server.
3. When prompted, provide a username and password to log on. The Untangle Client will launch.
Next Step: If you want to enable remote access so that you can log on to Untangle Server from outside the protected network, go to Enabling Remote Access to Untangle Server.

Restarting Untangle Server

You can restart or reboot the Untangle Server without physical access to the system.

To reboot the Untangle Server:

1. From the Navigation Pane, click the Config tab > System.
2. On the “Support” tab, Under the Manual Reboot section, click the Reboot button.

Do not use the power button on the front of the Untangle Server or the emergency power switch on the back of the Untangle Server to power off the Untangle Server. These methods do not provide the Untangle Server a graceful shutdown. Instead, use the Untangle Server’s direct-connect interface.

To power off the Untangle Server

1. Connect a monitor, keyboard, and mouse to the Untangle Server. Your monitor displays the Untangle logo and Navigation bar.
2. In the Navigation bar, click the Shutdown button. The Untangle Server shuts down.

You can also shutdown Untangle without physical access to the system:

1. From the Navigation Pane, click the Config tab > System.
2. To Shutdown, click the Shutdown button under the Manual Shutdown section.

Resetting Untangle Server To Factory Defaults

You might want to reset the Untangle Server to factory defaults if you experience problems with your configuration, or if you want to experiment with different configurations. If you forgot your admin password, you can change that password without resetting the Untangle Server to factory defaults. Go to Resetting the Password for Administrator’s Account.

To return to factory defaults:

Warning: This procedure erases all configuration information from the Untangle Server.
Before You Begin: Back up your configuration just in case you'd like to return to this configuration: Backing up Untangle Server's Configuration.

1. Using a keyboard, video and mouse, connect directly to the Untangle Server.
   When connected directly to the Untangle Server, a window with Untangle's logo appears.

2. Click Recover Utilities.

3. Click Yes to continue with the reset. The next screen offers a few options.

4. Select the Return To Factory Defaults menu option.

5. Select Yes to return to factory defaults. When you log on to the Untangle Server, you are prompted to use the Setup Wizard to configure your Untangle Server, just as you did when you installed the Untangle Server the first time using the Untangle Server Quick Start Guide.

Accessing Event Logs

Most Software Products have an Event Log as part of their controls. Event logs present a table of significant events that the Untangle Server observed.

Event logs contain the underlying data from which the Untangle Server generates Untangle Reports. However, there are a few differences. Event logs provide real-time information whereas Untangle Reports provide next-day and weekly information. Moreover, the event logs show activity by IP address; Untangle Reports are more user-friendly because they show activity by user.

- Sometimes the events provide a dialog of which traffic was filtered:
  ... examined this web request from 1.2.3.4 and found no viruses ...

- Other times, the events indicate malicious content which was stopped by the Software Product:
  ... blocked email with subject Urgent Business Request as it was found to be a phishing email ...

To access an Event Log:

1. From the Software Product, click the Show Settings button.

2. Click the Event Log tab.

3. In the drop-down list, select the types of events that you want to view, and click the Refresh button. To view all events, select All Events.
Verifying if a Network Computer is Accessible

Using the ping command, you can determine if a specific system is accessible on the network and what its IP address is, if you only know its hostname.

To verify if a system is accessible on the network:

1. Launch a command prompt: Start > Run.

2. Type either the IP address or the hostname of the system that you want to contact, then Enter.

   > ping <hostname>

   > ping <IPAddress>

   • If you receive a message like the following, the system was accessible:

     PING myhost.dnsdojo.net (198.144.196.51) total tx: 5, total time: 4016.0 ms, percent answered: 20% sequence: 5 ttl: 64, delay: 0.047 ms, size: 45 bytes

   • If you provide an incorrect hostname or the DNS Server does not know that hostname, you receive a Unable to resolve the host message.
Applications

There are two types of Applications:

- **Filter Applications**: All the Applications *above* the Services pane in the interface can have unique configurations, which you can apply to specific virtual racks. Virtual racks enable you to create different policies for different sets of users.

- **Service Applications**: All the Applications *below* the Services pane are services and are "global." Each has a configuration that applies to all virtual racks. As such, if you remove any service from any rack, you will remove that service from all racks.

**Filter Applications**

<table>
<thead>
<tr>
<th>Spam Blocker</th>
<th>Phish Blocker</th>
<th>Spyware Blocker</th>
<th>Web Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Cache</td>
<td>Bandwidth Control</td>
<td>Kaspersky Virus Blocker</td>
<td>Virus Blocker</td>
</tr>
<tr>
<td>Protocol Control</td>
<td>Firewall</td>
<td>Ad Blocker</td>
<td>Intrusion Prevention</td>
</tr>
</tbody>
</table>
Spam Blocker

Spam Blocker is an intelligent email filter that identifies Spam (unsolicited bulk email) even when that spam is sent through an image. Spam Blocker uses an open source solution: SpamAssassin. Spam Blocker can scan any email that is transported by the following protocols: SMTP, POP, or IMAP. Each protocol has a set of controls to customize how Spam Blocker scans, manages, and notifies users of spam.

Settings

This section reviews the different settings and configuration options available for Spam Blocker.

You can quarantine all SMTP email or you can specify that Spam Blocker quarantine spam for specific users. For POP and IMAP email, you do not have quarantine and you cannot block these types of email because you must download the message to access it. You can, however, mark POP and IMAP as spam.

Before You Begin: If you have web mail (POP mail), configure your email program to download that mail automatically so that Spam Blocker can scan that email:

- Download Gmail To Outlook
- Download Gmail To Eudora
- Download Yahoo Mail To Outlook
- Download Hotmail To Outlook

To configure email scanning and quarantine:

1. From Spam Blocker, do one of the following:
   - If you have a local Microsoft Exchange Server, use the SMTP area.
     - The Drop Super Spam option for SMTP will drop spam that matches without processing it.
   - If you use Outlook to download web mail, use the POP3 area.
   - If you use an IMAP email client, use the IMAP area.

2. Specify how you want Untangle Server to behave:

<table>
<thead>
<tr>
<th>Scan SMTP/POP3/IMAP</th>
<th>When the check box is selected, the Untangle Server scans email for spam in both directions unless there is a custom policy that overrides these instructions.</th>
</tr>
</thead>
</table>
**Strength**

This controls the sensitivity of the spam scanner. There are five possible values ranging from extreme to very low as well as a custom score. You may wish to use a custom score if some legitimate emails are being classified as spam. **Note:** The value extreme means most sensitive to spam. Setting the scan strength to extreme will cause the greatest percentage of your mail to be considered spam. For more information, see What should I set for strength?

---

**Action**

This controls what actions Untangle Server should take on the message itself, should the message be determined to be spam:

- **Mark.** Causes the email message to have its subject changed to start with the phrase [Spam]. Users can then set up email client filter rules to cause such messages to be placed in special folders.

- **Pass.** Causes the message to be passed on to the recipient, even though it was detected as spam.

- **Drop.** Applies only to SMTP mail. Causes the message to be dropped, meaning the sender believes it was delivered yet it was never forwarded to the recipient. Although neither sender nor recipient know the message was dropped, it will still be noted in the Event Log.

- **Quarantine.** Applies only to SMTP mail. Causes the message to be quarantined. For more information on the operation of this feature, please refer to About Quarantine. As outlined in Creating Custom Policies, outgoing mail is not quarantined by default. **Note:** You may also set a threshold for **Super Spam** handling. This allows you to discard spam messages above a certain test score which would have otherwise been quarantined instead.

---

3. **Add any advanced configuration options you may wish to use:**

<p>| Add Email Headers | When the check box is selected, the Untangle Server will add information to the header of each email that says whether the email was classified as spam, its score, and the tests used |</p>
<table>
<thead>
<tr>
<th><strong>Message Size Limit</strong></th>
<th>Allows you to change the maximum size of a message that will be scanned for spam. The default maximum size is 262,144 bytes. Spam will typically be much smaller, as spammers rely on the sheer number of messages sent. <strong>This does not control the message size limit of messages passed through untangle.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable tarpitting</strong></td>
<td>Applies only to SMTP mail. If selected, enables the DNSBL feature, which refuses connections from email hosts that are blacklisted.</td>
</tr>
<tr>
<td><strong>Close connection on scan failure</strong></td>
<td>Applies only to SMTP mail. If Spam Blocker fails for any reason, this setting determines whether incoming email is allowed in without being tested, or will be blocked until messages can be tested.</td>
</tr>
<tr>
<td><strong>Scan outbound (WAN) SMTP</strong></td>
<td>Applies only to SMTP mail. This setting determines whether Spam Blocker will test outgoing mail as well as incoming mail.</td>
</tr>
<tr>
<td><strong>CPU Load Limit</strong></td>
<td>Applies only to SMTP mail. If CPU Load (as viewed at the top of your Untangle rack) exceeds this number, incoming connections are stopped until CPU load decreases. The default value is 7.</td>
</tr>
<tr>
<td><strong>Concurrent Scan Limit</strong></td>
<td>Applies only to SMTP mail. This is the maximum number of messages that can be scanned at the same time. The default value is 15.</td>
</tr>
</tbody>
</table>

4. Click the **Save** button.

**Next Step:** To specify who should or should not manage their quarantined email or to specify who should manage distribution lists' quarantined email, go to Specifying Who Manages Quarantined Email.

**Event Log**

Use the following terms and definitions to understand the Spam Blocker Event Log:

<table>
<thead>
<tr>
<th><strong>timestamp</strong></th>
<th>The time the event took place</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>The action taken on the mail.</td>
</tr>
<tr>
<td></td>
<td>• pass message - the message was not determined to be spam and</td>
</tr>
</tbody>
</table>
was passed
- mark message - the message was determined to be spam and marked
- block message - the message was determined to be spam and blocked (silently dropped)
- quarantine message - the message was determined to be spam and quarantined
- pass safelist message - the message was passed because the sender was on the user's or global safe pass-list.
- pass oversize message - the message was passed without being scanned because it was over the spam size limit.
- pass outbound message - the message was passed without being scanned because it was outbound (WAN-bound)

| client | The client IP Address of the protocol client. Recall that for SMTP this is the sender of the mail, and for IMAP/POP the receiver of the mail. |
| subject | The subject of the email. This may be blank if the email had no subject. |
| receiver | The recipient email address of the email. |
| sender | The sender of the email. Note that for spam, this is frequently blank. |
| score | This is the score applied to the email by the spam scanner. Higher values indicate more likely to be spam. |
| server | The server IP Address. Recall that for SMTP this is the machine receiving the email, and for IMAP/POP the machine holding the inbox. |

**Tarpit Event Log**

Use the following terms and definitions to understand Spam Blocker's Tarpit Event Log:

| timestamp | The time the event took place |
| action | The action taken on the mail. |
| sender | The sender of the email. Note that for spam, this is frequently blank. |
| DNSBL | The DNSBL server whose list matched the mail. |
Spam Blocker FAQs

Why doesn't Spam Blocker block all spam?

If you receive some spam in your email inbox, don’t be alarmed. Spam Blocker is working as evidenced by the large amount of spam in the quarantine. There are two main reasons why Spam Blocker might not block all your spam:

- Spam Blocker is a player in an "arms race" against spammers.
- Field testing indicates that our pre-configured Spam Blocker settings, which are conservative in labeling email as spam, are the best fit for most businesses. However, selecting a more aggressive scan strength setting from the drop-down menu in Spam Blocker's GUI is very easy, should you find that your business requires it.

When configuring my Untangle Server to mark spam received over IMAP, the subject of the mails changes to [Spam]... only after I click on the message. Why?

Most IMAP clients first fetch summary information about emails (subject, sender) so the end user can see a preview list of messages. Only when the user selects (clicks on) the message is the actual content of the message retrieved from the server. It is then that the Untangle Server is able to scan the message. Unfortunately, some email clients do not detect the change in subject and update their preview list.

What should I set for strength?

<table>
<thead>
<tr>
<th>Strength</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium (Threshold: 4.3)</td>
<td></td>
</tr>
<tr>
<td>Low (Threshold: 6.0)</td>
<td></td>
</tr>
<tr>
<td>Medium (Threshold: 4.3)</td>
<td></td>
</tr>
<tr>
<td>High (Threshold: 3.5)</td>
<td></td>
</tr>
<tr>
<td>Very High (Threshold: 3.3)</td>
<td></td>
</tr>
<tr>
<td>Extreme (Threshold: 3.0)</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td></td>
</tr>
</tbody>
</table>

Spam Thresholds

Spam Blocker identifies spam based on hundreds of characteristics. An example characteristic is an email greeting that begins with Dear. Another example is an email that is sent with high priority. Spam Blocker does not mark an email as spam simply because an email is sent with high priority. Each characteristic is weighted, producing an overall score. Spam Blocker uses this overall score to determine the probability that
the email is spam. This overall score plus a threshold (scan strength), which you can set, determines if Spam Blocker marks email as spam.

By default, Spam Blocker has a medium threshold. This threshold blocks most spam without interfering with legitimate email. If you increase the threshold above medium, Spam Blocker becomes more strict thereby marking some legitimate email as spam. Untangle recommends medium threshold because Untangle aims to achieve zero false positives; in other words, Untangle does want to mark any email spam if it isn't spam. Most businesses prefer this approach. However, your business might be different.

Spam Blocker provides you the ability to increase the threshold. If you want to catch clever spam that Spam Blocker does not catch when set to medium threshold, and don’t mind sifting through quarantined email to locate and release legitimate email, you can increase your threshold to high. However, keep in mind that Spam Blocker is constantly identifying new characteristics of clever spam, and so Spam Blocker changes its enforcement rules constantly—to keep up with spammers: spam that appears in your email inbox today, might not tomorrow.

To change the threshold, go to Settings.

**What is "custom" strength?**

This allows the user to set exactly the scan strength that is required. The lower the more likely email will be caught in the spam filter. This settings is recommended only for people in special circumstances.

**What is tarpit?**

Tarpit is an option in Spam Blocker. If Tarpit is checked, when an SMTP session is first caught Spam Blocker will check if the client IP is on a DNSBL. If it is it will reject the session, if not, the session will be accepted.

This means that SMTP connections are outright refused from blacklisted servers before they can even send email. This increases the total spam capacity of a given server by quite a bit and also saves bandwidth. However, it may increase false positives as all emails from blacklisted servers are rejected. It will NOT increase spam detection accuracy.

Tarpit events are in the Tarpit Eventlog.

**We receive tons of email. Can I adjust the maximum number of messages to be scanned at once?**

For SMTP, yes. That is available in advanced configuration. The default maximum number of concurrent messages to be tested is 15. Depending on the hardware you
are using, you may be able to adjust that number upwards, but raising it too high could affect your performance overall. If you want to adjust the number, try doing it in small increments, not multiples.

My CPU load is always above 7. I still need to test for spam. What do I do?

Raising the number will allow you to test for spam, but will likely also increase the CPU load. You obviously can’t lower the number and still be able to scan emails. If your CPU load is that high, that’s an indication that your hardware is not robust enough for your site. If your user count increased since you installed your server, or the volume of the internet traffic has increased substantially, this could be a cause. You may also have been spending as little for hardware as you could get away with. Regardless, you probably also are being impacted in other areas without realizing it. You should determine exactly what the hardware specs are on your server to determine whether you should supplement the existing hardware or replace it with something more robust.

Does Spam Blocker’s underlying public rules make it less effective?

No. Actually, the openness makes it more effective whereas security through obscurity is not a effective way to gain security. Spam Blocker’s underlying rules are public. Although it is true that public rules provide smart spammers information to help determine how to evade the rules, smart spammers can, and do, use trial-and-error techniques to figure out the rules — without any public information. Even when smart spammers know the rules, they can’t always evade them. Many spammers don’t read the public rules, and don’t understand them as evidenced by old rules that still catch a lot of spam. By making the rules public, the large community of "good guys" improves the existing rules and produces new, clever rules that spammers can’t evade. Spam Blocker is constantly updating its rules, so don’t disable automatic updates.

Note: If you’re a savvy user, and want to add rules to Spam Blocker’s underlying rules, you can contribute rules.

Emails with larger attachments somehow disappear or are not delivered. Why?

While Untangle is scanning attachments your email server is still waiting for the message, most likely triggering a timeout setting. If you’re using MS Exchange, you’ll want to increase the ConnectionInactivityTimeout setting.

If an unwanted email (spam, phishing, etc) is received for an email address that cannot be quarantined, but my rules are set to quarantine, What happens?

The Quarantinable Addresses rules take precedence over the actions for email rules. In this situation, the email would be marked rather than quarantined.
Why is blocking (or quarantining) of emails not an option for POP or IMAP?

POP and IMAP work differently than SMTP. When POP and IMAP are used, the client requests the mail when the user clicks on the email. At that point the message is downloaded from the server and scanned. Even if the application determines the message is spam, it still must be delivered to the client because the client is waiting and will not be able to read mail unless something is delivered. As a result, only MARK is an option.

Why can’t I block superspam for POP and IMAP emails like I can for SMTP?

For the same reason that you can’t quarantine POP/IMAP spam. The message is not scanned until it is requested by the mail client. At that point, the message (even if it is spam) must be delivered to the client to complete the transaction.

Why does the Event Log report the sender as my bank, yet it was fraudulent? Why does it not report the real sender?

One of the characteristics of phishing emails is that they use deception to change the apparent sender of an email. Although Untangle Server can detect the email as a phishing attempt, there is no way to determine the true sender.

Why is Subject (or sender) blank for some emails in the Event Log?

Not all emails (especially spam emails) have subjects. Some spammers also use tricks to cause there to be no detectable sender.

Why is mail not passing between my Exchange servers?

The Untangle Server forces Extended SMTP (ESMTP) to fall back to SMTP so that the transmitting emails may be scanned. When two Exchange servers are setup such that they require ESMTP communication, all communications will fail. This is enforced by transparent rewriting of the “EHLO” command to “HELO” and appropriate keywords are also stripped.

This can be avoided by adding a special "No Rack" policy or a Bypass rule for communication for these two servers. To add a "Bypass Rule" go into config->networking->advanced->Bypass Rules and create a rule that describe the traffic between your two servers. To add a "No Rack" policy, enter the Policy Manager, Custom Policies and add two policies to be processed by "No Rack", one from server A to server B port 25, and one from server B to server A port 25. The net effect is that any communications between these two servers will be ignored.

Can I forward my email to Untangle and then have Untangle forward the email to my mail server?
No. Untangle is a network gateway and is meant to be installed "in-line" with the traffic. Untangle does not store-and-forward mail. Untangle will transparently scan mail as it passes through it.

**Can I have untangle drop mail that is not to valid users?**

No. Untangle does not have a list of valid emails for your site. It is suggested that you configure your email server to not accept mail for invalid users. This is the default for almost all mail servers except Microsoft Exchange. The links below are instructions on how to configure your email server.

- Exchange 2003
- Exchange 2007

**How do I stop sending Quarantine Daily Digests?**

In Config > Email, you can uncheck the option for Send Daily Quarantine Digest Emails. This will prevent Quarantine Digests from being sent.

**I don't send Daily Digests. How can I keep from running low on disk space?**

This is generally not a problem, but if you have a small disk drive or you receive a huge volume of spam, you may need to shorten the number of days that you retain quarantined email for. This is adjustable in Config > Email.

**I need to keep a Quarantine for everyone, but how do I limit who receives a Quarantine Digest?**

You can decide whose spam can be quarantined, but they will receive a digest if you do that. You cannot turn the digest on or off for specific users once you have decided that they will or will not have a quarantine available.

**How do I resend Quarantine Daily Digests?**

You can resend digests by launching the Untangle Server's Request Quarantine Daily Digest Email window. Go to Resending Quarantined Daily Digests.

**Why are users not receiving a Quarantine Daily Digest?**
• The untangle server may not be configured to send email correctly. Check Config > Email

• Users might not have anything new in the quarantine. A daily digest is sent only if something new is in the quarantine.

• If this is happening for all users, make sure that you have not turned off the option for Quarantine Daily Digest delivery.

What happens to email recipients’ email when those recipients are not on the quarantinable address list?

If you removed the wildcard (*) and created a quarantinable address list, the Spam Blocker passes but marks the email as [Spam]—for those that are not on the list.

Why does my Quarantine have emails for people who don’t work here?

Spammers do not discriminate...they send spams in many ways to get their message into your mailbox. Untangle simply scans email for viruses, phishing attempts and spam. It does not look to see if the message is going to a valid recipient. In Config > Email > Quarantine > Quarantinable Addresses, change the Quarantinable Address from "*" to "@<mycompany>". Change <mycompany> to your company name. Only mail that is coming to your company will now be quarantined. Please note that spams may still come in for illegitimate email addresses that correspond to your domain name.

I have 600 messages in my quarantine. How can I go through them faster?

Look at the bottom of the Quarantine Digest. You can choose how many messages appear per page. You can set the maximum number to 25, 100, 1000 or all messages. That will help you go through them faster, but be warned. Choosing a high number causes a large web page to be loaded. Depending on how much memory your computer has available, that may cause your browser to crash...or worse.

I released an email from my Quarantine Digest. Where did it go?

It is likely that the email was captured again by Spam Blocker. To make sure this doesn’t happen, go to Config > Email > Outgoing Server and note the From Address that is being used by Untangle. Add this address to Config > Email > From-Safe List. This will prevent Untangle from scanning any email being released from Quarantine Digest.

I get two copies of the Quarantine Digest. Why?
You are likely a member of a email distribution list and the quarantine is not configured properly. Let’s use an example. You are a member of a list called sales@xyz.com. The list members are joebob@xyz.com, fredbob@xyz.com and bobbob@xyz.com. They all complain that they get two Quarantine Digests daily.

In the Quarantinable Forwards panel (Config > Email > Quarantine > Quarantinable Forwards), there is nothing listed. That means that each of these people gets a Quarantine Digest for their own email address as well as one for sales@xyz.com. Joe Bob is supposed to manage quarantines for the mailing list, so we should make an entry under distribution list address as sales@xyz.com and its corresponding send to address as joebob@xyz.com. That should take care of the problem. Don’t forget to save your changes.

If there is a mailing list with a large number of members (hugelist@xyz.com) and you wish to have multiple people responsible for checking the quarantines, create a new email distribution list in your mail server (notsohugelist@xyz.com) that contains the email addresses for the people who have this responsibility, then set the Untangle Quarantine Forwards pair to hugelist@xyz.com and notsohugelist@xyz.com. Only those people who have the responsibility will get Quarantine Digests for the mail list.

Why can’t my off-site users get their Quarantine Digests?

The most common reason is that the Quarantine Digest has a URL that has an IP address that is private (on the LAN). They need a URL that is accessible to the public. You can set that up as follows:

1. In Config > Administration > Public Address, define an IP address that is accessible on the outside. Make sure to click the Enabled button.

2. In Config > Administration, make sure that Enable Outside Quarantine Viewing is checked.

3. In Config > Networking > Hostname, determine if you can give a name to the Untangle Server. Enter that if appropriate. If a hostname is defined and it is resolvable on public DNS servers, check the Hostname resolves publicly box. If you wish to use a hostname and one is not available for you, you may wish to use Dynamic DNS to associate a hostname with an IP address. Refer to Configuring Untangle Server To Use Dynamic DNS for more information.
Phish Blocker
Phish Blocker provides pharming protection over the web and protection from phishing over both the web and email. Phish Blocker inspects email for phish, or fraudulent emails. A phishing email attempts to acquire sensitive information such as passwords and credit card details by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email. Phish Blocker scans all SMTP, POP, and IMAP email.

Settings
This section reviews the different settings and configuration options available for Phish Blocker.

Email Settings

Example of Phish Email
1. From Phish Blocker, do one of the following:
   - If you have a local Microsoft Exchange Server, use the **SMTP** area.
   - If you use Outlook to download web mail, use the **POP3** area.
   - If you use a rare, IMAP email client, use the **IMAP** area.

2. In the table, specify how you want Untangle Server to behave:

<table>
<thead>
<tr>
<th>Scan SMTP/POP3/IMAP</th>
<th>When the check box is selected, the Untangle Server scans email in both directions unless there is a custom policy that overrides these instructions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>This controls what actions Untangle Server should take on the message itself, should the message be determined to be phish:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mark.</strong> Causes the email message to have its subject changed to start with the phrase [Phish].... Users can then set up email client filter rules to cause such messages to be placed in special folders.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass.</strong> Causes the message to be passed on to the recipient, even though it was detected as phish.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Block.</strong> Applies only to SMTP mail. Causes the message to be blocked, meaning the sender believes it was delivered yet it was never forwarded to the recipient. Although neither sender nor recipient know the message was blocked, it will still be noted in the Event Log.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Quarantine.</strong> Applies only to SMTP mail. Causes the message to be quarantined. For more information on the operation of this feature, please refer to About Quarantine. As outlined in Creating Custom Policies, outgoing mail is not quarantined by default.</td>
</tr>
</tbody>
</table>

3. Click the **Save** button.
Web Settings

Enabling Google's Blocklist

Phish Blocker uses Google's blocklist (also known as Safe Browsing) to provide anti-phishing protection as you browse the Internet. Google's blocklist includes a list of known websites that trick you into disclosing sensitive information under false pretences. To ensure a high level of protection, Untangle Server updates Phish Blocker every six hours with updates to Google's blocklist. Even if you disabled automatic updates on your Untangle Server, your Phish Blocker receives Google's blocklist updates.

If you click on the URL in the phish email shown in Example Phishing Email, that link directs you to a site that is not registered to PayPal. That website is listed on Google's blocklist, so when you visit the website, Phish Blocker warns you that it's a phish website—protecting you against such website spoofing in the event that a phish email manages to pass the first barrier of protection, email anti-phishing protection.

Note: Advanced users can learn more about the intricacies of Google's blocklist by reading the specification, which is public.

In addition to filtering out phishing emails and websites, Untangle Server Phish Blocker blocks pharming websites.

Pharming websites mimic legitimate sites (often banking or ecommerce) and use social engineering to trick users into forfeiting their user names, passwords and other sensitive information when they mistakenly log into the fraudulent sites. The web properties often use URLs that look similar to the target site. For example, replacing the “w” in wells fargo with two “v”s (vvellsfargo.com), adding an extra “i” to wachoviiia.net, or by prefixing the target domain to the pharmer’s url, such as paypal.phishingsite.com. Further, pharming sites have become so well designed that visually determining the real from the fake has become nearly impossible.
Event Log

Phish Blocker provides two event logs: Web Event Log and Email Event Log.

Web Event Log

Use the following terms and definitions to understand the Phish Blocker’s Web Event Log:

<table>
<thead>
<tr>
<th>term</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>action</td>
<td>The action taken on the mail. The value depends on the mail protocol, but will contain descriptive text such as block or mark.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP Address of the protocol client. Recall that for SMTP this is the sender of the mail, and for IMAP/POP the receiver of the mail.</td>
</tr>
<tr>
<td>request</td>
<td>A description of the request made (e.g. <a href="http://someurl/somepath.html">http://someurl/somepath.html</a>).</td>
</tr>
<tr>
<td>server</td>
<td>The server IP Address. Recall that for SMTP this is the machine receiving the email, and for IMAP/POP the machine holding the inbox.</td>
</tr>
</tbody>
</table>

Email Event Log

Use the following terms and definitions to understand the Phish Blocker’s Email Event Log:

<table>
<thead>
<tr>
<th>term</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>action</td>
<td>The action taken on the mail. The value depends on the mail protocol, but will contain descriptive text such as block or mark.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP Address of the protocol client. Recall that for SMTP this is the sender of the mail, and for IMAP/POP the receiver of the mail.</td>
</tr>
<tr>
<td>subject</td>
<td>The subject of the email. This may be blank if the email had no subject.</td>
</tr>
<tr>
<td>receiver</td>
<td>The recipient email address of the email.</td>
</tr>
<tr>
<td>sender</td>
<td>The sender of the email. Note that for phishing emails, this is almost never legitimate.</td>
</tr>
<tr>
<td>server</td>
<td>The server IP Address. Recall that for SMTP this is the machine receiving the email, and for IMAP/POP the machine holding the inbox.</td>
</tr>
</tbody>
</table>
Phish Blocker FAQs

When configuring my Untangle Server to mark phishing emails received over IMAP, the subject of the mails changes to [PHISH]... only after I click on the message. Why?

Most IMAP clients first fetch summary information about emails (subject, sender) so the end user can see a preview list of messages. Only when the user selects (clicks on) the message is the actual content of the message retrieved from the server. It is then that the Untangle Server is able to scan the message. Unfortunately, some email clients do not detect the change in subject and update their preview list.

If an unwanted email (spam, phishing, etc) is received for an email address that cannot be quarantined, but my rules are set to quarantine, What happens?

The Quarantinable Addresses rules take precedence over the actions for email rules. In this situation, the email would be marked rather than quarantined.

Why is blocking (or quarantining) of emails not an option for POP or IMAP?

POP and IMAP work differently than SMTP. When POP and IMAP are used, the client requests the mail when the user clicks on the email. At that point the message is downloaded from the server and scanned. Even if the application determines the message is spam, it still must be delivered to the client because the client is waiting and will not be able to read mail unless something is delivered. As a result, only MARK is an option.

Why can't I block superspam for POP and IMAP emails like I can for SMTP?

For the same reason that you can't quarantine POP/IMAP spam. The message is not scanned until it is requested by the mail client. At that point, the message (even if it is spam) must be delivered to the client to complete the transaction.

Why does the Event Log report the sender as my bank, yet it was fraudulent? Why does it not report the real sender?

One of the characteristics of phishing emails is that they use deception to change the apparent sender of an email. Although Untangle Server can detect the email as a phishing attempt, there is no way to determine the true sender.

Why is Subject (or sender) blank for some emails in the Event Log?

Not all emails (especially spam emails) have subjects. Some spammers also use tricks to cause there to be no detectable sender.

Why is mail not passing between my Exchange servers?

The Untangle Server forces Extended SMTP (ESMTP) to fall back to SMTP so that the transmitting emails may be scanned. When two Exchange servers are setup such that they require ESMTP communication, all communications will fail. This is enforced by transparent rewriting of the "EHLO" command to "HELO" and appropriate keywords are also stripped.
This can be avoided by adding a special "No Rack" policy or a Bypass rule for communication for these two servers. To add a "Bypass Rule" go into config- >networking->advanced->Bypass Rules and create a rule that describe the traffic between your two servers. To add a "No Rack" policy, enter the Policy Manager, Custom Policies and add two policies to be processed by "No Rack", one from server A to server B port 25, and one from server B to server A port 25. The net effect is that any communications between these two servers will be ignored.

Can I forward my email to Untangle and then have Untangle forward the email to my mail server?

No. Untangle is a network gateway and is meant to be installed "in-line" with the traffic. Untangle does not store-and-forward mail. Untangle will transparently scan mail as it passes through it.

Can I have untangle drop mail that is not to valid users?

No. Untangle does not have a list of valid emails for your site. It is suggested that your configure your email server to not accept mail for invalid users. This is the default for almost all mail servers except Microsoft Exchange. The links below are instructions on how to configure your email server.

- Exchange 2003
- Exchange 2007

How do I stop sending Quarantine Daily Digests?

In Config > Email, you can uncheck the option for Send Daily Quarantine Digest Emails. This will prevent Quarantine Digests from being sent.

I don't send Daily Digests. How can I keep from running low on disk space?

This is generally not a problem, but if you have a small disk drive or you receive a huge volume of spam, you may need to shorten the number of days that you retain quarantined email for. This is adjustable in Config > Email.

I need to keep a Quarantine for everyone, but how do I limit who receives a Quarantine Digest?

You can decide whose spam can be quarantined, but they will receive a digest if you do that. You cannot turn the digest on or off for specific users once you have decided that they will or will not have a quarantine available.

How do I resend Quarantine Daily Digests?

You can resend digests by launching the Untangle Server's Request Quarantine Daily Digest Email window. Go to Resending Quarantined Daily Digests.
Why are users not receiving a Quarantine Daily Digest?

- The untangle server may not be configured to send email correctly. Check Config > Email
- Users might not have anything new in the quarantine. A daily digest is sent only if something new is in the quarantine.
- If this is happening for all users, make sure that you have not turned off the option for Quarantine Daily Digest delivery.

What happens to email recipients' email when those recipients are not on the quarantinable address list?

If you removed the wildcard (*) and created a quarantinable address list, the Spam Blocker passes but marks the email as [Spam]—for those that are not on the list.

Why does my Quarantine have emails for people who don’t work here?

Spammers do not discriminate...they send spams in many ways to get their message into your mailbox. Untangle simply scans email for viruses, phishing attempts and spam. It does not look to see if the message is going to a valid recipient. In Config > Email > Quarantine > Quarantinable Addresses, change the Quarantinable Address from *** to "@<mycompany>". Change <mycompany> to your company name. Only mail that is coming to your company will now be quarantined. Please note that spams may still come in for illegitimate email addresses that correspond to your domain name.

I have 600 messages in my quarantine. How can I go through them faster?

Look at the bottom of the Quarantine Digest. You can choose how many messages appear per page. You can set the maximum number to 25, 100, 1000 or all messages. That will help you go through them faster, but be warned. Choosing a high number causes a large web page to be loaded. Depending on how much memory your computer has available, that may cause your browser to crash...or worse.

I released an email from my Quarantine Digest. Where did it go?

It is likely that the email was captured again by Spam Blocker. To make sure this doesn’t happen, go to Config > Email > Outgoing Server and note the From Address that is being used by Untangle. Add this address to Config > Email > From-Safe List. This will prevent Untangle from scanning any email being released from Quarantine Digest.

I get two copies of the Quarantine Digest. Why?

You are likely a member of a email distribution list and the quarantine is not configured properly. Let's use an example. You are a member of a list called sales@xyz.com. The list members are joebob@xyz.com, fredbob@xyz.com and bobbob@xyz.com. They all complain that they get two Quarantine Digests daily.
In the Quarantinable Forwards panel (Config > Email > Quarantine > Quarantinable Forwards), there is nothing listed. That means that each of these people gets a Quarantine Digest for their own email address as well as one for sales@xyz.com. Joe Bob is supposed to manage quarantines for the mailing list, so we should make an entry under distribution list address as sales@xyz.com and its corresponding send to address as joebob@xyz.com. That should take care of the problem. Don’t forget to save your changes.

If there is a mailing list with a large number of members (hugelist@xyz.com) and you wish to have multiple people responsible for checking the quarantines, create a new email distribution list in your mail server (notsohugelist@xyz.com) that contains the email addresses for the people who have this responsibility, then set the Untangle Quarantine Forwards pair to hugelist@xyz.com and notsohugelist@xyz.com. Only those people who have the responsibility will get Quarantine Digests for the mail list.

**Why can’t my off-site users get their Quarantine Digests?**

The most common reason is that the Quarantine Digest has a URL that has an IP address that is private (on the LAN). They need a URL that is accessible to the public. You can set that up as follows:

1. In Config > Administration > Public Address, define an IP address that is accessible on the outside. Make sure to click the Enabled button.
2. In Config > Administration, make sure that Enable Outside Quarantine Viewing is checked.
3. In Config > Networking > Hostname, determine if you can give a name to the Untangle Server. Enter that if appropriate. If a hostname is defined and it is resolvable on public DNS servers, check the Hostname resolves publicly box. If you wish to use a hostname and one is not available for you, you may wish to use Dynamic DNS to associate a hostname with an IP address. Refer to Configuring Untangle Server To Use Dynamic DNS for more information.
Spyware Blocker
Spyware Blocker is a compilation of several open source projects. Spyware Blocker examines web requests from your protected network and does the following:

- Uses virus signatures to detect and identify specific viruses.
- Prevents keyloggers, a computer program that captures and stores the keystrokes of a computer user.
- Provides a URL blacklist to block known spyware websites (for example, www.gator.com).
- Provides a URL blacklist to block websites that require cookies.
- Blocks harmful Active X controls that are known to be spyware applications.
- Examines the IP addresses of websites that users visit, and compares them to a list of offending subnets.

In the unusual event that members of your organization visit a legitimate website that Spyware Blocker deems malicious, the Untangle Server’s interface enables you to create exception rules to remove this website from Spyware Blocker’s blacklist.

Settings
This section reviews the different settings and configuration options available for Spyware Blocker.

Block Lists
This tab controls the different mechanisms to classify and block content. Using this tab, you can selectively block Spyware and Ad URLs, cookies, and ActiveX controls.

Blocking Spyware Websites
Just make sure Block Spyware & Ad URLs and Spyware Blocker will be working - for more information on the User Bypass setting, see Unblocking Spyware Websites.

Blocking Cookies
If Block Tracking & Ad Cookies is checked, these cookies will be blocked by Untangle. If you need to add more, you can simply click manage list and enter a URL or IP - make sure Block is checked or nothing will happen!
Blocking ActiveX Controls

To block additional ActiveX Controls:

1. From Spyware Blocker, click the **Settings** tab.

2. Click the **Block Lists** tab, and click the **manage list** button under ActiveX section. The table that appears contains known malicious ActiveX controls, so do not clear the **block** check box.

3. Click the plus (add) button to the left of the table. A new row appears with the **block** check box selected.

4. Add the **identification** of the ActiveX control, and click the **Save** button.

5. Contact Untangle Technical Support to inform us of the new malicious ActiveX control that you identified as Untangle constantly improves its products.

Blocking All ActiveX Controls

If your end-users do not have job responsibilities that require them to download plugins, you might want to block all ActiveX controls—both malicious and helpful ActiveX controls. Spyware Blocker provides a long list of known malicious ActiveX controls, but this list is incomplete because not all malicious ActiveX controls are known by the Internet community.
To block all ActiveX Controls:

1. From Spyware Blocker, click the Settings button.
2. For the block all ActiveX checkbox, select the Block All ActiveX check box.
3. Click the OK button.

Monitoring Suspicious Traffic

This option allows you to log traffic going to known advertising and tracking companies, however traffic will not be blocked. You can add your own using the manage list button.

Pass List

Pass Lists are used to pass content that would have otherwise been blocked. This can be useful for "unblocking" sites that require functionality impaired by Spyware Blocker or allowing certain users special privileges.

Unblocking Spyware Websites

If a trustworthy user within your protected network needs to visit a site that is listed on one of the block lists because it is known to download spyware, you can unblock that website; in fact, Untangle recommends that you do so in order to maintain the highest workplace productivity.

If you need to prevent a website from being categorized as spyware, you can add that site to the pass list or use the Spyware Blocker's quick-passlist as outlined in this procedure. If you want specific users to have this privilege, but not all users, create a virtual rack for the users that need quick-passlist privileges.

To unblock a spyware website:

1. From Spyware Blocker, click the Settings button.
2. Do one of the following:
   - If you want to enable users to decide for themselves or others or both whether or not to block a known spyware website, specify a quick-passlist:
     a. Click the Block Lists tab.
     b. For the User Bypass setting, select Temporary or Permanent and Global:
Enabling Users to Unblock Spyware Websites

- **Temporary.** Enables the user that visits the spyware website and unblock that site for *himself/herself* for 1 hour. When the user visits a spyware website, the user receives a warning stating that it is a known spyware site. The user can bypass the warning and visit the site, or choose not to launch the website. If the user bypasses the warning, Spyware Blocker no longer alerts the user if the user visits that spyware site within the 1 hour timeframe. If the user choose not to launch the website, Spyware Blocker alerts the user to the hazard of launching a spyware site the next time the user visits the website.

- **Permanent and Global.** Enables any user to visit the spyware website and unblock that site for *himself/herself and all other users*. When the user visits a spyware website, the user receives a warning stating that it is a known spyware site. The user can bypass the warning and visit the website, or choose not to launch the website. If the user bypasses the warning, Spyware Blocker no longer alerts *all* users that visit that spyware site in the future. If the user choose not to launch the site, Spyware Blocker continues to alert the user to the hazard of launching a spyware site.
If you want to unblock specific sites for all users, create a pass list.

a. Click the **Pass List** tab.

b. Click the add (plus) button to the left of the table. A row appears with the **pass** check box selected.

c. In the new entry, type the domain name that you want to unblock. Domain field is the only required field. The format of the domain is `http://approved_domain` where `approved_domain` is replaced with the approved domain. Although it may seem as one could enter a full URL path into the domain field, domain only handles top-level domains. For example, attempting to place `http://some_domain.com/site1` into the pass list causes all paths at `http://some_domain.com` to be passed (such as `http://some_domain.com/site2`).

**Tip:** Administrators can enable/disable a domain from being bypassed by selecting the **pass** check box.

### Unblocking ActiveX Controls

Spyware Blocker provides you the ability to unblock ActiveX Controls, however Untangle recommends that you do not unblock any that are blocked by default because these are known to be malicious. If you add any additional ActiveX controls to the Spyware Blocker, you can then use the **block** check box to enable and disable individual ActiveX controls to ensure that you are properly identifying them.

### Event Log

Use the following terms and definitions to understand the Spyware Blocker Event Log:

<table>
<thead>
<tr>
<th>timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>The action which took place (e.g. block).</td>
</tr>
<tr>
<td>client</td>
<td>The client IP address of the traffic.</td>
</tr>
<tr>
<td>request</td>
<td>A description of the request made (e.g. <code>http://someurl/somepath.html</code>).</td>
</tr>
<tr>
<td>reason for action</td>
<td>The reason the action was taken (e.g. in URL list).</td>
</tr>
<tr>
<td>server</td>
<td>The server IP address of the traffic.</td>
</tr>
</tbody>
</table>
Spyware Blocker FAQs

My users complained that they cannot connect to somesite.com, and it keeps showing up in my Event Log as blocked. How can I stop somesite.com from being blocked?

You can add a rule to the Pass List for somesite.com, as described in Unblocking Spyware Websites.

While I agree that ActiveX is something I would like to keep out of my network, one of our business partner’s sites requires ActiveX. How should I configure my system?

First, disable all ActiveX Controls as described in Blocking All ActiveX Controls. Then, exclude your business partner from this restriction by adding the business partner’s domain to the Pass List as described in Unblocking Spyware Websites.
Web Filter

Web Filter appeals to customers who require an added level of protection or are subject to regulations. For example, Web Filter helps libraries comply with Children's Internet Protection Act; equally important, Web Filter helps schools control hate speech. Pornography is still a big workplace productivity problem for companies, and Web Filter's categorization is a great solution for this problem.

The main technical differences between these products is that Web Filter offers:

- **Real-time classification and updates.** Web Filter uses a community-based approach whereby a large base of Web Filter users and Untangle itself categorize URLs. However, Web Filter combines both human beings—and sophisticated web crawlers. Web Filter runs web crawlers throughout the day. If Web Filter's web crawlers detect a new site or if you visit a site that Web Filter doesn't know about, it immediately analyzes it, then does the following:
  - If Web Filter's engine can identify the content with high probability, it will categorize it.
  - If Web Filter's engine cannot identify the content with high probability, it will be assigned to be identified by a human.

Web Filters techniques result in more categorization (over 100,000 URLs daily), more accuracy, and faster turnaround time. When identifies a malicious website, customers get the update within seconds. Time is essential in web content filters because new websites go live very quickly.

- **Categorize HTTPS traffic by IP address.** Untangle can block site via a URL or the IP address of the web site. Since secure websites cannot be scanned, this feature tries to use reverse DNS to figure out the category. (If https appears in the URL, then you know it's a secure site.) If it cannot resolve, this option will block inbound and outbound SSL traffic on port 443.

So, for example, when you log on to your online banking account to view a statement, a secure site prevents others on the network from capturing private information such as your username and password. But, there's a dirty little secret that's known to those who want to bypass web filters. Often used in the pornography industry, the web site is set up as a secure site. Web Filter easily combats this tactic because Web Filter also categorizes the destination IP address, which isn't unknown. This feature is implemented via the Web Filter **Scan HTTPS** check box.

- **Detailed categorization.** Web Filter does a good job categorizing, but Web Filter offers over 53 categories and over 450 million categorized sites. The abundance of categories means that you can narrow your scope. For example, maybe you want to block websites related to Dating, but not Social Networking. You can do so with Web Filter.
Settings

This section reviews the different settings and configuration options available for Web Filter.

Block Lists

This tab controls the different mechanisms to classify and block or flag content.

Categories

Category blocking is driven by the zvelo SiteFilter database.

If block is checked any sites and URLs in that category will be blocked and flagged as a violation. If only flag is checked (but not block) the visit will be flagged as a violation but still allowed to pass. Flagging a visit as a violation has no visible effect to the user but makes finding and tracking undesired behavior in the reports easier.

Note: All URLs visited from machines behind an active application will be automatically tagged for categorization, but if you want to manually add or check a URL you can use the zvelo URL checker.

Categorize HTTPS traffic by IP address

When this option is enabled, will attempt to match HTTPS traffic to its IP address database since the destination IP address is all it has to work with.

Blocked Sites

To block a specific website:

1. From Web Filter, click the Block Lists tab and the Edit Sites button.
   1. In the table, click the add (+) button to the left of the table.
   2. In the new entry, add the URL that you want to block.
   3. Click Done

2. Click the Save button to save the newly added entries or the Apply button to save and continue adding new entries.

3. Click the OK button

Tip: If you want to temporarily unblock this website later, deselect the block check box.

Blocking File Types

To block content by file type:

1. From Web Filter, click the Block Lists tab and the Edit File Types button.

2. In the table, do one of the following:
If the file type that you want to block already appears in the table, select the **block** or **log** check box or both.

If you want to block a file type that isn't in the list, click the add (+) button to the left of the table, then specify the file type that you want to block.

3. Click the **Save** button, then **OK**.

**Blocking MIME Types**

**To block by MIME type:**

1. From Web Filter, click the **Block Lists** tab, and click the **Edit MIME Types** button.

2. In the table, do one of the following:
   - If the MIME type that you want to block appears in the table, select the **block** check box for that MIME type.
   - If you need to add a new MIME type, click the add (+) button to the left of the table, and in the new entry, add the MIME type that you want to block.

3. Click the **Save** button, then **OK**.

**Enforce safe search on popular search engines**

When this option is enabled, safe search will be enforced on all searches using supported search engines (Google, Yahoo, etc).

**Block pages from IP only hosts**

When this option is enabled, users entering the IP address rather than domain name will see a block page.

**User Bypass**

Some organizations may wish to allow certain users to bypass the Web Filter. This option is available under "User Bypass."

If User Bypass is set to **None** no users will be allowed to bypass the block page. If User Bypass is set to **Temporary** users will be allowed to bypass the block page for one hour from the time it is bypassed. If User Bypass is set to **Permanent and Global** then users will be allowed to bypass the block page and bypassed sites will be added to the permanent global pass list.

User Bypass is best when combined with Policy Manager so that only certain users are allowed to bypass.

**To configure User Bypass:**

1. From Web Filter, click the **Block Lists** tab.
2. Under **User Bypass** choose **None, Temporary, or Permanent and Global**

3. Click the **Save** button.

**Pass Lists**

**Pass Lists** are used to pass content that would have otherwise been blocked. This can be useful for "unblocking" sites that you don't want blocked or allowing certain users special privileges.

**Passed Sites**

If your organization deems a specific website to be useful and that site or URL should not be blocked regardless of its categorization, it can be added to the **Passed Sites** list.

**To pass a specific URL blocked by a category:**

1. From Web Filter, click the **Pass Lists** tab and the **Edit Passed Sites** button.

2. In the table, do one of the following:
   - If the URL that you want to pass appears in the table, select the **pass** check box for that URL.
   - If you need to add a new URL, click the add (+) button to the left of the table, and in the new entry, add the URL that you want to pass.

3. Click the **Save** button, then **OK**.

**To pass a specific URL blocked by a user-defined URL:**

1. From Web Filter, click the **Block Lists** tab and the **Edit Sites** button.

2. In the table, locate an existing URL that you want to pass, and clear the **block** check box, or simply delete the row.

3. Click the **Save** button, then **OK**.

**Passed Clients**

If you only have a few users that need to completely bypass Web Filter controls, consider using pass lists. If these users simply need a different Web Filter policy you should set up a separate rack using Policy Manager.

**Before You Begin:** It may be useful to assign the user a static IP address. If the Untangle Server is your router, go to Assigning Network Computers Static IP Addresses.

**To pass for specific users:**

1. From Web Filter, click the **Pass Lists** tab and the **Edit Passed Client IPs** button.
2. In the table, select the add (+) button. A new row appears.

3. In the **IP address/range** text box, specify the computer IP address and subnet mask of user that you want to be exempt from the web filter.

4. Click the **Update** button, then **Save**.

**Event Log**

Use the following terms and definitions to understand the Web Filter Event Log:

<table>
<thead>
<tr>
<th><strong>timestamp</strong></th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>The action which the Untangle Server took on the web request.</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>IP address of the client who made the request.</td>
</tr>
<tr>
<td><strong>request</strong></td>
<td>A description of the request made (e.g. <a href="http://someurl/somepath.html">http://someurl/somepath.html</a>).</td>
</tr>
<tr>
<td><strong>reason for action</strong></td>
<td>The reason the action was taken.</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>The server IP Address. The server is the computer that receives the request.</td>
</tr>
</tbody>
</table>

**Web Filter FAQs**

**Does Web Filter use a lot of memory and CPU?**

If your Untangle Server is operating well without Web Filter, then you won't see much of a difference if you run Web Filter. Web Filter doesn't use much memory, and there's very little CPU utilization.

**How do real-time updates work in an Untangle Server environment?**

Untangle Server keeps a local copy of the Web Filter database. If you visit a website that the Web Filter database doesn't know about, Web Filter phones home to the Web Filter service, then writes the new information to the Web Filter database.

**How long does Web Filter cache visited sites?**

Several days. Web Filter flushes non-frequently used cache. The website that you visit daily will not be cleared from cache.

**Can I import Web Filter pass lists into Web Filter?**

Not at this time. You should take a screenshot and manually add them to the list via the UI.

**Can I add to the categories?**
No. Web Filter has an extensive list of categories and taxonomy. If you feel there is a category that's missing, let us know.

**How should I handle false positives?**

You can use pass lists to treat false positives.

**Can I use Web Filter to block SSL sites?**

Web Filter can categorize HTTPS traffic based on IP. This means that if you've blocked "Proxy sites" then even HTTPS proxy sites will be blocked.

*Note:* This does not mean Web Filter can parse HTTPS as it is encrypted. Categorization is done via IP address. This means other forms of blocking like URL, file-type, mime-type, etc can not be done on HTTPS as the stream is encrypted and these require parsing of the HTTP protocol.

**I blocked a site but when I visit the site via HTTPS it isn’t blocked. Why?**

Web Filter scans and categorizes HTTPS traffic by IP address because the session itself is encrypted and cannot be scanned. As a result if you add "wellsfargo.com" to the block list and goto "https://wellsfargo.com" it will not be blocked because Untangle can only see the IP address not the hostname (wellsfargo.com). However, if you block the "Finance" category and goto "https://wellsfargo.com" you will notice it does not correctly connect and you can see a block event in the eventlog.

**Web Filter was blocking an HTTPS site, but I added it to the passlist. It is still blocked. Why?**

Web Filter does categorization of HTTPS by IP. The hostname and request are encrypted. This means if https://example.com/ is getting blocked, adding "example.com" to the passlist will have no effect because HTTPS is categorized by IP address. If you add the IP address of example.com to the passlist then HTTPS traffic to example.com will be allowed.

*Note:* If an entire domain is passlisted it will work for clients that specify SNI information in the HTTPS stream.

**Does the Web Filter event log show the AD user info?**

Currently, this is not possible, the event log will only show the IP addresses.

Possible work around. Open a browser and type the IPAddressoftheUntangle/adpb/debug (you might need to login) This will show you the current AD users that are logged in and their IP address. You can use this to find out which user did what on the event log. You might want to use ctrl f (find) on your keyboard.
Web Cache
The Web Cache application provides HTTP content caching: as web traffic passes through the Untangle Server it will be transparently cached. This will both save bandwidth by serving repeat content from the local cache and improve user experience by loading cached sites faster.

Just like the Web Filter and other applications on Untangle, Web Cache works transparently on traffic passing through the Untangle Server. There is no need to change any of the settings on any of the PCs behind Untangle to gain the benefits of web caching.

As content is downloaded from the web it is stored in a local cache on the disk. Upon later requests of the same web document the content is served directly from the local cache. The same document does not get downloaded multiple times, and the client gets a better user experience because they don’t have to wait on subsequent downloads of the same document.

Settings
This section reviews the different settings and configuration options available for Web Cache.

Status
The Status tab displays statistics from Web Cache - there are no settings to configure. You can also clear the cache from this tab.

Statistics

- **Cache Hit Count** displays the total number of HTTP requests that have been served from cache.

- **Cache Miss Count** displays the total number of HTTP requests that were not found in cache and thus were served using content retrieved from the external server where the content resides.

- **Cache Hit Bytes** displays the size, in bytes, of all HTTP requests that have been served from cache.

- **Cache Miss Bytes** displays the size, in bytes, of all HTTP requests that were not found in cache.

- **User Bypass Count** displays the number of HTTP sessions that bypassed the cache because the server hosting the content was listed in the user managed cache bypass list.

- **System Bypass Count** displays the number of HTTP sessions that bypassed the cache because the system determined they were not compatible with our caching model. Web Cache can generally handle all GET and HEAD requests, and we also allow smaller POST requests to transit through the cache logic. Everything else (ie: Large POST requests, non HTTP traffic, etc.) will be allowed to bypass the cache entirely.
Clear Cache

If content stored in the cache somehow becomes stale or corrupt, the cache can be cleared with the Clear Cache button. As noted in the GUI, clearing the cache requires restarting the caching engine, which will cause active web sessions to be dropped and may disrupt web traffic for several seconds.

Cache Bypass

The Bypass tab contains a list of domains which will bypass the caching mechanism.

To add a new entry to the Cache Bypass list:

1. From Web Cache, click the Settings button.
2. Click the Cache Bypass tab.
3. Click the add (+) button.
4. Specify the exception that you want to add:

<table>
<thead>
<tr>
<th>Enable</th>
<th>When this box is checked, the exception rule is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname of the site(s) you'd like Web Cache to ignore.</td>
</tr>
</tbody>
</table>
5. Click the OK button.

Event Log

Use the following terms and definitions to understand the Web Cache Event Log:

<table>
<thead>
<tr>
<th>timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>hit count</td>
<td>The total number of HTTP requests that have been served from cache.</td>
</tr>
<tr>
<td>miss count</td>
<td>The total number of HTTP requests that were not found in cache and thus were served using content retrieved from the external server where the content resides.</td>
</tr>
<tr>
<td>bypass count</td>
<td>The number of HTTP sessions that bypassed the cache because the server hosting the content was listed in the user managed cache bypass list.</td>
</tr>
<tr>
<td>system count</td>
<td>The number of HTTP sessions that bypassed the cache because the system determined they were not compatible with our caching model.</td>
</tr>
<tr>
<td>hit bytes</td>
<td>The size, in bytes, of all HTTP requests that have been served from cache.</td>
</tr>
</tbody>
</table>
**miss bytes**
The size, in bytes, of all HTTP requests that were not found in cache.

---

**Web Cache FAQs**

**How does Web Cache work?**

The WebCache rack node subscribes to all port 80 traffic. Each client request is forwarded to the squid cache running on the local appliance. If the cache has the content stored locally, we transmit the response directly to the client, allowing all the other nodes and services to act on the content as required, and life is grand. That's called a cache hit, and it's really pretty simple.

The real magic kicks in when handling a cache miss. In this case, we can't allow squid to go grab the content and hand it directly to the client like it normally would. We need the response to pass through all of the other apps and services. So we got a little creative with the Squid setup by configuring all external content to come from a peer cache. That peer cache is actually another thread within our WebCache node. When Squid connects back to us for a cache miss, we allow the original request to continue outbound as it normally would, and we intercept the response from the external server. This allows us to push a copy of the content into Squid while also returning it to the client at the same time.

**Is Web Cache Squid?**

There are two key components to the Web Cache application: the Web Cache rack application and the web caching engine (squid). The most complex piece of the content caching pie is the Web Cache application. For years, customers have been asking for an HTTP caching solution. However, for as simple as Untangle seems on the surface, there is a lot of complicated stuff going on under the hood. Support for multiple network interfaces, a virtual environment that supports our rack implementation and hierarchical application model, and a suite of diverse applications and services all working together in perfect harmony.

Adding web caching to our platform required engineering a method to insert the caching engine within the secure communications channel while ensuring all of the other applications and services continue to function normally. First and foremost, the cache must not allow the circumvention of any other content controls installed and configured on the appliance. Also, a single backend cache is shared across all application instances, so we had to design the cache application to ensure the other nodes and services affect the traffic flow outbound from the cache rather than putting their potentially modified results into the cache. This prevents, for example, the porn block page from one policy/rack from being cached and served to users of a different policy/rack who are allowed to view porn. Something none of us would ever do, but it makes for a fun example of the technical challenges of our solution.

The other piece of the pie is the caching engine. Sure... we could have written this ourselves... we're smart like that. But the truly smart thing to do here was leverage an
existing solution. Something that is mature, stable, well written, and highly efficient. The natural choice was Squid. It works. It works very well, and fortunately we were able to devise a way to hook it into the traffic stream to meet all the challenges mentioned above.

TLDR; Web Cache does leverage squid, but it is not squid. It is an Untangle application.

Is Web Cache a "proxy?"

I would recommend avoiding use of the word "proxy." "Proxy" means a lot of things to a lot of different people so it can be confusing.

Web Cache is not a SOCKS proxy. Historically web caches have often been implemented using SOCKS proxying, but there are web caches that do not require using a SOCKS proxy. Likewise there are SOCKS proxys that do not provide web caching. The word "proxy" while often associated with web caching, is a separate function.

The Web Cache application does not require nor provide SOCKS proxy functionality.

Also beware that Untangle itself is a “transparent proxy” because it filters traffic at layer-7 as an in-line device.
Bandwidth Control

The *Bandwidth Control* applications gives administrators the power to monitor and control bandwidth usage on the network. This ensures that the network continues to operate smoothly and that bandwidth is shared optimally based on what's important to your organization.

Many organizations struggle with bandwidth related issue, such as students using all the bandwidth watching online videos or users downloading files using BitTorrent, while more important tasks struggle to complete because the lack of available bandwidth.

Bandwidth Control provides tools to monitor and control the different applications and users' use of network bandwidth. Many options are available such as:

- Prioritize time-critical applications, such as online meetings, webinars or VOIP.
- Prioritize important websites, like salesforce.com or the company website
- Give different users and/or groups different bandwidth usage rights
- Give important servers and services bandwidth reservations
- Track and monitor bandwidth usage and bandwidth abusers
- Troubleshoot bandwidth-related network slow-downs
- Deprioritize unimportant apps and traffic like YouTube, other video or games sites.
- Limit abusers' bandwidth when using unwanted protocols, like BitTorrent or P2P.
- Deprioritize certain tasks (like backups and updates) so that they can run at all times without interfering with network operation.
- Optimize real-time applications like chat, web, Skype, games, etc.
- Limit hosts to certain hourly/daily/weekly bandwidth quotas.
- More!

The Bandwidth Control help will start from the basics of getting Bandwidth Control running on the network and later cover how to craft some custom rules to cover specific issues.

**Settings**

This section describes the settings of Bandwidth Control.

**Status**

This tab shows the current status of Bandwidth Control. Initially after installation, Bandwidth Control will need configuration before it can be enabled.
Status
Bandwidth Control is unconfigured. Use the Wizard to configure Bandwidth Control.

Run Bandwidth Control Setup Wizard

To configure Bandwidth Control, click on **Run Bandwidth Control Setup Wizard**

**Setup Wizard**

The setup wizard configures the initial configuration of Bandwidth Control.

After the welcome screen, you will be asked to set the bandwidth rates of your WAN interface.

**Configure WAN download and upload bandwidth**

Please enter the External WAN's download and upload bandwidths below.

<table>
<thead>
<tr>
<th>Bandwidth (Kbit)</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download</td>
<td>10000</td>
</tr>
<tr>
<td>Upload</td>
<td>1000</td>
</tr>
</tbody>
</table>

It is suggested to set these around 95% to 100% of the actual measured bandwidth available for this WAN. **WARNING:** These settings must reasonably accurate for Bandwidth Control to operate properly!

This is the most important setting in the configuration of Bandwidth Control. If you are unsure it is recommended to run some bandwidth tests when there is no other activity to determine the true download and upload rates of your WAN connection. Entering a value around 95%-100% of the measured value is typically ideal. If the value is too low, Bandwidth Control will unnecessarily limit bandwidth to the value you have entered. If the value is too high, Bandwidth Control will be less effective as it will over-allocate bandwidth and lose some ability to differentiate by priority.

You will be asked to repeat this process for each WAN interface.

After setting the WAN settings, choose a starting configuration that best suites your organization.

**Choose a starting configuration**

Several initial default configurations are available for Bandwidth Control. Please select the environment most like yours below.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>School</td>
<td></td>
</tr>
</tbody>
</table>

Each configuration's goals are described as well as what is prioritized and deprioritized. These rules can be customized later - this is just a starting configuration.
In addition to the starting configuration, quotas can also be configured. Most sites will not need quotas, however quotas can be extremely useful in some scenarios to prevent users from monopolizing resources.

To enable quotas, click on *Enable* and provide information that best suites your organization.

- **Quota Clients** describes which clients will be given quotas. Be careful to not give a range that includes any servers and machines that you don't want to have quotas.

- **Quota Expiration** describes the expiration time of each quota (or length of time the quota will be in use.) After a quota expires a new quota will be granted.

- **Quota Size** is the size of the quota each host is granted (in bytes).

- **Quota Exceeded Priority** is the priority given to hosts after (if) they exceed their quota.

More information on Quotas and how they work can be found in the Quota section.

After this your configuration of Bandwidth Control is complete and Bandwidth Control is enabled!

[edit]

**Bandwidth Monitor**

Also available on the *Status* tab is the *Bandwidth Monitor*

To open the Bandwidth Monitor click on *Open Bandwidth Monitor* and select the interface to monitor and click *Refresh*. Bandwidth Monitor can still be used when Bandwidth Control is disabled.
**Bandwidth Monitor**

The Bandwidth Monitor shows real-time network usage on the network.

Open Bandwidth Monitor

The Bandwidth Monitor provides a view into the current usage of bandwidth on a specific interface.

Each row shows a session going through Untangle and its current bandwidth usage and properties. This allows for the sorting of sessions by the various properties to determine the current usage of bandwidth on the network.

<table>
<thead>
<tr>
<th>Column Header</th>
<th>Property Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total KB/s</td>
<td>Total kilobytes per second used by this session</td>
</tr>
<tr>
<td>Client KB/s</td>
<td>Kilobytes per second of data sent by the client</td>
</tr>
<tr>
<td>Server KB/s</td>
<td>Kilobytes per second of data sent by the server</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol of the session (TCP or UDP)</td>
</tr>
<tr>
<td>Bypassed</td>
<td>True if this session is bypassed (not scanned)</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority assigned to this session (by Bandwidth Control and/or QoS)</td>
</tr>
<tr>
<td>Policy</td>
<td>The policy or rack handling this session (if not bypassed)</td>
</tr>
<tr>
<td>Client Interface</td>
<td>The interface of the client of this session</td>
</tr>
<tr>
<td>Client (Pre-NAT)</td>
<td>The client IP of this session</td>
</tr>
<tr>
<td>Server (Pre-NAT)</td>
<td>The server IP of this session</td>
</tr>
</tbody>
</table>
Client Port (Pre-NAT) | The client port of this session (0-65535)
---|---
Server Port (Pre-NAT) | The server port of this session (0-65535)
Server Interface | The interface of the server of this session
Client (Post-NAT) | The client IP of this session (after NAT and port forwards)
Server (Post-NAT) | The server IP of this session (after NAT and port forwards)
Client Port (Post-NAT) | The client port of this session (after NAT and port forwards)
Server Port (Post-NAT) | The server port of this session (after NAT and port forwards)
Local | True if this session is to the Untangle Server itself
NATd | True if this session has been NAT translated.
Port Forwarded | True if this session has been port forwarded.

Note: This tool only shows existing sessions. As such very short lived sessions will not be visible.

Rules

The rules tab contains most of the configuration and settings controlling the behavior of Bandwidth Control. Rules determine the action that will be taken when traffic passes through Bandwidth Control.

For each session the rules are evaluated in order until the first match is found. The action associated with the matching rule is performed and the data chunk is sent on its way. If no rule is found the no action is taken. If the session has been given no priority it is given the default priority of QoS (Medium by default).

Technical Note: The rules are actually consulted not only when the session is formed but also again on the first ten packets because some matchers such as "HTTP: Hostname" or "Protocol Control: Signature" are not known until several packets into the session. Also, All of a host's sessions will be reevaluated when they are added/removed to the penalty box or when a quota is exceeded.

Example: A quick example scenario with three rules shows how this works. Let's create three rules. Let's assume we want to prioritize web traffic so it's fast, and we also want to deprioritize a certain user's traffic because he/she has been problematic. Everything else should get the Medium priority.

- Rule 1 If Protocol = TCP and Destination Port = 80 then Set Priority = High
- Rule 2 If "Directory Connector: Username" = "dmorris" then Set Priority = Low
- Rule 3 If Protocol = TCP or UDP then Set Priority = Medium

As such, all port 80 (web) traffic will get High priority as it immediately matches the first rule and no more rules are evaluated. All of user dmorris's will be deprioritized to Low except dmorris's port 80 web traffic because it matched the first rule. Everything else will be given the Medium priority as it matched neither the first nor second rule.

Extensive rule sets can be created (and imported and exported) that carefully assign the correct priorities to the desired traffic and perform the desired actions at the desired times. The next section covers how a rule works and the different "matchers" and "actions" that can be configured in each rule.

Anatomy of a Rule

A Rule is a collection of matchers and an action to take place if all matchers match the session being evaluated.

The above rule has two matchers, one to verify that it only matches TCP traffic and one to verify it only matches port 80 traffic. If the session matches these attributes, it will have its priority set to High. If this rule is put at the top of the rule list, all TCP port 80 sessions will be given the High priority.
Matchers can match on many attributes of a session. Below are the matchers available for rules.

**Matchers**

<table>
<thead>
<tr>
<th>Column Header</th>
<th>Legal Value</th>
<th>Property Description</th>
<th>Required Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>IP Matcher</td>
<td>Matches if the session's client/source IP matches this value.</td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP Matcher</td>
<td>Matches if the session's server/destination IP matches this value.</td>
<td></td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port Matcher</td>
<td>Matches if the session's server/destination port matches this value.</td>
<td></td>
</tr>
<tr>
<td>Source Interface</td>
<td>Checkboxes</td>
<td>Matches if this session's client/source interface is checked</td>
<td></td>
</tr>
<tr>
<td>Destination Interface</td>
<td>Checkboxes</td>
<td>Matches if this session's server/destination interface is checked</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Checkboxes</td>
<td>Matches if session's protocol interface is checked</td>
<td>Protocol Control</td>
</tr>
<tr>
<td>Client in Penalty Box</td>
<td></td>
<td>Matches if session's client IP is in the penalty box.</td>
<td>Protocol Control with enabled signature</td>
</tr>
<tr>
<td>Server in Penalty Box</td>
<td></td>
<td>Matches if session's server IP is in the penalty box.</td>
<td>Protocol Control</td>
</tr>
<tr>
<td>HTTP: Hostname</td>
<td>Glob Matcher</td>
<td>Matches if this in an HTTP session to the set hostname. (*untangle.com)</td>
<td>Any HTTP processing app</td>
</tr>
<tr>
<td>HTTP: URI</td>
<td>Glob Matcher</td>
<td>Matches if this in an HTTP session request the given URI. (<em>index.html</em>)</td>
<td>Any HTTP processing app</td>
</tr>
<tr>
<td>Protocol Control: Signature</td>
<td>Glob Matcher</td>
<td>Matches if this session matches the given Protocol Control signature (ie &quot;Bittorrent&quot;).</td>
<td>Protocol Control</td>
</tr>
<tr>
<td>Control: Signature Category</td>
<td>Matcher</td>
<td>given Protocol Control signature's category (ie &quot;Instant Messenger&quot;).</td>
<td>with enabled signature</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Protocol Control: Signature Description</td>
<td>Glob Matcher</td>
<td>Matches if this session matches the given Protocol Control signature's description (ie &quot;chat&quot;).</td>
<td>Protocol Control with enabled signature</td>
</tr>
<tr>
<td>Web Filter: Category</td>
<td>Glob Matcher</td>
<td>Matches if this session is an HTTP session to the given category site. (ie &quot;Gambling&quot;)</td>
<td>Web Filter</td>
</tr>
<tr>
<td>Web Filter: Category Description</td>
<td>Glob Matcher</td>
<td>Matches if this session is an HTTP session to the given category site's description. (ie &quot;Gambling&quot;)</td>
<td>Web Filter</td>
</tr>
<tr>
<td>Web Filter: Category is Flagged</td>
<td></td>
<td>Matches if this session is an HTTP session to a flagged category site.</td>
<td>Web Filter</td>
</tr>
<tr>
<td>Directory Connector: Username</td>
<td>Glob Matcher</td>
<td>Matches if this session is from an IP associated with the given username.</td>
<td>Directory Connector</td>
</tr>
<tr>
<td>Directory Connector: User in Group</td>
<td>Glob Matcher</td>
<td>Matches if this session is from an IP associated with a username in the given group.</td>
<td>Directory Connector</td>
</tr>
<tr>
<td>Client has no Quota</td>
<td></td>
<td>Matches if the client IP has no Quota</td>
<td></td>
</tr>
<tr>
<td>Server has no Quota</td>
<td></td>
<td>Matches if the server IP has no Quota</td>
<td></td>
</tr>
</tbody>
</table>
## Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Priority</td>
<td>Priority</td>
<td>Sets the matching session to the given priority.</td>
</tr>
<tr>
<td>Send Client to Penalty Box</td>
<td>Priority, Penalty</td>
<td>Sets the matching session's client IP to the penalty box for the given amount of time with a given penalty priority.</td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td></td>
</tr>
<tr>
<td>Apply Penalty Priority</td>
<td>n/a</td>
<td>Applies the penalty priority for the session's IP penalty box entry.</td>
</tr>
<tr>
<td>Give Client a Quota</td>
<td>Quota Expiration,</td>
<td>Gives the matching session's client IP a quota of the given size that expires in the given time.</td>
</tr>
<tr>
<td></td>
<td>Quota Size</td>
<td></td>
</tr>
</tbody>
</table>

## Priorities

There are 7 Priorities: Very High, High, Medium, Low, Limited, Limited More, Limited Severely. The overall effect of bandwidth control is to map traffic to these priorities which are enforced by the QoS engine.

The first four priorities can be thought of as "normal" priorities: Very High, High, Medium, and Low. They are given certain precedence over bandwidth rights. Very High traffic has the option to consume bandwidth before High, Medium, and Low. The Very High bucket will be assigned the largest amount of bandwidth, less to High, even less to Medium, and much less to Low.

The other three priorities, Limited, Limited More, and Limited Severely, are even lower and are different in that they will never use all the bandwidth even if there is more bandwidth available. The classes are punitive because they will limit bandwidth under all scenarios.

To read much more in depth about the effects of prioritization and how bandwidth allotment works read QoS#QoS_Priorities.

## Penalty Box

The Penalty Box tab shows the users currently in the "Penalty Box." The word "Penalty Box," sometimes called the sin bin, comes from the sports hockey, rugby, and others. It typically is used when a player breaks a given rule they must go to the penalty box for a length of time.

The same logic is used in the Bandwidth Control Penalty Box. Using the Send Client to Penalty Box action rules can be written to send certain IPs to the penalty box for a
period of time (configurable in the rule) when they break certain rules. Likewise a rule can also be added using the Client in Penalty Box matcher and the Apply Penalty Priority action to punish penalty boxed IPs in the desired fashion. The following screenshot shows a host in the penalty box.

Typical uses for this are hard-to-block and hard-to-control applications like bittorrent. Bittorrent opens many many sessions and usually only some of the sessions get identified as "BitTorrent" sessions.

As instead of just using the "Set Priority" action, you can add that IP to the penalty box with the given priority and then all of that IPs sessions will be given the appropriate priority (assuming you have the appropriate Apply Penalty Priority rule). Please note that you’ll want to Log rather than Block bittorrent in the Protocol Control application since Bandwidth Control will be taking care of the action.

Quotas

The Quotas tab shows the current quotas and statistics about their current status.

Quotas are set amounts of data that can be used over a certain amount of time. This is useful for sites where you want to punish excessive usage. For example, I have a hotel I want each IP to get 1 Gb a day, but if this amount is exceeded it will be considered excessive and that host will receive much less bandwidth.

Quotas are not given on this page, that happens in the rules with the Give Client a Quota action. This allows the rules to run non-stop and perform all the necessary quota-maintenance so they quota operation can become a hands-off operation once configured.
**Refill** can be used to immediately refill the desired Quota, and **Drop** can be used to immediately expire the current quota.

In configurations where quotas are desired, the easiest way to give quotas is to create a rule at the top of the rule list that gives a quota to all desired hosts that currently do not have a quota.

**Note:** You must add the **Client Host has no Quota** matcher otherwise this rule will always match first and no other rules will be evaluated.

This rule will assure that hosts are given quotas the first time they are seen. As a given host downloads and uploads data it is counted against the quota. When the quota is expired the **Client Host has exceeded Quota** matcher will match allowing you to match all sessions for those that have exceeded quotas.
A rule (just below the first rule) to give all quota exceeded hosts to a Limited priority will mean that once a host exceeds its quota all of its sessions get the Limited priority (and the hosts gets less bandwidth until the quota expires.)

Using quotas and rules bandwidth abusers are handled completely automatically and requires no administrator intervention.

**Event Logs**

Bandwidth Control provides three event logs: #Prioritize Event Log and #Penalty Box Event Log and #Quota Event Log.

**Prioritize Event Log**

This log shows the prioritization of sessions.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The assigned priority</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that assigned the priority</td>
</tr>
<tr>
<td>Client</td>
<td>The client IP:port</td>
</tr>
<tr>
<td>Server</td>
<td>The server IP:port</td>
</tr>
</tbody>
</table>

**Penalty Box Event Log**

This log shows the penalty box related events.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The address associated with this event</td>
</tr>
<tr>
<td>Action</td>
<td>Enter if the address was added to the penalty box, Exit if the address is leaving the penalty box.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that matched to cause this event (for Enter actions only)</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the penalty (for Enter actions only)</td>
</tr>
</tbody>
</table>
Quota Event Log

This log shows the quota related events.

<table>
<thead>
<tr>
<th><strong>Timestamp</strong></th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>The address associated with this event</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Quota Given or Quota Exceeded</td>
</tr>
<tr>
<td><strong>Rule</strong></td>
<td>The rule that matched to cause this event (for Quota Given actions only)</td>
</tr>
<tr>
<td><strong>Quota Size</strong></td>
<td>The original size of the quota</td>
</tr>
</tbody>
</table>

Bandwidth Control FAQs

**Why are the rules evaluated on the first ten packets of a session?**

Often rules involve session "meta-data" such as HTTP-Hostname or Protocol-Control-Signature. These meta-data tags are usually completed fairly quickly (first few packets) but they are usually not known until the first few packets. As such the session is evaluated initially and the next 9 packets. This is to ensure that all rules that involve meta-data have a chance to fire. After the first ten packets the meta-data typically does not change and the rules are no longer consulted.

**Dropping a Quota does not seem to work. Why?**

If you have a rule set to give quotas automatically if a host doesn't have a quota it is probably being given a new quota again very quickly which gives the appearance that you can't delete the quota.

**Does Bandwidth Control work with PPPoE?**

No. PPPoE uses a special interface and is not supported by Bandwidth Control (nor QoS).
Kaspersky Virus Blocker
Kaspersky Virus Blocker protects your network against viruses - it took top honors at Untangle’s AV Fight club (virus.untangle.com) last August and has been recognized by leading industry publications. As you know, viruses arrive over the network using several techniques, so Kaspersky Virus Blocker scans many protocols for the presence of viruses in traffic:

- Email: SMTP, POP, IMAP
- Web: HTTP
- File Transfer: FTP

Why Two Virus Blockers?

Virus Blocker and Kaspersky Virus Blocker complement each other. These two particular solutions together are better than either one alone because they have different engines and virus signature formulations. Most traditional virus blockers use similar engine technology, and so they tend to be redundant rather than complimentary. Different engines can catch viruses that each other might miss. As an analogy, if you have two police departments that employ different techniques to look for criminals, the odds of catching more criminals increases.

Settings

This section reviews the different settings and configuration options available for the virus scanner.

Web Settings

This section reviews the different settings and configuration options for web traffic.

To change virus scanning of web traffic:

1. From Virus Blocker or Kaspersky Virus Blocker, click the Show Settings tab.
2. Specify the HTTP settings:
   a. Click the Web tab.
   b. Select the Scan HTTP check box, then click the Advanced Settings hotspot.
3. Specify the file types that you want to scan:
   a. Click the File Extensions button.
   b. Select the scan check box for each file type that you want to scan, then click Save.
4. Specify the MIME types that you want to scan:
   a. Click the MIME Types button.
   b. Select the scan check box for each MIME type that you want to scan, or click the add (+) button and add your own MIME type, then click Save.

5. Click OK or Apply.

6. (Optional) You can add .htm, .html, .js (javascript) and .css to the default File Extension list, since by default these file types (web extensions) are not included in the default File Extension list. You must add them to the File Extension List if you wish to have them scanned as well.
   a. Click the File Extension button.
   b. For each file type, select the add (+) button, and add the file type, then click Done.
   c. Click Save.

Advanced Settings

- **Disable HTTP Resume**: The HTTP protocol has an advanced feature where an interrupted file download may be resumed (restarted) where it left off. Although a handy feature for unreliable networks, the Untangle Server is unable to perform virus scans when this feature is enabled. When HTTP download resume is permitted, it is possible that a file containing a virus could be received over multiple connections. When this occurs, the Untangle Server only sees parts of the file at once and cannot know if it contained a virus.

- **Scan Trickle Rate**: This is an advanced feature, controlling how quickly files are downloaded relative to scanning. **Caution**: As an advanced feature, you should not change this value unless instructed to by a member of Untangle Technical Support or one of their authorized representatives.

Email Settings

This section reviews the different settings and configuration options for email traffic.

To change virus scanning of email:

1. From Virus Blocker or Kaspersky Virus Blocker, click the Show Settings tab.
2. Click the Email tab.
3. Select the Scan check box for the type of email that your company uses.

<table>
<thead>
<tr>
<th>Scan SMTP/POP3/IMAP</th>
<th>When the check box is selected, the Untangle Server scans email for viruses in both directions unless there is a custom policy that overrides these instructions.</th>
</tr>
</thead>
</table>
If you have a local Microsoft Exchange Server, click the SMTP tab.

If you use Outlook to download web mail, click the POP tab.

If you use a rare, IMAP email client, click the IMAP tab.

If Untangle Server detects a virus:

- **pass message.** Sends email without removing the virus.
- **remove infection.** Removes the virus without changing any user data.
- **block message.** Blocks the email without removing the virus.

4. Click the **Save** button.

**FTP Settings**

This section reviews the different settings and configuration options for FTP traffic.

**To change virus scanning of file transfers:**

1. From Virus Blocker or Kaspersky Virus Blocker, click the **Show Settings** tab.
2. Click the **FTP** tab.
3. Select the **scan** check box, and click the **Save** button.

**Advanced Settings**

- **Disable FTP Resume:** The FTP protocol has an advanced feature that allows an interrupted file download to be resumed (restarted) where the download ended. Although a handy feature for unreliable networks, the Untangle Server cannot scan a file transfer for viruses when this feature is enabled. When FTP download resume is permitted, a file containing a virus could be transmitted over multiple connections and the Untangle Server will only see parts of the file and be unable to perform a complete scan.

- **Scan Trickle Rate:** This is an advanced feature, controlling how quickly files are downloaded relative to scanning. **Caution:** As an advanced feature, you should not change this value unless instructed to by a member of Untangle Technical Support or one of their authorized representatives.
Event Log

Use the following terms and definitions to understand the virus scanner Event Log:

<table>
<thead>
<tr>
<th><strong>timestamp</strong></th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>The action taken on the document (HTTP response, FTP file, or email). The value depends on the mail protocol, but will contain descriptive text such as block, mark, etc.</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>The client IP Address of the protocol client. For SMTP this is the sender of the mail, and for IMAP/POP the receiver of the mail. For HTTP this is the address of the client browser machine. For FTP, this is the address of the machine receiving files.</td>
</tr>
<tr>
<td><strong>traffic</strong></td>
<td>This is a descriptive field identifying the type of traffic (HTTP, mail, etc).</td>
</tr>
<tr>
<td><strong>reason for action</strong></td>
<td>The reason the action was taken.</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>The server's IP address. For SMTP this is the machine receiving the email, and for IMAP/POP the machine holding the inbox. For HTTP this is the address of the server machine sending the document. For FTP this is the address of the machine transmitting the files being downloaded.</td>
</tr>
</tbody>
</table>

Kaspersky Virus Blocker FAQs

**How do Untangle Server's Virus Blockers compare to "brand-name" virus blockers?**

According to an independent evaluation, Virus Blocker "beats the pants off its commercial competition".

**If I use the Untangle Server, do I need to install virus software on individual network computers?**

If you have Untangle's Virus Blockers running on the Untangle Server, the Untangle Server scans all inbound and outbound email traffic that goes *through* the Untangle Server. This protection is your first layer of protection. Imagine this scenario:

Angela is a Resume Writer at Angelic Resumes, Inc. One day she works from a remote location, and downloads an infected file from the Internet to her personal laptop, then to her USB drive. She returns to the office the next day, and, using the USB drive, saves the infected file directly to her desktop computer. Her desktop computer is now infected with a virus. To make matters worse, she emails that file to her coworkers. Her coworkers download the file, and now their desktops are also infected.
In this scenario the file was transferred without going through the Untangle Server. If Angela had emailed the file to her coworkers work email accounts from her personal email account, that email would have passed through the Untangle Server, and the Untangle Server would have prevented the virus from entering your protected network.

You cannot fully ensure that all traffic enters and exits your Untangle Server, Untangle recommends an additional layer of protection. Consider installing anti-virus software on all network desktops and laptops.

**For Email, why is blocking (or quarantining) of emails when a virus is detected not always an option?**

Only the SMTP protocol allows the Untangle Server to block email messages. The details of the POP and IMAP protocols do not allow the Untangle Server to block or quarantine email messages.

**When configuring my Untangle Server to mark virus emails received over IMAP, the subject of the mails changes to [VIRUS]... only after I click on the message. Why?**

Most IMAP clients first fetch summary information about emails (subject, sender) so the end user can see a preview list of messages. Only when the user selects (clicks on) the message is the actual content of the message retrieved from the server and the Untangle Server is able to scan the message. Unfortunately, some email clients do not detect the change in subject and update their preview list when the Untangle Server marks the message.

**What happens to virus hoaxes?**

Spam Blocker, not Virus Blocker or Kaspersky Virus Blocker, blocks virus hoaxes because this type of email is spam, and does not carry an actual virus.

**If I have both virus blockers installed, are one or both used and in which order?**

If you have both virus scanners installed, KAV is applied to a message first: if a message passes KAV, then and only then is Virus Blocker applied to the message (there’s no point in scanning the message twice if the first scanner has rejected it.) This is not to say one scanner is inherently better than the another: note that KAV is complemented by Virus Blocker and in the case of a virus-free message, the computational overhead of the virus scan includes both scanners; where as a message that would be rejected by both scanners incurs the computational and time cost of just KAV. To perform a valid comparison, you should run test messages through the Untangle Gateway with no scanners installed, KAV by itself, the Virus Blocker by itself and lastly both scanners installed together and compare the results.

**How can I test that viruses are being blocked?**

An easy way to test HTTP virus scanning is to download the eicar test from a machine behind Untangle. If virus scanning is not working the file will download successfully (it is harmless). If it is working a block page will be displayed.
Why does the Event Log say this file is blocked, but I can still download it?

When downloading over the web small files are blocked with a block page. Larger files are treated differently. They are fed to the client at a slower rate than they are actually downloaded so the client does not time out while the download happens. After Untangle scans the complete file it will either refuse to send the rest if there is a virus or immediately send the rest. This means for large files the event log says the file is "blocked" then checking the file size on the client will show that you do not actually have the complete file.

Emails with larger attachments somehow dissapear or are not delivered. Why?

While Untangle is scanning attachments your email server is still waiting for the message, most likely triggering a timeout setting. If you're using MS Exchange, you'll want to increase the ConnectionInactivityTimeout setting.
**Virus Blocker**

Virus Blocker is based on an open-source virus scanner, Clam AntiVirus. Clam AntiVirus is well-known for its speed and accuracy. If fact, according to an independent evaluation, Clam "beats the pants off its commercial competition".

Virus Blocker does the following:

- Detects viruses, worms, and trojan horses.
- Scans within archives and compressed files: Zip, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet Files, MS CHM, and MS SZDD.
- Protects against an archive bomb, a file that is repeatedly compressed. Such a file causes virus scanners or other programs to crash or hang by consuming all CPU resources. Intensive resource consumption occurs when the virus scanner scans numerous levels of files within files.

**Settings**

This section reviews the different settings and configuration options available for the virus scanner.

**Web Settings**

This section reviews the different settings and configuration options for web traffic.

**To change virus scanning of web traffic:**

1. From Virus Blocker or Kaspersky Virus Blocker, click the **Show Settings** tab.
2. Specify the HTTP settings:
   a. Click the **Web** tab.
   b. Select the **Scan HTTP** check box, then click the **Advanced Settings** hotspot.
3. Specify the file types that you want to scan:
   a. Click the **File Extensions** button.
   b. Select the **scan** check box for each file type that you want to scan, then click **Save**.
4. Specify the MIME types that you want to scan:
   a. Click the **MIME Types** button.
   b. Select the **scan** check box for each MIME type that you want to scan, or click the add (+) button and add your own MIME type, then click **Save**.
5. Click **OK** or **Apply**.
6. (Optional) You can add .htm, .html, .js (javascript) and .css to the default File Extension list, since by default these file types (web extensions) are not included in the default File Extension list. You must add them to the File Extension List if you wish to have them scanned as well.
   
a. Click the File Extension button.
   
b. For each file type, select the add (+) button, and add the file type, then click Done.
   
c. Click Save.

Advanced Settings

- **Disable HTTP Resume**: The HTTP protocol has an advanced feature where an interrupted file download may be resumed (restarted) where it left off. Although a handy feature for unreliable networks, the Untangle Server is unable to perform virus scans when this feature is enabled. When HTTP download resume is permitted, it is possible that a file containing a virus could be received over multiple connections. When this occurs, the Untangle Server only sees parts of the file at once and cannot know if it contained a virus.

- **Scan Trickle Rate**: This is an advanced feature, controlling how quickly files are downloaded relative to scanning. **Caution**: As an advanced feature, you should not change this value unless instructed to by a member of Untangle Technical Support or one of their authorized representatives.

Email Settings

This section reviews the different settings and configuration options for email traffic.

To change virus scanning of email:

1. From Virus Blocker or Kaspersky Virus Blocker, click the Show Settings tab.
2. Click the Email tab.
3. Select the Scan check box for the type of email that your company uses.

<table>
<thead>
<tr>
<th>Scan SMTP/POP3/IMAP</th>
<th>When the check box is selected, the Untangle Server scans email for viruses in both directions unless there is a custom policy that overrides these instructions.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>o If you have a local Microsoft Exchange Server, click the SMTP tab.</td>
</tr>
<tr>
<td></td>
<td>o If you use Outlook to download web mail, click the POP tab.</td>
</tr>
<tr>
<td></td>
<td>o If you use a rare, IMAP email client, click the</td>
</tr>
</tbody>
</table>
### FTP Settings

This section reviews the different settings and configuration options for FTP traffic.

**To change virus scanning of file transfers:**

1. From Virus Blocker or Kaspersky Virus Blocker, click the **Show Settings** tab.
2. Click the **FTP** tab.
3. Select the **scan** check box, and click the **Save** button.

### Advanced Settings

- **Disable FTP Resume**: The FTP protocol has an advanced feature that allows an interrupted file download to be resumed (restarted) where the download ended. Although a handy feature for unreliable networks, the Untangle Server cannot scan a file transfer for viruses when this feature is enabled. When FTP download resume is permitted, a file containing a virus could be transmitted over multiple connections and the Untangle Server will only see parts of the file and be unable to perform a complete scan.

- **Scan Trickle Rate**: This is an advanced feature, controlling how quickly files are downloaded relative to scanning. **Caution**: As an advanced feature, you should not change this value unless instructed to by a member of Untangle Technical Support or one of their authorized representatives.
## Event Log

Use the following terms and definitions to understand the virus scanner Event Log:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>action</td>
<td>The action taken on the document (HTTP response, FTP file, or email). The value depends on the mail protocol, but will contain descriptive text such as block, mark, etc.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP Address of the protocol client. For SMTP this is the sender of the mail, and for IMAP/POP the receiver of the mail. For HTTP this is the address of the client browser machine. For FTP, this is the address of the machine receiving files.</td>
</tr>
<tr>
<td>traffic</td>
<td>This is a descriptive field identifying the type of traffic (HTTP, mail, etc).</td>
</tr>
<tr>
<td>reason for action</td>
<td>The reason the action was taken.</td>
</tr>
<tr>
<td>server</td>
<td>The server’s IP address. For SMTP this is the machine receiving the email, and for IMAP/POP the machine holding the inbox. For HTTP this is the address of the server machine sending the document. For FTP this is the address of the machine transmitting the files being downloaded.</td>
</tr>
</tbody>
</table>
Virus Blocker FAQs

How do Untangle Server’s Virus Blockers compare to "brand-name" virus blockers?

According to an independent evaluation, Virus Blocker "beats the pants off its commercial competition".

If I use the Untangle Server, do I need to install virus software on individual network computers?

If you have Untangle’s Virus Blockers running on the Untangle Server, the Untangle Server scans all inbound and outbound email traffic that goes through the Untangle Server. This protection is your first layer of protection. Imagine this scenario:

Angela is a Resume Writer at Angelic Resumes, Inc. One day she works from a remote location, and downloads an infected file from the Internet to her personal laptop, then to her USB drive. She returns to the office the next day, and, using the USB drive, saves the infected file directly to her desktop computer. Her desktop computer is now infected with a virus. To make matters worse, she emails that file to her coworkers. Her coworkers download the file, and now their desktops are also infected.

In this scenario the file was transferred without going through the Untangle Server. If Angela had emailed the file to her coworkers work email accounts from her personal email account, that email would have passed through the Untangle Server, and the Untangle Server would have prevented the virus from entering your protected network.

You cannot fully ensure that all traffic enters and exits your Untangle Server, Untangle recommends an additional layer of protection. Consider installing anti-virus software on all network desktops and laptops.

For Email, why is blocking (or quarantining) of emails when a virus is detected not always an option?

Only the SMTP protocol allows the Untangle Server to block email messages. The details of the POP and IMAP protocols do not allow the Untangle Server to block or quarantine email messages.

When configuring my Untangle Server to mark virus emails received over IMAP, the subject of the mails changes to [VIRUS]... only after I click on the message. Why?

Most IMAP clients first fetch summary information about emails (subject, sender) so the end user can see a preview list of messages. Only when the user selects (clicks on) the message is the actual content of the message retrieved from the server and the Untangle Server is able to scan the message. Unfortunately, some email clients do not detect the change in subject and update their preview list when the Untangle Server marks the message.
What happens to virus hoaxes?

Spam Blocker, not Virus Blocker or Kaspersky Virus Blocker, blocks virus hoaxes because this type of email is spam, and does not carry an actual virus.

If I have both virus blockers installed, are one or both used and in which order?

If you have both virus scanners installed, KAV is applied to a message first: if a message passes KAV, then and only then is Virus Blocker applied to the message (there's no point in scanning the message twice if the first scanner has rejected it.) This is not to say one scanner is inherently better than the other: note that KAV is complemented by Virus Blocker and in the case of a virus-free message, the computational overhead of the virus scan includes both scanners; where as a message that would be rejected by both scanners incurs the computational and time cost of just KAV. To perform a valid comparison, you should run test messages through the Untangle Gateway with no scanners installed, KAV by itself, the Virus Blocker by itself and lastly both scanners installed together and compare the results.

How can I test that viruses are being blocked?

An easy way to test HTTP virus scanning is to download the eicar test from a machine behind Untangle. If virus scanning is not working the file will download successfully (it is harmless). If it is working a block page will be displayed.

Why does the Event Log say this file is blocked, but I can still download it?

When downloading over the web small files are blocked with a block page. Larger files are treated differently. They are fed to the client at a slower rate than they are actually downloaded so the client does not time out while the download happens. After Untangle scans the complete file it will either refuse to send the rest if there is a virus or immediately send the rest. This means for large files the event log says the file is "blocked" then checking the file size on the client will show that you do not actually have the complete file.

Emails with larger attachments somehow disappear or are not delivered. Why?

While Untangle is scanning attachments your email server is still waiting for the message, most likely triggering a timeout setting. If you're using MS Exchange, you'll want to increase the ConnectionInactivityTimeout setting.
**Intrusion Prevention**

Intrusion Prevention is an ID (Intrusion Detection) system that intercepts all traffic and detects malicious activity on either the network or individual computers or both. To detect malicious activity, Intrusion Prevention uses signature detection, a method that draws upon a database of known attack patterns. Intrusion Prevention's interception of malicious activity does not have any impact on system performance and is transparent to users, with the exception of the malicious user. If Intrusion Prevention detects malicious activity, the session for that activity is terminated.

Intrusion Prevention is pre-configured with reasonable defaults. Because of this it does not require much customization, though you can change these defaults or add your own rules, as Blocking or Logging using Intrusion Prevention Rules shows.

**Settings**

This section reviews the different settings and configuration options available for Intrusion Prevention.

**Status**

The Status tab simply shows you information about Intrusion Prevention's definitions - there is nothing to configure.

**Rules**

Intrusion Prevention provides a list of rules (signatures) that you can block, log, or ignore. To make things easy for you, Untangle evaluated each rule and numerous networks, and determined the appropriate default settings for each rule using the following criteria:

- If the rule is *always* known to block malicious exploits, Intrusion Prevention blocks and logs this rule by default.
- If the rule is *sometimes* known to block malicious exploits, Intrusion Prevention logs this rule by default.
- If the rule is *never* known to block malicious exploits, Intrusion Prevention neither blocks nor logs this rule by default.

In most cases, you do not need to change the default settings. You should only need to disable a rule if that rule blocks traffic from a unique software application that you must use.

- If you block a rule, Intrusion Prevention enables the rule and blocks traffic that matches the rule signature.
- If you log a rule, Intrusion Prevention logs traffic that matches the rule signature.
To block or log a rule:

1. From Intrusion Prevention, click the **Show Settings** tab.
2. Click the **Rules** tab.
3. In the Rules table, select the **block** or **log** check box for the rules that you want to block or log or both.
4. Click either the **OK** or **Apply** button.

**About Rule Variables**

Intrusion Prevention provides a list of default rules that block exploits. There are also rule variables that provide additional instructions for these rules. These rules are called *Snort variables*. These variables are used in rules to specify criteria for the source and destination of a packet. Snorts most important variable is `$HOME_NET`. `$HOME_NET` defines the network or networks you are trying to protect.

Under no circumstance should you change or delete these exceptions. You can add exceptions, but only if you are very familiar with Snort variables and the `snort.conf` configuration file.

**To view rule variables:**

1. From Intrusion Prevention, click the **Show Settings** button.
2. Click the **Rules** tab.
3. Scroll down to the **Variables** table. This table contains all the rule exceptions.

**Learning More About Signature ID Rules**

Intrusion Prevention is based on http://www.snort.org. If you want to learn more about the exploits that Intrusion Prevention blocks or the signature IDs (SIDs) that Intrusion Prevention uses, do one of the following:

- From Intrusion Prevention, click the **Rules** tab, then, for a give rule, click the **info** link in the info column. A web page launches, providing you more information about the exploit.
Blocking or Logging an Intrusion Prevention Rule.

- If a rule in Intrusion Prevention state no info in the info column, then search for the SID on snort.org's website as shown in Searching snort.org for SID Rules. A SID is a numeric number; you can locate the SID in the id column of Intrusion Prevention.

Searching snort.org for SID Rules
Event Log

Use the following terms and definitions to understand the Intrusion Prevention Event Log:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>action</td>
<td>The action that was taken on the traffic. Valid values are block and pass.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP address of the traffic.</td>
</tr>
<tr>
<td>reason for action</td>
<td>The rule that was applied to the traffic.</td>
</tr>
<tr>
<td>server</td>
<td>The intended server IP address of the traffic.</td>
</tr>
</tbody>
</table>

Intrusion Prevention FAQs

Why aren’t most of Intrusion Prevention’s rules blocked by default?

Because most of the rules can block non-malicious traffic in addition to malicious exploits. To make things easy for you, Untangle evaluated each rule and numerous networks, and determined the appropriate default settings for each rule using the following criteria:

- If the rule is **always** known to block malicious exploits, Intrusion Prevention blocks and logs this rule by default.
- If the rule is **sometimes** known to block malicious exploits, Intrusion Prevention logs this rule by default.
- If the rule is **never** known to block malicious exploits, Intrusion Prevention neither blocks nor logs this rule by default.

To change the defaults, go to Blocking or Logging using Intrusion Prevention Rules.
Protocol Control
Protocol Control uses an open-source tool, L7-filter. Protocol Control blocks and logs well-known protocols from entering or leaving your protected network. Unwanted protocols might include Peer-to-Peer (P2P), such as Bittorrent, and Instant Messaging, such as AOL Instant Messenger. You might also want to block users from playing some video games and from streaming media.

Protocol Control blocks unwanted protocols on any port. However, you must specify which protocols that you want Protocol Control to block and log. By default Protocol Control does not block any protocols; it simply logs Instant Messaging protocols.

Protocol Control uses signatures to identify unwanted protocols on all ports. Many protocols, such as Instant Messaging and Peer-to-Peer, are difficult to block with a traditional firewall because of their "port hopping" behavior. If clients are blocked after trying to connect through their default port, they will connect over port 80 or port 25. Port 80 and port 25 cannot be blocked without blocking Web and e-mail traffic. Protocol Control can identify this hopping behavior, and log and block the connections.

If Protocol Control does not support a protocol that you want to block, you can use the Untangle Server's user interface to create custom new rules to block unsupported protocols. However, not all protocols can be blocked because some protocol designers hide the protocol's signature (for example, Skype).

Settings
This section reviews the different settings and configuration options available for Protocol Control.

Protocol List
You can choose to block traffic that uses a specific protocol from either entering or leaving your protected network. Protocol Control lists most well-known protocols. You can also log such traffic in the Protocol Control Event Log and have it reported in Reports if, for example, you want to determine if anyone within the network is using a particular protocol such as file sharing.
Monitoring Protocol Usage

Often System Administrators know that their network is slow due to user activity, but don't know what type of network activity is slowing down their network. If this applies to you, Untangle recommends that you first log all protocols, then review the Protocol Control's Untangle Report to determine which protocols cause poor network performance. Bittorrent is frequently the culprit.

**Caution:** As with most Untangle Server's Software Products, you can create your own protocol control entries. However, configuring regular expressions to match Internet protocols is an advanced topic. If you create a new entry set to **Block** and your expression contains errors, legitimate traffic will be blocked.
To block or log a protocol:

1. From Protocol Control, click the **Show Settings** button.

2. Click the **Protocol List** tab.

3. Select the row that corresponds to the protocol that you want to block, and select either the **block** checkbox, **log** checkbox or both.

4. Click either the **OK** or **Apply** button.

**Event Log**

Use the following terms and definitions to understand the Protocol Control Event Log:

<table>
<thead>
<tr>
<th><strong>timestamp</strong></th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>The action that was taken on the traffic. Valid values are block and pass.</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>The client IP address of the traffic.</td>
</tr>
<tr>
<td><strong>request</strong></td>
<td>The protocol of the traffic.</td>
</tr>
<tr>
<td><strong>reason for action</strong></td>
<td>The rule that was applied to the traffic.</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>The intended server IP address of the traffic.</td>
</tr>
</tbody>
</table>
Protocol Control FAQs

How do I add a protocol to Protocol Control?

Protocol Control provides numerous default protocols that you can block, but if you want to block a protocol that Protocol Control doesn't list, you must add that protocol. To add a protocol you must provide Protocol Control the protocol's signature. To determine the signature, you must analyze the packets, and this process can be tricky. Contact Untangle Technical Support to request the signature.

I've already installed the Firewall. Isn't Protocol Control redundant?

The Firewall application works to block traffic for IP addresses and/or ports. For well-behaved applications (such as legitimate web and email servers) the port can be used to identify the protocol. However, less legitimate applications may use different ports, or malicious users may deliberately use unwanted services on obscure ports.

Protocol Control scans all traffic, looking for a match even if traffic was not transported across the expected port for that protocol.

I want to block a file sharing protocol for some of my users but not all. How can I do this with Protocol Control?

The Protocol Control cannot by itself filter just for some machines, and not others. However, you can create new Policies and Virtual Racks (See Policy Management) to partition some of your users through Protocol Control with [some file sharing protocol] blocked and not others.
Firewall
Firewall provides traditional firewall functionality, blocking or logging traffic based on rules. Although the term "Firewall" has grown to encompass many functionalities, the Untangle "Firewall" is a simple traditional firewall used to block traffic. Other functionalities (such as port forwarding or blocking protocols) are in other apps or networking configuration.

Firewall uses a simple list of rules to determine what traffic to block (or log) and what traffic to pass. Each time untangle catches a new session, the list of rules is evaluated in order. Firewall takes the first matching rule and applies the corresponding action stated in that rule.

Rules are based on a combination of the following:

- Traffic Type (Protocol)
- Source Interface
- Destination Interface
- Source Address
- Destination Address
- Source Port
- Destination Port

Settings
Since Firewall rules are different for most networks, the settings will be covered a bit differently from the other applications.

Using Firewall
Using Firewall rules network administrators can construct a rule set that blocks and allows traffic according to their preferences. By default, the default action of the Firewall is set to Pass.

Typically, Untangle is installed as a NAT/gateway device, or behind another NAT/gateway device in bridge mode. In this scenario all inbound sessions are blocked except those explicitly allowed with port forwards. As such, the Firewall application is not needed to filter inbound sessions, but can still be used to tightly control outbound sessions (often called Egress filtering). In cases where inbound sessions are not being blocked the Firewall application can filter those sessions like any other session.
The following are the most common use cases for Firewall.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Everything except Explicitly Allowed Traffic</td>
<td>In this scenario all traffic is blocked except explicitly allowed traffic. This can be the most secure, but can also require higher maintenance and be more problematic for users. To do this simply change the default action to Block then create an explicit rule that allows all traffic you want to pass. Typically this means creating a pass rule for outbound DNS, web traffic and any other protocols, and creating a pass rule for any inbound traffic you may have. (Note: In this scenario, any port forwards must also have accompanying Firewall rules or the Firewall will block that forwarded traffic)</td>
<td>To do this change the default action to <strong>Block</strong> then create an explicit rule that allows all traffic you want to pass. Typically this means creating a pass rule for outbound DNS, web traffic and any other protocols, and creating a pass rule for any inbound traffic you may have. (Note: In this scenario, any port forwards must also have accompanying Firewall rules or the Firewall will block that forwarded traffic)</td>
</tr>
<tr>
<td>Explicitly Block Some Ports or Machines</td>
<td>In this scenario most traffic is passed, but Firewall is being used to explicitly limit some ports or machines from passing certain types of traffic. This is a very commonly used scenario as it provides a good compromise between security and maintenance which suits many organizations.</td>
<td>To do this change the default action to <strong>Pass</strong> and create an explicit rule for traffic that should be blocked.</td>
</tr>
<tr>
<td>Using Firewall for Logging and Information</td>
<td>Another common scenario is to use firewall for debugging and logging information to see what is happening on the network.</td>
<td>To do so, simply set the default action to Pass and then create a rule to log traffic. Using Firewall as a tool can help network administrators see what is going on and save that information in Reports.</td>
</tr>
</tbody>
</table>
Anatomy of a Firewall Rule

Firewall matches the sessions/connections using rules based on traffic criteria. When a new session is caught, the rules are evaluated in order. If all of a session's attributes match all of the criteria of a session it is considered a match. Firewall applies the action of the first matching rule. If no rule matches - the default action is applied.

Each rule matches traffic based on certain criteria which consist of the protocol (traffic type), as well as source and destination interfaces, and source and destination addresses and ports. See the table below for detail values.

**Note:** Firewall matches against connections - not packets. The criteria evaluated are the criteria of the connection. If a connection is passed, all associated packets in a connection will automatically be passed without evaluating the rules.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>The traffic type criteria selects the protocol to be matched. Valid values are TCP, UDP, both TCP &amp; UDP, or any.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Interface</td>
<td>The client's interface. The client is the host that initiates the request. Your choices are any (all), External, DMZ, VPN, Internal, any WAN interface and any non-WAN interface. If one of your interfaces doesn't appear in the list, go to Adding Network Cards or Testing Internet Connection.</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>The server's interface. The server is the host that services the request. Your choices are any (all), External, DMZ, VPN, Internal, any WAN interface and any non-WAN interface. If one of your interfaces doesn't appear in the list, go to Adding Network Cards or Testing Internet Connection.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The IP address of the host which initiated the connection. Addresses are specified in IP Matcher format, which can be simple addresses, address ranges (address-address), or subnets with CIDR (address/subnet) notation.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The IP address of the host which received the connect request. Addresses are specified in IP Matcher format, which can be simple addresses, address ranges (address-address), or subnets with CIDR (address/subnet) notation.</td>
</tr>
<tr>
<td>Source Port</td>
<td>The port of the connection source. Valid values are in Port Matcher format. <strong>WARNING:</strong> Usually the source port is randomly chosen by the sender and will be a value between 0 and 65535. In most rules this should be left as Any.</td>
</tr>
<tr>
<td><strong>Destination Port</strong></td>
<td>The port of the connection destination. Valid values are in Port Matcher format.</td>
</tr>
</tbody>
</table>

**Example: Blocking SSH Traffic on Port 22**

The following example shows a rule that blocks SSH traffic going out the external interface.

**Note:** Although you can use the Firewall to achieve your goal, consider using the Protocol Control. Protocol Control does not require that you know the ports on which applications communicate. Moreover, you don't need to create a rule. You need only select one check box to achieve your goal. Of course, for those that are used to a traditional firewall, Untangle's Firewall offers the typical features, including port blocking.

**Building a Ruleset**

For each new connection the rules are evaluated in order until the first matching rule is found. This allows the administrator to create very detailed firewall policies by carefully ordering the rules. For example if the first rule is to allow SSH traffic from 192.168.1.10 and the next rule is to block all SSH traffic, then the result is that SSH is blocked for all IPs except 192.168.1.10. Rules can be combined in this manner to create fine-grained firewall policies.

Rules can also be easily reordered by dragging the reorder icon on each rule and hitting either the **OK** or **Apply** button.

**Note:** Additionally the Firewall application can be combined with Policy Manager and AD Connector to have different sets of rules apply for different users or even different times of day.
Event Log

Every rule that has "log" checked creates a firewall event. The Firewall Event Log is used to view recent events.

Note: When no rule matches the default action is taken and no event is logged. To log all events then a final rule should be created with the same action as the default action but with the log checkbox checked and all criteria set to "any." This will match all sessions that have not been matched by a previous rule and log them all. It is advised this is only done for debugging purposes as this will log many events.

Use the following terms and definitions to understand Firewall Event Log:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>action</td>
<td>The action that was taken on the traffic. Valid values are block and pass.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP address of the traffic.</td>
</tr>
<tr>
<td>reason for action</td>
<td>The rule that was applied to the traffic.</td>
</tr>
<tr>
<td>server</td>
<td>The intended server IP address of the traffic.</td>
</tr>
</tbody>
</table>
Firewall FAQs

Why doesn’t the Untangle Server’s Firewall have rules enabled by default?

- When the Untangle Server is your router, it is performing NAT. NAT protects you from most threats.
- When the Untangle Server is a bridge, the Untangle Server is already behind a firewall. A firewall protects you from most threats.

The default is pass all?! Why? That’s so insecure!

As explained above, most Untangles are install in router mode meaning that NAT is being performed on traffic. This means all inbound traffic is blocked regardless of the settings in the Firewall app. Only explicitly port forwarded traffic goes inside your network. Alternatively, most bridge mode deployments are installed behind NAT devices so the Firewall app (and Untangle) will only see traffic that’s already explicitly been blessed with a port forward in the external NAT device.

Given this, the "pass all" default really amounts in most scenarios to "block everything inbound, nothing outbound" which is the most common policy for most organizations. Given that most organizations run NAT, most of firewalls utility is for controlling outbound traffic (egress) and rules can easily be added to do that.

Can I have a firewall and still use NetMeeting?

Yes. However, on the Untangle Server, you need to pass specific protocols and open specific ports as outlined in Firewall. A Microsoft article, How to Establish NetMeeting Connections Through a Firewall, explains which protocols to pass and which ports to open.

How do I identify insecure ports?

There are free programs on the Internet that identify insecure ports. More information can be found here.

We currently have a firewall, which lets us do port mapping. I don’t see that feature in your Firewall. Will you be adding it, or is there an alternative?

Port mapping (redirection or port forwarding) is a feature available in Networking configuration. Read more about port forwarding.

I want to lock-down my network but for a few exceptions. What is the best way to do this?

You can set the default behavior to block, as discussed in Anatomy of a Firewall Rule. Then, create a few rules to pass.

Should I use pre-NAT or post-NAT addresses/ports in firewall rules?

Firewall rules always match on the address which has more information. In other words if the entire internal network is being NATd from 192.168.*.* to 1.2.3.4, Firewall will match on the 192.168.*.* for traffic to and from this network. At the session layer this
works out to be pre-NAT on source address, post-NAT on destination address, pre-NAT on source port, and post-NAT on destination port. An easy way to remember this is that it always matches where it gets the most information.

**How do I create a rule to log all traffic, inbound and outbound?**

You will need to create a rule with "any" with log check mark box checked.

| Enable Rule: | ✓ |
| Description: | pass all and log for troubleshooting |
| Action: | Pass |
| Log: | ✓ |

**Rule**

- **Traffic Type:** ANY
- **Source Interface:** any
- **Destination Interface:** any
- **Source Address:** any
- **Destination Address:** any
- **Source Port:** any
- **Destination Port:** any

**How come my firewall rules are not being triggered?**

Firewall rules work from top to bottom. Very first rule that the traffic matches, it will use that rule. So if you have an incorrect rule or a generic rule that the rule is matching, your other rules might not be triggered.
Ad Blocker
Ad Blocker is a service that allows you to block a majority of advertising content that is delivered to users on web pages that they request. Ad Blocker uses downloadable filter subscriptions from a variety of sources which contain lists of web sites and extensions that are typically used to deliver advertising.

Settings
Once Ad Blocker has been downloaded and installed in your rack, it will download its configuration files. The configuration is made up of a large list of web sites and web site extensions that are known to be used for advertising purposes. This list is provided to all users by Untangle, and is updated on a regular basis.

While the default Ad Blocker configuration should work for most users, you may wish to make some adjustments. If you use Untangle and produce web advertising, we will effectively keep you from seeing your own ads. You may also encounter web pages that do not display correctly if the page names chosen by the web site developer are on the list to be blocked.

Status
The Status tab simply shows Ad Blocker’s statistics - there is nothing to configure.

Filters
Ad Blocker’s filter list will populate with many entries to match common ad serving strings, but you are free to add to and edit this list as you see fit.

Blocking a web site or web extension
To unblock specific sites:
1. From Ad Blocker, click the Filters tab.
2. Click the Add button in the upper left and add your new blocking rule.
3. Be careful when selecting blocking criteria as you may block much more content than planned if your criteria is not carefully specified.
4. Remember to save your changes.

Unblocking a web site or web extension
To unblock specific sites:
1. From Ad Blocker, click the Filters tab, and find the rule you would like to modify.
2. Once you find it, either uncheck its Enable checkbox or delete the rule.
3. Remember to save your changes.
Pass Lists

If a web site that users wish to access is being blocked by several different Ad Blocker criteria, you can add the site (or users) to a Pass List.

Passing Specific Sites

To pass specific sites:

1. From Ad Blocker, click the Pass Lists tab, and click the manage list button below Sites.
2. In the table, select the add (+) button. A new row appears.
3. In the IP address/range text box, specify the URL of the site that you want to be exempt from Ad Blocker.
4. Click the Save button.

Passing Specific Users

Before You Begin: It may be useful to assign the user a static IP address. If the Untangle Server is your router, go to Assigning Network Computers Static IP Addresses.

To pass specific users:

1. From Ad Blocker, click the Pass Lists tab, and click the manage list button below Client IP addresses.
2. In the table, select the add (+) button. A new row appears.
3. In the IP address/range text box, specify the computer IP address and subnet mask of user that you want to be exempt from the web filter.
4. Click the Save button.

Event Log

Use the following terms and definitions to understand the Ad Blocker Event Log:

| timestamp | The time the event took place. |
| action    | The action which the Untangle Server took on the web request. |
| client    | IP address of the client who made the request. |
| request   | A description of the request made (e.g. http://someurl/somepath.html). |
| reason for action | The reason the action was taken. |
server | The server IP Address. The server is the computer that receives the request.

Ad Blocker FAQs

How does Ad Blocker keep up with ads?

The list that Ad Blocker uses contains known advertising web sites that are linked off of web pages, as well as known extensions that are used from non-advertising sites. As new advertisers start delivering content, the list is updated. Untangle grabs these updates and makes them available to your server, so that your Ad Blocker is being updated on a regular basis.

My ads do not show up on pages where they're supposed to!

If you are an advertising user, you definitely want to know that your ads are appearing when and where they're supposed to. You'll need to change your Ad Blocker configuration to see your own ads.

Some advertising is getting through. How can I get rid of them?

If the ads persistently get through, you'll need to change your Ad Blocker configuration to do this. You'll either need to block the web site that is delivering the ads, or block the extension. You will need to be very careful when choosing how to block the ads you are concerned with, as you could easily block an entire web site or block the specific method that is used for non-advertising purposes on other websites.
### Service Applications

<table>
<thead>
<tr>
<th>Commtouch Spam Booster</th>
<th>IPsec VPN</th>
<th>Captive Portal</th>
<th>WAN Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN Balancer</td>
<td>Policy Manager</td>
<td>Directory Connector</td>
<td>Attack Blocker</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenVPN</td>
<td>Configuration Backup</td>
<td>Reports</td>
<td></td>
</tr>
</tbody>
</table>
Commtouch Spam Booster

Commtouch Spam Booster is an add-on product that works in conjunction with Untangle's Spam Blocker to increase its effectiveness. It is not a replacement for Spam Blocker. If you intend to use Commtouch Spam Booster, you must use Spam Blocker as well. It is designed to detect and process spam that comes in text files as well as graphics files, and it is not limited by language. It will serve you whether your spam comes in English, Spanish, or Cyrillic.

Settings

There are no user-configurable settings for Commtouch Spam Booster: it simply works! You may adjust thresholds and spam handling characteristics in Spam Blocker, but Commtouch Spam Booster does not require any user intervention.

Commtouch Spam Booster FAQs

How does it work?

Commtouch Spam Booster installs as a plug-in to Spam Blocker. As Spam Blocker processes messages for spam, it will also send most of the messages to the Commtouch Spam Booster plug-in. Commtouch will then check the message against its internet-based spam database, and a test result is returned to Spam Blocker. Based on this result, messages that may have been passed by Spam Blocker may be reclassified as spam, and will be handled according to your Spam Blocker configuration. In addition, messages that may have been incorrectly categorized as spam by Spam Blocker (false positives) will now be passed through.

Not all messages are sent to Commtouch Spam Booster for further processing. Messages that are obviously spam do not require further processing. This is the only type of message that would be processed only by Spam Blocker.

Is there a specific order in which Spam Blocker and Commtouch Spam Booster must be installed?

No. You may install Spam Blocker, then Commtouch Spam Booster, or you may install both at the same time by installing just Commtouch Spam Booster. Commtouch Spam Booster will automatically install Spam Blocker if it is not already installed.

Does Spam Blocker still work if Commtouch Spam Booster is turned off?

Yes, but it does not gain the added effectiveness that Commtouch Spam Booster provides.

I uninstalled Spam Booster by accident. Does that cause problems with Spam Blocker?

No. Spam Blocker will work fine without it, but it will work better with it.

I was using Commtouch Spam Booster in trial mode and it expired. What impact does that have?
Same as turning it off or uninstalling it. Spam Blocker will still work fine, but you lose the added effectiveness of Commtouch Spam Booster.

**If this makes Spam Blocker more effective, doesn’t that increase the risk of false positives?**

No. It actually is the opposite of that. Messages are able to be tested against a wider cross-section of messages, which means that they can be more accurately categorized.

**What are Boost Messages?**

These are messages that Commtouch Spam Booster classified as spam that would not otherwise have been classified as spam with just Spam Blocker. In other words, this is the extra spam that Commtouch Spam Booster is classifying.

**Will this block spam that comes in audio files?**

Spammers depend on being able to send as many messages as possible to be able to make money. They would not use audio files just because of the file size needed for their message.

**Will this slow down processing of mail?**

No. As Spam Blocker passes messages, it will send those not marked as spam on to Commtouch Spam Booster. The stream continues flowing until all messages have been processed. The only delays encountered would be the additional overhead of the first message being submitted to Commtouch, and the last message returned from Commtouch.

**Will this eliminate backscatter mail messages that we receive?**

No. Backscatter messages are legitimate messages, though they also may be used by spammers to get their message into your inbox.

**Why don’t the number of Spams and Non-Spams add up to the number of Scanned Messages?**

This is something that you may see when looking at the faceplate of Commtouch Spam Booster. The number of scanned messages will be larger, the difference between the two numbers comes from messages that rarely occur are not displayed in the counter (an example is a malformed message). Because Spam Booster is installed as a service, the number of Scanned Messages is for all racks combined. This applies when you are using Policy Manager in your Untangle server.

**Why does Spam Blocker show a larger number of messages scanned than does Commtouch Spam Booster?**

If Spam Blocker can clearly determine that a message is spam, there is no need for Spam Booster to provide a second opinion. You are most concerned about the messages that Spam Blocker is unsure about.
IPsec VPN
The IPsec VPN service provides secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

Settings
This section describes the settings of IPsec VPN.

IPsec Options
The IPsec Options tab includes settings that are common to all IPsec connections.

NAT Traversal
The IPsec protocol not only protects the data in a packet, it also protects the packet header which ensures the authenticity and security of all data transmitted across the tunnel. NAT, or network address translation, works by rewriting the source IP address to be that of the gateway, which breaks the IPsec security chain. The NAT Traversal checkbox can be used to enable a workaround that allows IPsec to encode additional information into each packet, keeping the security chain intact when the Untangle is behind a NAT device.

IPsec Tunnels
The IPsec Tunnels tab is where you create and manage the IPsec VPN configuration. The main tab display shows a summary of all IPsec tunnels that have been created.

Tunnel Editor
When you create a new tunnel, or edit and existing tunnel, the tunnel editor screen will appear with the following configurable settings:

<table>
<thead>
<tr>
<th>Enable</th>
<th>This checkbox allows you to set a tunnel to either enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This field should contain a short name or description.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>This field allows you to set the connection type to any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select Tunnel to specify a host-to-host, host-to-subnet, or subnet-to-subnet tunnel. This is by far the most common connection type.</td>
</tr>
<tr>
<td></td>
<td>• Select Transport to specify a host-to-host transport mode tunnel. This connection type is much less common, and would generally only be used if you are attempting to establish and IPsec connection to another host which specifically requires this mode.</td>
</tr>
<tr>
<td></td>
<td>• Select Passthrough to disable IPsec processing on packets associated with the tunnel. We can't imagine a scenario where you would use this connection type. I mean seriously, if you</td>
</tr>
</tbody>
</table>
don't allow IPsec to process the packets then you don't really have a tunnel, right? Still, the underlying protocol supports this mode, and so here we are.

- Select Drop to cause the kernel to drop IPsec packets associated with the tunnel.
- Select Reject to cause the kernel to reject IPsec packets associated with the tunnel.

<table>
<thead>
<tr>
<th>Auto Mode</th>
<th>This field controls how IPsec manages the corresponding tunnel when the IPsec process re-starts, such as when the server boots or when you make changes to the IPsec configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Select Start to have the tunnel automatically loaded, routes inserted, and connection initiated.</td>
</tr>
<tr>
<td></td>
<td>- Select Add to have the tunnel load in standby mode, waiting to respond to an incoming connection request.</td>
</tr>
<tr>
<td></td>
<td>- Select Ignore to have the IPsec process ignore the tunnel completely.</td>
</tr>
<tr>
<td></td>
<td>- Select Route to load the tunnel and insert the routes only. This would only be used for special routing cases.</td>
</tr>
<tr>
<td></td>
<td>- Select Manual to indicate the tunnel will be controlled manually. You probably don't want to select this option, since there isn't really a way to manually control IPsec tunnels on the Untangle appliance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>This field allows you to select the network interface that should be associated with the IPsec tunnel on the Untangle server. When you select a valid interface, the Local IP field (see below) will automatically be configured with the corresponding IP address. If for some reason you want to manually configure an IP address that is not currently active, you can set the Interface to Custom and manually input the IP address below.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>External IP</th>
<th>Use this field to configure the IP address that is associated with the IPsec VPN on the Untangle server. Normally this field will be read-only and will automatically be populated based on the Interface selected above. If you select Custom as the interface, you can then manually enter the local IP address.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Remote IP</th>
<th>This field should contain the public IP address of the host to which the IPsec VPN will be connected.</th>
</tr>
</thead>
</table>

<p>| Local       | This field is used to configure the local network that will be reachable                                                        |</p>
<table>
<thead>
<tr>
<th>Network</th>
<th>from hosts on the other side of the IPsec VPN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP</td>
<td>This field is used to configure the IP address of the Untangle server on the network configured in the Local Network field.</td>
</tr>
<tr>
<td>Remote Network</td>
<td>This field is used to configure the remote network that will be reachable from hosts on the local side of the IPsec VPN.</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>This option causes the IPsec protocol to regenerate the encryption seed data every time the tunnel encryption keys are refreshed, increasing the overall security of the encrypted data.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>This field should contain the shared secret or PSK (pre-shared key) that is used to authenticate the connection, and must be the same on both sides of the tunnel for the connection to be successful. Because the PSK is actually used as the encryption key for the session, using long strings of a random nature will provide the highest level of security.</td>
</tr>
</tbody>
</table>

**Event Logs**

**IPsec State**

The IPsec State tab allows you to see the status of all established IPsec connections. There will typically be two entries per tunnel, one with details about the local side of the connection, and another with details about the remote side of the connection.

**IPsec Policy**

The IPsec Policy tab allows you to see the routing table rules associated with each IPsec VPN that is active.

**IPsec Log**

The IPsec Log tab allows you to see the low level status messages that are generated by the underlying IPsec protocol components. This information can be very helpful when attempting to diagnose connection problems or other IPsec issues.
IPSEC VPN FAQS

What’s the difference between tunnel and transport mode?

When using **tunnel** mode, you can think of the payload packet as being completely encased in another packet. In addition, IPsec can allow or deny packets access to the tunnel depending on policies. When using **transport** mode, communication is limited between two hosts. Only one IP header is present, with the rest of the packet being encrypted. Unless you have very specific needs, you'll most likely want to use **tunnel** mode.

What devices can I connect to with Untangle’s IPsec VPN?

We have currently verified that IPsec VPN can successfully connect to other Untangle boxes and pfSense - we're currently testing with other devices (m0n0wall, Sonicwall, etc) and will update this space as needed.

If I install Untangle behind a NAT device, what do I need to forward to Untangle for IPsec VPN to connect?

You will need to forward ESP, AH, and UDP port 500 from the public IP to the Untangle server. You may also need to enable NAT traversal. However, it is recommended to give Untangle a public IP.

Can I use IPsec on a server that uses DHCP to get its external address?

It is recommended use IPsec VPN on Untangle servers configured with static IPs. However, technically it can work with DHCP, but you will need to reconfigure the tunnel whenever the IP address actually changes. On some ISPs this is rare and servers will often have the same IP for months. On other ISPs IPs change daily.

Does IPsec tunnel traffic go through other Untangle applications?

**No.** Currently all traffic coming and entering an IPsec tunnel is bypassed. The other apps will not see this traffic.

How do I connect IPsec between Untangle and my IPsec Device?

IPsec should work with any compatible endpoint, but unfortunately Untangle doesn't have the resources to test against specific devices. Use the Untangle/pfSense settings below as a guide; the pfSense settings are pretty standard Phase 1/Phase 2 configurations which should have similar settings on any device. If those settings do not work against an Untangle tunnel then the devices might not work together using IPsec.

Can I connect IPsec from Untangle to Cisco RV series?

These settings have **not** been verified by Untangle Support:

- Keying Mode : IKE with Preshared key
- Phase1 DH Group : Group 2
- Phase1 Encryption: 3DES
- Phase1 Authentication: SHA1
- Phase1 SA Life Time: 86400 seconds
- Perfect Forward Secrecy: checked
- Phase2 DH Group: Group 2
- Phase2 Encryption: 3DES
- Phase2 Authentication: SHA1
- Phase2 SA Life Time: 3600 seconds
- Preshared Key: <same as on UT>
- Advanced (all unchecked except)
  - AH Hash Algorithm: SHA1

**Can I connect IPsec from Untangle to a Cisco 870 series?**

These settings have **not** been verified by Untangle Support (thanks djoey1982):

- **On the Untangle:**
  - Connection Type: Tunnel
  - Auto Mode: Start
  - Interface: External
  - External IP: (The external IP address of this server)
  - Remote IP: (The public IP address of the remote IPsec gateway)
  - Local Network: (The private network attached to the local side of the tunnel)
  - Local IP: (The IP address of this server on the local private network)
  - Remote Network: (The private network attached to the remote side of the tunnel)
  - Perfect Forward Secrecy (PFS): unchecked
  - Shared Secret: <same as Cisco>
- **Link to Cisco 870 Settings:** Cisco 870 Settings
**Captive Portal**
Captive Portal allows administrators to require network users to complete a defined process, such as logging in or accepting a network usage policy, before accessing the internet. Captive Portal can authenticate users against the Local Directory inside Untangle, RADIUS or Active Directory if Directory Connector is installed. Directory Connector authenticated users can be given special policies using Policy Manager and will be given special per-user reports in Reports.

**Getting Started**
After installing Captive Portal completing the following steps will work for typical installations.

1. Define what users/machines will be "captured" and required to complete the portal process before accessing the internet. For example, enabling the first example rule in the Capture Rules table in the Captive Hosts tab will force all machines on the internal interface.

2. Set any "special" IPs that unauthenticated machines will need to access. These can be set in Passed Hosts by adding them to the Pass Listed Server Addresses. Typically this will be the DNS server and the DHCP server if it is on the other side of Untangle. If Untangle is handling these resources this is not necessary.

3. Set any "special" machines that always need access to the internet. These can be set in Passed Hosts by adding them to the Pass Listed Client Addresses.

4. Customize the Portal Page by editing settings on the "Captive Page" tab. If "Basic Login" is chosen, set the appropriate authentication method for users on the "User Authentication" tab.

5. Turn on Captive Portal by pressing the On button on the faceplate.

After enabling, "captured" machines will be forced to "authenticate" on the portal page before accessing the internet. Unauthenticated machines will have all web traffic redirected to the portal page until they have successfully authenticated.

**Settings**
This section reviews the different settings and configuration options available for Captive Portal.

**Captive Hosts**
The **Captive Hosts** tab configures which machines and what traffic will be "captured" by the Captive Portal. This can be done by configuring a set of **Capture Rules**. Capture Rules describe what traffic is to be captured by Client Interface, Client IP, Server IP, Times of Day, Days of Week, and combinations thereof. The example below shows a rule that captures all clients behind the Internal interface.
All enabled rules are evaluated in order to determine whether or not traffic is captured. Once any rule matches the given traffic no further rules are evaluated. An enabled rule that has Capture unchecked means that traffic will not be captured and no further rules are evaluated. This is useful for special cases where traffic is not to be captured. For example if all Internal machines are to be captured the above example rule can be added. However, if all machines should be given unauthenticated access between midnight and 1AM to grab updates and new anti-virus signatures then a rule can be added at the top with Client Interface set to Internal and Time of Day set to 00:00-01:00 and Capture unchecked.

Capture Bypassed Traffic

The Capture Bypassed Traffic setting determines whether or not bypassed traffic (according to Bypass Rules) are captured. This includes Ping traffic and other bypassed traffic like DHCP. If enabled, even bypassed traffic like Ping, DHCP, and any other bypassed traffic will not pass until a machine is authenticated. If disabled, bypassed traffic will pass even when the machine is unauthenticated. This will need to be disabled if DHCP must pass through Untangle for machines to get addresses. This should be disabled if machines should be able to pass no traffic at all before authenticating.

Passed Hosts

The passed hosts tab is useful for describing machines that should not be captured.

Similar to the Client IP Pass List in Web Filter, machines added to the Pass Listed Client Addresses will have access to the internet without having to authenticate. This is useful for servers that are on a captive network but should not be captive.

Traffic to certain destinations can also be exempt from capture by adding them to the Pass Listed Server Addresses list. Typically this will be the DNS server and the DHCP server if it is on the other side of Untangle. If Untangle is handling these resources this is not necessary. It is also useful for any resources that should be
available to all machines despite being unauthenticated such as update servers or servers that are required for the authentication process.

**Captive Page**

This tab controls the functionality on the portal page displayed to unauthenticated captive users.

**Captive Portal Page** allows the selection of three different captive pages.

- **Basic Message** is a page used when users should see/accept a message before being allowed to the internet. It has several tunable properties such as **Page Title**, **Welcome Text**, **Message Text** and **Lower Text**. Additionally if **Agree Checkbox** is enabled users must check an "accept" checkbox (labeled with **Agree Text**) before continuing.

**Note:** All boxes accept HTML code, but invalid HTML will prevent the page from properly rendering.

**Captive Portal Page Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page Title</td>
<td>Captive Portal</td>
</tr>
<tr>
<td>Welcome Text</td>
<td>Welcome to the Untangle\reg; Captive Portal</td>
</tr>
<tr>
<td>Message Text</td>
<td>Click Continue to connect to the Internet.</td>
</tr>
<tr>
<td>Agree Checkbox</td>
<td></td>
</tr>
<tr>
<td>Agree Text</td>
<td>Clicking here means you agree to the terms above.</td>
</tr>
<tr>
<td>Lower Text</td>
<td>If you have any questions, Please contact your network administrator.</td>
</tr>
</tbody>
</table>
Below is an example of a Basic Message page a user might see if there is no agree checkbox.

Basic Login is a basic page that requires users to login. Similar to Basic Message it has several properties that can be configured. Once a user hits the login/continue button the user will be authenticated using the Authentication method select on the User Authentication tab.

Note: All boxes accept HTML code, but invalid HTML will prevent the page from properly rendering.
Below is an example of a **Basic Login** page.
Custom is a setting that allows the uploading of a fully custom Captive Page. This is for experienced web developers that are comfortable with developing and PHP and javascript - Untangle's support department can not help with custom development of custom Captive Pages.

If Custom is selected it is advised to turn off automatic upgrades. Newer versions of Untangle may be incompatible with any custom captive page so the upgrade must be handled by hand. An example Custom Page implementation can be downloaded here.

The View Page Button can be used to view what the configured captive page looks like. This button only works when Captive Portal in on.

Session Redirect

Session Redirect defines how users will be redirected to the captive page.

Redirect URL defines the location that users will be sent after successful authentication. If Redirect URL is blank they will be sent to the original destination.

Redirect HTTP traffic to HTTPS captive page controls whether users will receive an HTTP or HTTPS login page. HTTPS is more secure as login credentials will be communicated over an encrypted channel, but users will receive a warning without a valid certificate signed by a certificate authority.

Redirect HTTPS traffic to HTTPS captive page controls whether or not unauthenticated users will have their HTTPS traffic redirected to the HTTPS login page. If enabled all HTTPS traffic goes to the captive page. If disabled, HTTPS traffic will be blocked.

User Authentication

This section controls how users will be authenticated if a login page is used as the Captive Page.

None is used in the case where no login is required.

Local Directory can be used if Captive Portal should use the local list of users and passwords in the local directory to authenticate users.

RADIUS can be used if users should be authenticated against a RADIUS server. This option requires Directory Connector to be installed and enabled and configured.

Active Directory can be used if user should be authenticated against an Active Directory server. This option requires Directory Connector to be installed and enabled and configured.
Session Settings

Idle Timeout controls the amount of time a machine/computer can be completely idle before it is automatically logged out. Note: while a machine may be "idle" or "not in use" it is still active on the network level. In this case idle means zero network activity. This usually happens when a machine is turned off or unplugged from the network.

Timeout controls the amount of time a machine before a machine/computer will be logged out. After this the user must log in again.

Allow Concurrent Logins controls if multiple machines/computers can use the same login credentials simultaneously. For example, if enabled two users can both use the same username and password to login.

Event Log

Captive Portal provides two event logs: Login Event Log and Block Event Log.

Login Event Log

Use the following terms and definitions to understand the Login Event Log:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>The time the event took place.</td>
</tr>
<tr>
<td>client</td>
<td>The client IP address.</td>
</tr>
<tr>
<td>username</td>
<td>The client username (if applicable).</td>
</tr>
<tr>
<td>action</td>
<td>The action taken for the client.</td>
</tr>
<tr>
<td>authentication</td>
<td>The authentication type used.</td>
</tr>
</tbody>
</table>

Block Event Log

The Block Event Log shows all traffic that is being blocked because the source machine has not been authenticated. This is useful for finding out what traffic is being blocked and if there is any that should not be blocked. Often idle machines without logged in users can be active on the network making this log quite large. If there is activity that shouldn't be blocked under any circumstances this can be fixed by modifying the Capture Rules the client and server pass lists or creating bypass rules if Capture Bypass Traffic is unchecked.
Use the following terms and definitions to understand the Block Event Log:

<table>
<thead>
<tr>
<th><strong>timestamp</strong></th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>The action taken for the client.</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>The client IP address.</td>
</tr>
<tr>
<td><strong>reason</strong></td>
<td>The reason why the client was blocked.</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>The server the client was attempting to contact.</td>
</tr>
</tbody>
</table>

Captive Portal FAQs

**Can I use Captive Portal and the Active Directory Login Script?**

Yes, provided you make sure to keep them separate - users should **not** be logging in with Captive Portal authentication set to Active Directory and be running the ADLS. If they are both used, Untangle uses the most recent information to determine the correct username. This can very confusing as the ADLS updates on login and every few minutes and the Captive Portal users will also login after every timeout sometimes with a different username.

**Users behind the Captive Portal can't get to the internet and are not seeing the login page. Why?**

If clients are using a DNS server outside untangle, you should add this to the passed server list. In order for clients to see the login page, their homepage must successfully resolve and when they try to connect they will see the login page instead of the requested site. If Untangle is providing DNS this is not required.

**How can I allow users to log themselves out of Captive Portal?**

If you need users to be able to log themselves out, they can put `<untangle's_IP>/users/logout` to make this happen.
**WAN Failover**

WAN Failover works in conjunction with multiple WAN interfaces to assure that you maintain a path to the internet if a loss of connectivity occurs on one of your WAN connections. It is intended to allow your Untangle to use connectivity provided by multiple ISPs. You must install and configure multiple WAN connections before you can take advantage of WAN Failover's capabilities. If you have not already done so, instructions for doing that are available here.

Once installed, it will appear in the Services section of your Untangle rack. Because WAN Failover is a service, it affects all normal traffic in your network. You may use WAN Balancer in your network under normal operating conditions, but if failover is required, all traffic will be routed across the remaining functional connection(s).

You may also wish to consider using WAN Balancer in your network as well. This would allow you to be able to distribute connectivity across multiple WAN connections on a regular basis, rather than simply maintaining a second connection should failover be required.

**PLEASE NOTE** that WAN Failover does not support PPPoE connections.

**Settings**

Once WAN Failover is installed in your rack, click **Settings** to access the WAN Failover configuration, then click **Rules**. You will see the **Failure Detection Rules** that are defined. If this is your first time on this screen, no rules have been defined. Click the **Add** button to define a failover rule. The following configuration screen will be displayed.
You may configure how WAN Failover works for each WAN interface. Begin by choosing a WAN interface. You may wish to provide a description of the interface so that you know which one is which. WAN Failover is based on test criteria that you provide here. If the testing that you specify fails, the interface will be considered to be offline and all traffic from this interface will now be routed to the other WAN connection(s).

These are the configuration options:

- **Testing Interval** determines how often (in seconds) your specified test will be executed.

- **Timeout** is the maximum amount of time that may pass without receiving a response to your test.

You should make sure that you allow for enough time to pass if you have a poor connection to the internet, or a connection that often has long latency (delays) associated with it. You should also make sure that the value you choose here is less than what you have specified for **Testing Interval**.

- **Failure Threshold** is how many failures are acceptable during the testing period.
• **Test Type** is the specific method you will use to determine whether failover will be initiated. In all cases, responses to the test method are expected to verify internet connectivity. The test types are as follows:

  - **Ping** - A simple network ping test to the **IP address** that you specify.
  - **Address Resolution Protocol (ARP)** - No configuration is necessary for this. The WAN interface will automatically attempt to contact with the default gateway.
  - **DNS** - UDP packets will be transmitted to the previously-defined upstream DNS server.
  - **HTTP** - HTTP protocol will be used in transmission of TCP packets to the **URL** that you specify.

When specifying targets for ping or HTTP tests, you should choose a location external to your local network, and not too far upstream. Each upstream connection increases the possibility of latency and/or network problems creating false failures. Once you have entered these settings, click **Save** to lock in your settings.

**Event Log**

Use the following terms and definitions to understand the WAN Failover Event Log:

<table>
<thead>
<tr>
<th>timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interface involved in this action.</td>
</tr>
<tr>
<td>action</td>
<td>The action which the Untangle Server took.</td>
</tr>
</tbody>
</table>

**WAN Failover FAQs**

**I have installed and configured WAN Failover and nothing is happening. What should I do?**

Check your Multi-WAN setup to make sure that you've set this part up properly. Also check your WAN Failover settings.

**What tests should I use for Failover?**

Untangle provides four test methods. In each case, your Untangle server sends out data packets and waits for an expected reply, up to the maximum amount of time that you have specified. You can use a ping test, which sends a specified number of bytes to the IP address that you specify via ICMP. You can use ARP, which Untangle will use...
to communicate with your default gateway. You can use DNS, where Untangle sends data via UDP to the upstream DNS server that you have previously configured. Finally, you can use HTTP requests via TCP to a URL (or IP address) of your choosing.

**Is a Ping test better than the HTTP test?**

Yes and no. Ping tests are simpler and more straightforward than the HTTP test, but many network operators block ping requests because they can be used for Denial of Service attacks. In both cases, you should select IP addresses that are external to your network but relatively close to you. As the number of network hops increases, the chances of encountering a bad or slow link increases. When that happens, Untangle may interpret it as a network problem and report one of your WAN connections as failing.

**I only have one internet connection. Why would I want WAN Failover?**

With a single WAN connection, it’s obvious that you have no alternative if your internet connection fails. You can monitor the uptime of your ISP with WAN Failover by defining a rule that will log service interruptions. If downtime is hurting you financially, WAN Failover can help you document that rather inexpensively.

**Does WAN Failover support PPPoE?**

No. This protocol is not supported in a failover environment.
WAN Balancer
WAN Balancer works in conjunction with multiple WAN interfaces to distribute internet connectivity across multiple connections. It is intended to allow your Untangle to use connectivity provided by multiple ISPs. You must install and configure multiple WAN connections before you can take advantage of WAN Balancer's capabilities. If you have not already done so, instructions for doing that are available here.

Because WAN Balancer is a service, it affects all normal traffic in your network. You cannot direct traffic from one rack to one WAN connection, and traffic from another rack to a second WAN connection unless you add specific static NAT rules in your networking configuration.

You may also wish to consider using WAN Failover in your network as well. This would allow you to be able to reconfigure traffic flow on-the-fly should there be an interruption in service from one of your ISPs.

Settings
Configuration of WAN Balancer is simple, yet allows you to optimize traffic flow between your LAN and the internet via two configuration options:

Traffic Allocation

<table>
<thead>
<tr>
<th>Interface</th>
<th>Weight</th>
<th>Resulting Traffic Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>100</td>
<td>76.9% of Internet traffic on the External interface</td>
</tr>
<tr>
<td>DMZ</td>
<td>30</td>
<td>23.1% of Internet traffic on the DMZ interface</td>
</tr>
</tbody>
</table>

In Settings, click the Traffic Allocation tab. You will enter settings here (as Weight) that determine how traffic is divided among your WAN connections. You need to tell Untangle about the speed ratio between the WAN connections. PLEASE NOTE that in this example, the DMZ connection has been configured to be a second WAN connection. It will not be a WAN connection unless you configure it to perform that role.

In the example shown here, Untangle displays the bandwidth percentages for each connection. If you have two 3 megabit/second connections, you could enter 3 for each, and Untangle will translate that to 50% for each. As shown here, the external connection is using a 10 Mb/s link and the DMZ (second WAN) connection is using a 3 Mb/s link. A zero was added to each, though that was unnecessary. Untangle looked at the ratio of the two as compared to the total incoming bandwidth to determine the percentages of traffic that will be distributed to each interface.

PLEASE NOTE that you may only enter integer (whole) numbers. If you have a 1.5 Mb/s connection and a 3 MB/s connection, you may wish to double the numbers (or multiply by 10 as is shown here). Once you have entered these settings, click Save to lock in your settings.
Also note that if you turn off WAN Failover or uninstall it from your rack, traffic allocation defined by your WAN Balancer configuration will not be changed. In this condition, a non-functioning connection will not be detected, so traffic will still be distributed according to your defined rules even if one of the links is down.

### Source Routing

![Source Routing Table]

You may also wish to specify **Source Routing** settings. This allows you to associate certain traffic (by IP address/range) with a specific WAN interface. In the example shown, traffic associated with internal address 192.168.1.170 is being directed to the DMZ interface (which has been defined as a WAN interface). The /32 netmask for a single address has been omitted in this example, but you can use netmasks to specify entire subnets.

You would typically use Source Routing if you have VOIP and data traffic, and wish to keep them separate. You could also use this for other purposes (mail server vs. regular traffic, web server vs. regular traffic). Remember that Source Routing rules are evaluated from the top down, so traffic will be routed according to the first matching rule.

### WAN Balancer FAQs

**I installed and configured WAN Balancer, but nothing is happening. What should I do?**

Check your Multi-WAN setup to make sure that you've set this part up properly.

**Are the bandwidth settings percentages?**

No. You enter bandwidth numbers for each connection that are relative to each other, and Untangle will determine the proper percentages. If you have a 3 Mb/s connection, and a 10 Mb/s connection, you could simply enter 3 for the first and 10 for the second.

**Why can't I accurately enter the speed of my 1.5 Mb/s connection?**

The bandwidth settings accept integers (whole numbers) only. To accurately represent the speed difference, either enter double the speed of each connection or multiply by ten.
**Why is some of my internet traffic being stopped?**

Check the status of your WAN Failover service. If it has been uninstalled, is turned off or is not functioning normally and you have lost one of your internet connections, traffic allocation defined by WAN Balancer is still being performed even though one of your connections is down.

**If a source route specifics that certain traffic should always use one WAN - what happens when that WAN interface is down?**

If a source route specifics a certain subnet should always use a given WAN that traffic is forced out that WAN. For example, A source route rule can always route 192.168.10.0/24 traffic out the DMZ WAN interface. However if the DMZ WAN interface is determined to be down according to the WAN Failover app, then the source route rule is ignored and that traffic will go out the other WAN(s).
Policy Manager

The Policy Manager works by creating rules or policies. Using policies, you can route traffic based on the network interface and/or endpoints. A policy binds traffic that matches certain criteria to a Virtual Rack. Policy Manager enables you to:

- Use multiple, distinct copies (instances) of any filter applications, but not services.
- Install and configure each instance into a different rack.
- Assign each rack a policy.
- Route a particular type of traffic to the a chosen rack.

Settings

Since the policy rules are implemented differently for most networks, the settings will be covered a bit differently than the other applications.

About Routing and Virtual Racks

Applications are not installed into an Untangle Server, but into a virtual rack. The Untangle Server ships with a single virtual rack called the Default Rack. You cannot remove this rack. The Default Rack serves companies that have basic protection needs. You can also create custom virtual racks. Your Untangle Server can have many virtual racks and each rack can contain zero or more applications. The racks are customizable in that you can apply different rules for any Application, though not for services.

In addition to rules enforced by the Applications, you can further control your network by using network traffic policies. Traffic arrives at one network interface of your Untangle Server and leaves on another. After the traffic enters and before it exits the Untangle Server, several applications can scan and/or modify the traffic. To illustrate how the Untangle Server handles traffic, go to Routing Behind a Simple Web Page Request.

Parent Racks

To ease the configuration of multiple racks we recommend using the Parent Rack system. Upon creating a new rack, you can set the new rack to have a Parent Rack - if you use this system, the new rack will be created with all of the settings inherited from the rack you specify as the Parent. If you need to change settings, just add the application to the new rack. The app installed in the child will override the settings from the parent and the child rack app can now be configured as desired. This is useful because it saves you from having to reconfigure applications you want to operate the same in multiple racks, such as the virus scanners.
Using the example of a school, we would have students going to the Default Rack, then create a new Teacher Rack which uses the Default Rack as its Parent Rack. If you go to the Teacher Rack, all the apps will be greyed out and you will not be able to modify any settings because they are copied from the Default Rack. By adding in a new copy of Web Filter, you can modify the web filter settings so the teachers can access websites the students cannot, however settings for all other applications will still be copied from the Default Rack.

**Using Policies To Route Traffic To Racks**

The Untangle Server routes traffic to racks by consulting its list of policies. Think of policies as rules, binding a type of traffic to a rack. A given policy can be expressed as:

If the traffic looks like X, route it to rack Y

Where Y is the name of the rack and X defines the type of traffic. The simplest way to differentiate traffic is by its:

- **Interfaces**: The client and server's Internal, External, DMZ, VPN interfaces. The list of interfaces depends on the network interfaces that you have installed in the Untangle Server.

- **Endpoints**: The IP address of client and server. Partition traffic based on one or both endpoints enables you to target traffic to a rack of Applications between locations as granular as specific computers.

**Deciding When To Use Multiple Racks**

Are you wondering if you need more than the Default Rack? Normally, you don't. However, if you cannot configure a given Application to meet all of your needs, you might need more than one rack. Here are some common use cases for additional racks:

- **Applying very different requirements to different sets of users**: If your organization is a large school, you might need two different racks: one for students and one for teachers. There are many websites that you want teachers and librarians to access, but you do not want students to access. For an example, go to Example: Creating a Custom Policy for a School.

**Tip**: If you only have a few users that need to bypass web content controls, consider using **Pass Lists** in Passed Clients, not a separate rack. In this case, a pass list is an easier solution to implement and maintain.

- **Setting up a DMZ to host an Internet-facing web server**: The policies associated with web traffic to your own web server (filtering, scanning) should be different than those for employees browsing the web. Simply create a DMZ Rack, then apply a custom policy that handles the traffic from the External interface to the DMZ interface.

- **Setting up a special file transfer relationship between your organization and an external business partner**: File transfers between these two groups may permit certain file types (executable code), yet these file type transfers are...
blocked for the general Internet. Simply create a Partner Rack and a Company Rack.

- **Setting up a VPN:** Since many users use a VPN to access a protected network from home (where their home networks might not be as secure), you might want to restrict access to critical internal systems by VPN users.

The previous list highlights cases where a single instance of an Application cannot be configured for all situations (for example, Web Filter should scan for traffic from desktops yet not to a company’s own web server). Multiple racks let you install and configure instances of just those Applications that you need for the type of traffic you are dealing with.

**Creating Special Racks for Servers**

Use a special rack called a **No Rack** to apply policies to servers, not users. The most common case where you might need to use a **No Rack** is if you want two Microsoft Exchange Servers to communicate with each other. This way, the Microsoft Exchange Servers’ traffic will not be filtered by any Applications.

As discussed in About Routing and Virtual Racks, the Untangle Server ships with a single rack called **Default Rack**, and you can install additional, custom virtual racks. All newly created racks contain only the service applications, which run on all racks.

The **No Rack** virtual rack does not appear in the virtual rack drop-down list (in the main interface). It is not a rack because it is not designed to contain Applications. **No Rack** is available by default from within the Policy Manager. When you modify a default policy or create a custom policy for the **No Rack**, simply specify **No Rack** from the drop-down list of virtual racks. For minimal protection, the **No Rack** does enable NAT.

**Adding a Virtual Rack To Untangle Server**

Add additional virtual racks beyond the **Default Rack** that Untangle Server provides if you want to use custom policies. If you want to create custom policies, you must install Policy Manager. To learn about virtual racks, go to Deciding When To Use Multiple Virtual Racks.

**To add a new virtual rack:**

1. Launch the Policy Manager.
2. From the Policy Manager, click the add (+) button.
3. Specify the rack name, and provide a description to state the purpose of the rack, then click **Update**, then **Save**.
4. Verify that the rack was created: From the Rack Dashboard, select the Rack drop-down list as shown in Creating Virtual Racks, then select the rack that you just created. By default, this new virtual rack contains only service Applications.

**Next Step:** Install, configure, and turn on Software Products to your new rack. Go to Installing Software Products.
Preparing To Assign Users To Policies

Normally you'd simply configure your router for DHCP, allowing the router to automatically assign IP addresses to users' computers. The most common way to assign users to a policy is done by user IP address. If the router assigns the IP address automatically to a user's computer and that IP address changes (which is inevitable), the Policy Manager can no longer enforce policies for that user. Because of this, you should assign static IP addresses to virtual rack users. After all, you're asking the Policy Manager to keep track of users and their activity. When you assign static IP addresses, group users into logical IP address ranges.

In a 255.255.255.0 network, where you have IP address 192.168.1.1-192.168.1.254 and using the example in Example: Creating a Custom Policy for a School, create the following ranges on your router — whether that router is an Untangle Server or not:

- 192.168.1.51-192.168.1.150 (Teachers & Staff)
- 192.168.1.151-192.168.1.254 (Students)

To assign a static IP address to a computer when your router is an Untangle Server, go to Assigning Network Computers Static IP Addresses.

Creating Custom Policies

If you want to create custom policies, you must install Policy Manager. As mentioned in About Routing and Virtual Racks, most deployments do not need to create custom policies. However, you need to create a custom policy to do any of the following:

- Differentiate traffic both on network interfaces and endpoints.
- Create a policy that applies to one user in a virtual rack.
- Create policies that apply to specific times during the day or week.

To create a custom policy:

Before You Begin:

- Review the example in Example: Creating a Custom Policy for a School.
- Create a Virtual Rack other than Default Rack. Go to Adding a Virtual Rack To Untangle Server.
- For each virtual rack user, assign a static IP address. Go to Preparing To Assign Users To Policies.

1. Launch the Policy Manager.
2. In the Policies table, click the add (+) button.
3. Specify the endpoints, interfaces, and virtual rack for the new custom policy, and click Update.
<table>
<thead>
<tr>
<th><strong>Protocol</strong></th>
<th>The network protocol of the traffic that you want the Untangle Server to scan. Valid values are TCP, UDP, PING or TCP &amp; UDP.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>The network interfaces on which the traffic travels. Your choices are Internal, External, DMZ, any other network interface that is installed, any WAN interface, and any non-WAN interface.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The IP address(es) to which you want the policy to apply. The address are described in the IP Matcher format. Any is a valid value, and means that the client address is removed as a traffic selection criteria. See also Preparing To Assign Users To Policies.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port on which you want the policy to apply. Valid values are in Port Matcher format. Note that Port Matcher supports the value any. <strong>Tip:</strong> If you don't wish to scan certain types of traffic, do not create an empty Virtual Rack. Instead, select No rack as the rack in your custom policy.</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>The user to whom you want this policy to apply. The users from your Active Directory are listed as (Active Directory). The users from your Local LDAP directory are not listed and must be entered in manually.</td>
</tr>
<tr>
<td><strong>Time of Day</strong></td>
<td>The range of time, based on a 24-hr clock (also called military/army/railway time), that you want to policy to be active. In 24-hour time clock, the day begins at midnight, 00:00, and the day ends at 23:59.</td>
</tr>
<tr>
<td><strong>Days of Week</strong></td>
<td>The days that you want the policy to be active.</td>
</tr>
</tbody>
</table>
| **Rack** | A list of available virtual racks. Select one of these virtual racks for each policy.  
- If you do not want to scan certain types of traffic, do not create an empty virtual rack. Instead, select No rack from the drop-down list.  
- The **Enable this Policy** check box enables you to activate or deactivate a policy. If you clear the checkbox, you deactivate the policy without deleting the policy settings. |

4. If you added more than one custom policy, Reorder them if necessary. Policies should be listed in order as they are evaluated in the order that they are listed.
5. If you don’t want the Untangle Server to evaluate this policy at this time, clear the live check box to disable it.

6. Click Save.

Routing Behind a Simple Web Page Request

The Untangle Server uses the following pieces of information to process a web page request:

- The IP address of the requester (client) and the IP address and port of the requestee (server). These IP addresses are called endpoints. The client and server is defined by client-server architecture.

- Two network interfaces—the client’s interface and the server's interface.

To make routing easier to visualize, consider this scenario:

Emma is sitting at her desktop on the protected network (connected to the internal interface). Emma decides she wants to learn more about networking so she visits Google in her web browser.

Since Emma's computer is behind an Untangle Server running NAT, the IP address of her computer is 10.0.0.129. When Emma opens the Google home page in her browser, the Untangle Server sees a TCP traffic request from IP address 10.0.0.129 (Emma's computer) to IP address 66.102.7.99 on port 80 (66.102.7.99 is one of the many IP addresses of Google).

After Emma makes the page request from her desktop and until that request arrives at Google, the following sequence of events occur:

1. A request is sent from Emma's machine (10.0.0.129) to the Untangle Server (which acts as the network gateway) where it is received on the your Untangle Server's internal interface. The Untangle Server now considers this request's client interface to be the internal interface.

2. The Untangle Server inspects the request, and finds the source/client IP address to be 10.0.0.129.

3. Using the destination name of www.google.com, the Untangle Server sends a request to a DNS server, who returns the IP address 66.102.7.99.

4. It adds the Google web server port number onto the destination address (66.102.7.99:80).

5. The Untangle Server routes the traffic to Virtual Racks for inspection.

6. One or more Software Products inspects this traffic. In this case, the Web Filter inspects the request and finds no malicious or flagged content.

7. The Untangle Server consults its policies to determine the server interface of the traffic to that server IP:port, 66.102.7.99:80. In this case, the Untangle
Server determines that the server is connected to the external interface.

8. The request is sent from the Untangle Server to 66.102.7.99:80, exiting the Untangle Server on the external interface.

In this example, Emma's request had two endpoints: Emma's machine and Google's Web Server.

---

**Example: Creating a Custom Policy for a School**

Imagine that you are the Network Administrator at a public school. Let's assume that you need to create policies that enforce the following workplace environment:

- No web content restrictions for teachers and other staff. In this case, use the Default Rack for teachers and administrators.
- Many web content restrictions for students when they are (or should be) in class. For example, they cannot access www.myspace.com during class. In this case, create a virtual rack called Student Work Rack.
- Some web content restrictions for students when they are on break. For example, they can access www.myspace.com during break. In this case, create a virtual rack called Student Play Rack.

---

**Reordering Custom Policies**

This example assumes a 255.255.255.0 network that provides an IP address range of 192.168.1.1-192.168.1.254. The router has the following IP addresses assigned, as described in Preparing To Assign Users To Policies:

- 192.168.1.51-192.168.1.150 (Teachers & Staff)
- 192.168.1.151-192.168.1.254 (Students)

The following example shows these two policies:

- **Policy #1**: Uses Student Play Rack to enable students to visit www.myspace.com during lunch.
**Policy #1**

**Student Play Rack**

*Okay to browse myspace!*

<table>
<thead>
<tr>
<th>Policy Management</th>
<th>Racks</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Rack</td>
<td>Teachers &amp; Staff: anything goes</td>
<td>[X] ?</td>
</tr>
<tr>
<td>Student Play Rack</td>
<td>Students: okay to browse myspace</td>
<td>[X] ?</td>
</tr>
<tr>
<td>Student Work Rack</td>
<td>Students: cannot browse myspace</td>
<td>[X] ?</td>
</tr>
</tbody>
</table>

**Policy #2:** Uses Student Work Rack to block students from visiting www.myspace.com during class.

**NOTE:** policies are evaluated in the order they are listed and the FIRST policy that matches a network event is the one that is applied to the event. Thus, in this example, we want the 'Student Play' policy to come first, so when it matches an event access to the controlled site is permitted. Then, we want the 'Student Work' policy to come second so the controlled site is denied otherwise. Then, we want the 'Default' policy to come last in the list, so any default rules are enforced as a fail safe, i.e., should a teacher be accessing the web from a student computer but not necessarily accessing myspace.

**Custom Policy #1**
Policy #2

Policy Manager FAQs

Can I use my existing Active Directory groups to create policies for different groups of users?

Yes, if you’re using the Directory Connector application you can use Policy Manager to accomplish this. Simply set up the policy to your liking, click Users, and you will be able to select your groups from the list.

When should I create a virtual rack?

Create a virtual rack when you want to apply different rules to different users. For more information, go to Deciding When To Use Multiple Virtual Racks.

I’m using the Untangle Server’s OpenVPN. Do I need to create extra virtual racks/policies for the VPN users?

You do not have to create extra virtual racks/policies to use VPN. The VPN interface is, by default, inside the external and DMZ interfaces, but outside of the internal interface. The single Default Rack is sufficient for most deployments.

One case where you would need to create extra virtual racks/policies is when not all VPN users are equal and you want to apply different rules to different VPN users. If all VPN users are equal, have the policies dealing with the VPN interface route traffic to the Default Rack.
I only want to scan inbound email traffic, not outbound. Do I need to create a new virtual rack and policies?

No. By default, outbound email traffic is not scanned. If you would like it to be, this option is available in Spam Blocker.

I created a new custom policy. Now it’s not there. Why?

Custom policies are a feature of Policy. If you do not have a valid subscription to Policy Manager (or a trial) you can not create new policies.

Why can’t I add/remove entries from the Default Policies tab?

Default Policies ensure that all possible types of traffic are handled by the Virtual Racks.

If you were allowed to delete a Default Policy and you did not add a Custom Policy that is the equivalent of the Default Policy that you deleted, the Untangle Server would be unable to handle some types of traffic.
Directory Connector

Directory Connector enables Untangle to communicate with your directory services allowing creation of per-user policies and per-user reports. Directory Connector also supplies connectors for communicating with external directory services so that other apps (such as Captive Portal) can authenticate users against external directories. Directory Connector creates a mapping for usernames to IP address such that policies can be created per username/group and reports can be viewed by username. Directory Connector’s connectors allow communicate with external directory services such as Active Directory or any directory service that supports RADIUS.

Settings

This section reviews the different settings and configuration options available for Directory Connector.

Status

This tab lists current IP addresses mapped to usernames by either the Active Directory Login Script or Captive Portal login. The IP address is mapped to the AD account name if using the AD script, AD account name if using login on Captive Portal, or the RADIUS account name if using Captive Portal

Active Directory Connector

The Active Directory connector tab contains settings for connecting and communicating with the Active Directory Server. The "Active Directory Test" tests these settings by communicating with the server.

After this is set correctly, other applications can use the connector to authenticate users using the Active Directory Server. Example: Captive Portal can be configured to authenticate logins using Active Directory.

To configure Active Directory Server:

Before you begin:

1. Ensure that your Active Directory users are in one domain. Users can be in multiple Active Directory Organizational Units (OUs), but must be under one domain. Multiple domains are not supported at this time.

2. If you are using your Active Directory server as your DNS server, ensure that your Untangle Server has it's external interface DNS setting configured to point at your Active Directory server.

3. The Active Directory server should added to the bypass list of Captive Portal if Captive Portal is used.
AD Sample Settings

1. In the Active Directory (AD) Connector tab, select the Enabled radio button.

2. Provide the AD Server IP or internal hostname in the AD Server IP or Hostname field.

3. Specify the port on which the Untangle communicates with your Active Directory server (default is port 389).

4. Provide the Active Directory domain name and the username and password for an administrator account (usually Administrator).

5. In the Active Directory Domain field, enter the AD name. The AD name is available from Active Directory tree.

6. (Optional) Active Directory Organization. The Active Directory organization unit (OU) that contains the users.
   - If you want the Untangle Server to find all your users, do not type any value in the Active Directory Organizational field.
   - If, for some reason, you want to limit the users to a specific part of the Domain tree, specify the OU path. For example, to include only users in the MyBusiness Organizational Unit, the entry will be:

```
OU=MyBusiness
```
   - If you want to limit the users more to just a specific end of the Domain tree, specify the entire OU path. For example, to include only users in the MyBusiness Organizational Unit the entry will be:
7. Click the **Active Directory Test** button. You will be asked to save your Settings. Click **Continue**.
   
   - If you receive a **Success!** message, you have successfully enabled access to the Active Directory Server.
   
   - If you receive a **Failure!** message, the Active directory test failed.

8. Click the **Active Directory Users** button. The Untangle Server outputs a list of users in the text box. If the list does not include users that expect:

   - Verify that you have the correct domain.

   - Verify that you have the correct OU, if you specified an OU.

9. Click the **Save button**.
**Active Directory Login Script**

If you want to use the Username Map for per-user/group policies or per-user reports you can use the Active Directory Login Script.

The ADLS is a small script installed on your network clients using a group policy. Once installed on a client, the script starts each time the user logs on to the network and immediately notifies the Untangle Server that the user is on the network, and the Untangle remembers this IP address. Any activity for that IP address is automatically mapped to the user's username. This scripts runs on login and periodically in the background to keep the Directory Connector Username Map up to date with any login, logouts, IP changes, etc.

**To install the Active Directory Login Script:**

**Before you begin:** This procedure assumes that you are logged on to the Active Directory Server and are remotely logged on to the Untangle Server.

1. In the Active Directory (AD) Connector tab, click on the AD Login Script button. The Active Directory Login Script download page launches.

2. Click on the download link. The Active Directory login script now resides on your AD server. You need to install the script to the correct location. The file name is adlogin_user.vbs.

3. To apply AD login script for the **entire domain**. This methods uses a group policy to apply the AD login script to an entire domain and all OUs within that domain. Use this method if you have more than 10 users and newer Windows Server platform.

4. To apply AD login script for **specific users**. Use this method if you have 10 or less users and older Windows Server platform.

**ADLS for the entire domain**

**To apply AD login script for the entire domain:**

1. Download Group Policy Management tool, which is installed by default in R2.

2. Log on to the domain controller (Active Directory Server), then launch the Group Policy Management tool by doing one of the following:
   - `Start > Program files > Administrative Tools > Group Policy Management`
   - From a command line prompt, run `gpmc.msc`. 
3. Create the group policy:
   a. From Group Policy Management, right-click on the domain and select **Create and Link a GPO here**. The New GPO dialogue box appears.
   b. Specify a name for the group policy. Consider Untangle as part of the group policy name. The new group policy appears in the list of group policies.

4. Add the AD Login Script to the policy:
   a. Right-click on the group policy that you just created, and click **Edit**.
   b. Go to **User Configuration > Windows Settings > Scripts (Logon/Logoff)**. The Scripts (Logon/Logoff) window appears in the right frame.
   c. Click on the **Logon** icon. The Logon Properties window appears.
   d. Click the **Show Files** button. A Windows Explore window launches.
   e. Copy the adlogon_user.vbs file that you downloaded in Download Active Directory Login Script to this location.
   f. Click the **Add** button, browse for the script, then click **OK**.
5. Apply users to the group policy:

   In the Logon Properties window, click on the **Add** button, type a descriptive script name, then click **OK**.

a. In the **Select User, Computer or Group** window, select the OU or Group to which you want to apply this GPO.
6. From a command line prompt, activate the group policy that you just created.

gpupdate /force

**ADLS for specific users**

**To apply AD Login Script for specific users:**

1. Log on to the domain controller (Active Directory Server), then save the adlogon_user.vbs file to `\localhost\NETLOGON`.

2. Using an editor, create a local.bat file that has the following lines:

   ```
   @echo off
   \ADServerIPAddress\netlogon\adlogon_user.vbs
   ```

3. Save the local.bat file to `\localhost\NETLOGON`.

4. From the domain, go to the **Users** folder.

5. Right-click the user that requires the AD Login script. The Properties window appears.
6. Click the Profile tab and in the Logon script field type the name of the AD Login script.

7. Launch the Group Policy Management Console (GPMC), then launch the Group Policy Object Editor.

8. Copy the adlogen_user.vbs file that you downloaded in X to this location. You return to the Logon Properties window.

**Supported Active Directory Configurations**

The Untangle Server's Active Directory integration is designed to address the most common needs of small to medium sized businesses. Although the requirements below are very specific, they are easily met in most small to medium sized business computing environments.

**Supported Server OS**

<table>
<thead>
<tr>
<th>AD Server OS</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008</td>
<td>Yes*</td>
</tr>
<tr>
<td>Windows Small Business Server 2008</td>
<td>Yes*</td>
</tr>
<tr>
<td>Windows Small Business Server 2003</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Small Business Server 2003, R1</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Small Business Server 2003, R2</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2003, Standard SP2</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2003, Standard R2</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 2000 Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows NT 4.0 Server</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: For Windows Server 2008, if you’ve installed it with the strictest security settings, you must disable the signed LDAP security requirement. For more information, please follow the instructions here but disable the requirement instead. You should then run gpupdate /force on the server to update the group policy in effect.
Supported Client OS

- Windows 2000 Professional (5.0 SP4 Rollup 1 v2) or later
- Windows XP Professional SP2 (5.1.2600 Service Pack 2) or later
- Windows Vista (6.0 Build 6000) or later

RADIUS

The RADIUS connector enables authentication to directory services using the RADIUS protocol. Other applications such as Captive Portal can use the RADIUS connector to authenticate and identify users.

To configure RADIUS:

1. Open the Settings on Directory Connector and open the RADIUS tab
2. Click the 'Enabled' checkbox to enable the RADIUS connector
3. Enter the directory server's IP in RADIUS Server IP or Hostname:
4. Enter the port to communicate with the directory server (default: 1812) in Port:
5. Enter the shared secret from the RADIUS Server in Shared Secret:
6. Select the Authentication Method supported by the server. Options are CLEARTEXT, PAP, CHAP
7. Test your setup using the RADIUS test.
8. Click the Save button.

After RADIUS is configure you can configure Captive Portal to use RADIUS authentication to validate usernames.
Directory Connector FAQs

What about shared IP addresses, like with a Terminal Server?

The Directory Connector works by mapping IP addresses to usernames; any IP address sharing will mean the Directory Connector will not be able to tell these users apart. After some testing, we’ve seen that a product offering from Elusiva when paired with Captive Portal allows these users to be differentiated and become subject to policies and filtering. This has currently been tested with Directory Connector, Web Filter, Policy Manager and Captive Portal, however the ADLS hasn’t yet been tested - we’ll update this space with more information as it becomes available.

The ADLS never completes or isn’t working. Why?

You’ll need to make sure Domain Controller has the following settings:

ComputerConf > Admin Templates > System > Scripts
- Run logon scripts synchronously = disabled
- Run startup scripts asynchronously = enabled

UserConf > Admin Templates > System > Scripts
- Run logon scripts synchronously = disabled

One user was still having issues; he solved it by running the script as a program at login. You may want to try this if the above isn’t working:

User Configuration > Policies > Administrative Templates > System > Logon > Run These Programs at System Logon

I only see 1000 usernames, but I have more users. Why?

Untangle can read more than 1000 users from AD, but AD must be configured to send more than 1000 users. Run these commands from the command prompt on the AD server to do enable AD to send up to 5000 users:

ntdsutil.exe

LDAP policies

Connections

Connect to server addomainname.local

Quit

Set MaxPageSize to 5000

Commit Changes
I have followed all the steps and to best of my knowledge, installed it correctly. How come the logon script does not work?

One way to check to see if your logon script is working or not is to check the status page to view the current Username Map. If you are seeing no entries after running the script manually or via the logon, if Untangle is in bridge mode verify that your interfaces are not backwards. You can also edit the script and make sure the internal IP of Untangle is listed.

Does the GPMC (Group Policy Management Console) work with 64bit OS?


Why are my Security Groups not showing up?

Security Groups will not be displayed when using the Active Directory Users button in the settings, but they will be displayed when selecting users in the Policy Manager. Only Security Groups will be shown, not OUs.

I'm authenticating Captive Portal users against Active Directory, but no names show up in the Username Map. Why?

Captive Portal must go into the rack after Directory Connector to properly work. Please note this refers to the order in which they are installed into the rack, not the order they appear in the rack. If you're seeing this issue, simply remove Captive Portal to the rack, then add it back into the rack and reconfigure it. The next time a user logs in through it, they should correctly populate the Username Map.
**Attack Blocker**

The Attack Blocker protects your network in a few ways:

- Sanitizes all packets the Untangle Server receives. This packet-cleaning is a built-in function and has no administrative settings.
- Protects against lower-level networking attacks.
- Protects against Denial of Service (DOS) attacks.

**Settings**

This section reviews the different settings and configuration options available for Attack Blocker.

**Status**

The Status tab simply tells you if Attack Blocker is active - there are no settings to configure.

**Exceptions**

Use the Exception list to identify a virtual computer (IP Address) that represents more than one physical computer. As discussed in How does it work?, Attack Blocker tracks the relative activity of computers on its network. If an IP address represents more than one physical computer, as is the case if you have a router performing NAT behind an Untangle Server that's a bridge, then Attack Blocker must know this IP address; otherwise, Attack Blocker considers that network to be an unusually active single computer and rejects that network's traffic.

**To add a new entry to the Exception list:**

1. From Attack Blocker, click the **Settings** button.
2. Click the **Exceptions** tab.
3. Click the add (+) button.
4. Specify the exception that you want to add:

<table>
<thead>
<tr>
<th>Enable</th>
<th>When this box is checked, the exception rule is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The IP Address of the computer that needs special consideration.</td>
</tr>
<tr>
<td>User Count</td>
<td>The number of users (computers) that this address represents. For example, if 5 users are behind a NAT system, the external IP address of that NAT system needs a user count of 5.</td>
</tr>
</tbody>
</table>
5. Click the **OK** button.
Event Log

Use the following terms and definitions to understand the Attack Blocker Event Log:

<table>
<thead>
<tr>
<th>timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>The source IP address of the traffic.</td>
</tr>
<tr>
<td>source interface</td>
<td>The network interface on which the traffic arrived at the Untangle Server.</td>
</tr>
<tr>
<td>reputation</td>
<td>As described in How does it work?, the reputation is a relative value assigned to clients to indicate their consumption of network resources. This value is usually between 0 and 100, with larger numbers indicating greater resource consumption.</td>
</tr>
<tr>
<td>limited</td>
<td>The number of times the source client was limited (in a period of time) corresponding to the event. For a review of what it means for clients to be limited, go to How does it work?</td>
</tr>
<tr>
<td>dropped</td>
<td>The number of times the source client had traffic dropped (during a period of time) corresponding to the event. For a review of what it means for clients to have traffic dropped, go to How does it work?</td>
</tr>
<tr>
<td>reject</td>
<td>The number of times the source client had a session rejected. For a review of what it means for clients to have traffic dropped, go to How does it work?</td>
</tr>
</tbody>
</table>

Attack Blocker FAQs

How does it work?

Attack Blocker tracks traffic from all hosts (IP addresses). The number of connections and the volume of data are monitored. If a given host is significantly more active than others, its reputation increases. Reputation is expressed as a number on a relative scale. Large reputation numbers indicate that a given host is consuming more resources (more connections, more bytes transferred) than its peers.

As the load on an Untangle Server increases, it may not have enough resources to service all requests. Rather than slow everyone down, the Attack Blocker takes action against hosts with the largest reputation numbers. In this way, hosts that hog all the bandwidth are allocated fewer resources while other less demanding hosts experience no change in service and performance levels. There are three actions that the Attack Blocker can take against hosts with large reputation numbers.

Attack Blocker Actions
• **Limited.** Attack Blocker limits a host's access to resources inside the protected networks. The limited host experiences a mild slowdown in network performance.

• **Dropped.** Attack Blocker causes a host's traffic to be dropped, slowing down traffic greater than if the traffic was simply limited.

• **Rejected.** Attack Blocker rejects a host's traffic for a given session, temporarily preventing the host from accessing the protected networks.

By using reputation numbers to allocate resources, the Attack Blocker protects a network from Denial of Service attacks. When a host attempts to flood a network protected by the Untangle Server, the attacking host's reputation number increases so that the host moves from experiencing a limited slowdown to being denied access to protected resources.

The action that the Untangle Server takes depends on the reputation of the offending host. The action of *rejecting* the host completely is extreme, so Attack Blocker walks a fine line between allowing hosts to be active (such as a heavily loaded email server) and shutting down a host's session that is threatening to bring down your network. However, if the Attack Blocker determines that a host's activity is threatening your network, it will reject that host's session. In most cases, limiting the host and dropping the host's packets is enough to protect your network.

The Attack Blocker does not have any settings for sanitizing packets, but does have a setting to specify a host that is treated differently than its peers in terms of reputation calculation. This administrative setting is explained in Exceptions.

**If I have a single big machine (database, file server, print server, etc) and another smaller server. Will my big machine develop a bad reputation?**

The reputation for the big machine will be higher than the small machine. In a normal deployment this should not be a concern, as the Untangle Server should not be limited in its overall resources. If slowdown under heavy load is a concern, the big machine can have its reputation calculated differently as discussed in How does it work?
OpenVPN

OpenVPN is an SSL-based VPN (virtual private network) that supports both site-to-site and client-to-site configurations. When you create new clients or sites, OpenVPN creates a custom executable for each client that contains the client, configuration, and authentication information. Users simply need to install the custom executable on their computers. OpenVPN supports the following operating systems:

- Windows 2000/XP and higher
- Mac OS X
- Linux
- OpenBSD
- FreeBSD
- NetBSD

Supported VPN Configurations

A Virtual Private Network (VPN) is a secure connection between a remote host or network and a local network over an otherwise insecure medium (i.e., the Internet). With any VPN connection, there is a client and server. Your Untangle Server can be a VPN server, allowing remote clients or sites to connect to the exported internal network. Your Untangle Server can also be a VPN client, gaining access to remote Untangle VPN servers and their internal network.

When you configure OpenVPN, you choose between two types of configurations:

- **Untangle in VPN Server Mode.**

  In this mode, VPN clients connect to the Untangle server to establish an encrypted communication channel. Each VPN client authenticates via a secure key unique to that client. Implicit is that the server is protecting network resources from another untrusted network (usually the Internet). The VPN connection allows the remote client to reside on an untrusted network yet access protected resources behind the VPN server. VPN clients are either individual computers running VPN software client or another Untangle server (second Untangle) in VPN Client mode (more on this further down) to provide a secure connection for all the computers behind the second Untangle providing access to resources behind the primary Untangle running VPN server mode. Untangle in VPN Server Mode can accept connections from both desktop/laptop software VPN clients and Untangle servers in VPN Client Mode.

- **Untangle in VPN Client Mode.**

  In this mode, the Untangle provides connectivity for all the computers behind it to a remote network behind another Untangle in Server Mode. In this mode, Untangle in
VPN Client Mode provides a single encrypted connection to the other Untangle in Server Mode so the resources behind each Untangle can access remote resources on the other end.

**Note:** Remote networks in Site-to-Site configurations must have networks which do not have overlapping IP addresses. Sites cannot use the same IP address space.
Untangle Server in VPN Server Mode

To configure Untangle as VPN Server:

**Note:** If you have already configured your Untangle as a VPN client, you will need to remove the OpenVPN module from the rack and then install the module again to reset OpenVPN to the initial state and get the VPN configuration wizard.

1. Click on **Settings** and click on **Configure as VPN Server**.
2. Click 'Next after reading the warning.
3. In the next step is to generate a certificate to secure the VPN communication.
   1. Enter the organization or company name
   2. Select the Country
   3. Enter a two letter abbreviation for the state or region.
   4. Enter city name
   5. Press 'Next
4. The next step has the IP ranges which will be exported to the remote VPN clients and sites enabling access to those IP ranges. By default the internal network of the Untangle is added. If there are other IP ranges which are handled by the Untangle such as DMZ addresses, they can be add at this point by clicking on the **Add** button.
5. Press **Close** as the configuration for Server Mode is complete.

With the Untangle Server VPN Server Mode configured, continue with the steps below to add VPN clients and sites which will connect to this VPN server.

VPN Desktop/Laptop Clients

To configure desktop/laptop VPN clients (software VPN):

Create VPN Client

By adding clients, these remote resources will have access to the resources behind the Untangle VPN server.

1. Click the **Clients** tab.
2. Click the **Add** button under **VPN Clients**.
   1. Enter a client name. Type a descriptive name to identify the user. For example, you might use the user's computer name.
2. In the Address pool drop-down list, choose the address pool to which you want to assign the user. Generally use the default pool that is created automatic during the VPN Server wizard.

3. Click **Done**.

3. Click ‘Apply’ to save the new VPN client.

Providing Access to VPN Users

**Note:** The **distribution** button doesn’t appear in the distribution column until you add and save the VPN Clients to your configuration.

**Distribute VPN Client Key**

For VPN Clients, specify the user’s email address and click the Send Email button. The Untangle Server emails the VPN user a link to download the key and OpenVPN Client as the one shown in Downloading Key and OpenVPN Client. For greater security, you can download the key directly from the client to which you want to provide access, or to a USB key from another remote client.

1. Click the **Distribute Client**.

2. Specify the user’s email address and click the Send Email button. The Untangle Server emails the VPN user a link to download the key and OpenVPN Client as the one shown in Downloading Key and OpenVPN Client. For greater security, you can download the key directly from the client to which you want to provide access, or to a USB key from another remote client.
Email or Download User's VPN Key

3. Ensure that VPN users download the key and OpenVPN Client properly. Users should click on the OpenVPN link as shown in Downloading Key and OpenVPN Client.

Email for User's VPN Key

1. For systems other than Windows, download the configuration files instead of the Windows installer and install the OpenVPN client specific for your system at openvpn.net

2. For Windows 2000 and XP
   1. Download the Windows installer from the link in the email.
   2. Install normally by double clicking on the executable installer.

3. For Windows Vista and 7
   1. Download the Windows installer from the link in the email.
   2. Right click on the executable installer and select Run as administrator
   3. After completing the installation we need to change the OpenVPN client to run as administrator.
      1. Click on Start Menu -> Programs -> OpenVPN and right click OpenVPN GUI.
2. Select **Properties**.

3. Click on **Compatibility** tab.

4. Select **Run this program as an administrator**.

5. Click **OK**

---

**VPN Site Clients**

**To configure Untangle Server VPN clients:**

Where an entire remote network connects to a VPN server. A VPN Client site can represent many individual hosts (machines) within its protected network. This configuration is common for remote offices, where a handful of employees need to join the protected network at headquarters. When a group of computers (a network) establishes a VPN connection to a server, the group of computers is said to be a site. An Untangle Server can also act as a remote site, bridging the internal network at that remote location to another Untangle Server acting as a VPN server.

On the Untangle server in VPN server Mode do the following"

1. Click the **Clients** tab.

2. Click the **Add** button under **VPN Sites**.

   1. Enter a site name. Type a descriptive name to identify the site. For example, you might use the city name.

   2. In the Address pool drop-down list, choose the address pool to which you want to assign the user. Generally use the default pool that is created automatic during the VPN Server wizard.

   3. Network address is the IP address space of the remote network. For example the remote office network is 192.168.200.0/24 so enter 192.168.200.0 in the Network address field and Network Mask 255.255.255.0 in the Network mask field. The main site and all of the remote sites must have different network address ranges.

4. Click **Done**.

5. Click ‘**Apply**’ to save the new VPN site.

3. Click the **Distribute Client** and download the VPN Site configuration (config.zip).

At this point the Untangle VPN Server has a key ready for the remote Untangle Client VPN. The simplest way to transfer VPN key to the remote site is to login to both the VPN Server and the VPN Client sites on the same browser.
Untangle Server in VPN Client Mode

1. Login to the remote Untangle server which will serve as the VPN Client.
2. Click on OpenVPN Settings button.
3. At the Welcome screen click Next button
4. Select Upload Configuration and upload the configuration file (config.zip) previously downloaded.
5. Once the Success popup appears, click OK.
6. You are now connected to the main office.
7. Click OK at the bottom of the site.

Revoking Users' VPN Access Temporarily

To secure your network, temporarily disable a user's key if that user does not intend to use the VPN for an extended period of time, such as in the event of an employee's leave of absence. If you want to permanently remove a user's key, go to Revoking Users' VPN Access Permanently.

To temporarily disable a VPN user's key:

1. From OpenVPN, click the Show Setting button.
2. Click the VPN Clients tab.
3. In the VPN Clients area, clear the Enabled check box that corresponds to the user, then click the Save button.

Revoking Users' VPN Access Permanently

To secure your network, always disable a user's key if that user loses a laptop on which a key is installed. To revoke a user's VPN access, you must disable the user's key. In this case, the user needs to reinstall the VPN client and key. This procedure removes a user from a VPN Site or VPN Client, revokes the user's certificate, and permanently invalidates the key that was previously issued to the user.
About OpenVPN Event Logs

Event logs are only available on the Untangle Server in VPN Server mode. The client side only has if it's connected or not in the Status tab. Use the following terms and definitions to understand the OpenVPN Event Log:

<table>
<thead>
<tr>
<th>start time</th>
<th>The time the connection was established.</th>
</tr>
</thead>
<tbody>
<tr>
<td>end time</td>
<td>The time the connection was terminated.</td>
</tr>
<tr>
<td>client name</td>
<td>The name of the connection's client.</td>
</tr>
<tr>
<td>client address</td>
<td>The IP address of the connection's client.</td>
</tr>
<tr>
<td>Kbytes sent</td>
<td>The number of Kilo bytes that have been sent on the connection.</td>
</tr>
<tr>
<td>Kbytes received</td>
<td>The number of Kilo bytes that have been received on the connection.</td>
</tr>
</tbody>
</table>

OpenVPN FAQs

Can I install the OpenVPN client that came with Untangle onto a Vista or Windows 7 Operating System?

Yes! The OpenVPN client that Untangle bundles with the Untangle server is compatible with Vista and Win7, both 32-bit and 64-bit versions.

Please note, you will need to install and run as an Administrator, and may need to login as the administrator to the Vista machine or disable the UAC. To disable the UAC, please check out this URL: [1]

What operating systems does OpenVPN support?

OpenVPN supports the following operating systems:

- Windows 2000/XP and higher
- Linux
- OpenBSD
- FreeBSD
- NetBSD
- Mac OSX
- Solaris

**I started OpenVPN and my network died. Why?**

The most common cause is because the address pool assigned to VPN users is in the same address range used by LAN users. Unless your LAN uses addresses that are in the default VPN address pool, leave the VPN address pool as is. Otherwise, change the pool as needed to make sure they are different. For more information, go to Prepare To Configure Your VPN Server.

**If a user or site loses a secure key, how do I disable the old key and issue a new one?**

When you remove a user from a VPN Site or VPN Client, you revoke that user's certificate and invalidate the key that was previously issued to that user. To permanently revoke a user's key, go to Revoking Users' VPN Access Permanently.

**Can I administer an Untangle Server over a VPN connection?**

Yes! To administer the Untangle Server, you must include the internal address of the system in one of the Exported hosts networks. This internal address can either be one of the following:

- A single entry that contains the IP address with a 255.255.255.255 netmask. For example, 192.168.1.1/255.255.255.255.
- An entry that contains a network that includes the IP address. For example, 192.168.1.0/255.255.255.0.

**Can I use OpenVPN with my Mac OS X workstation?**

Yes! OpenVPN supports many platforms, including Mac OS X - you'll need to install a VPN client on your Mac.

**To install a Mac OS X VPN client for use with Untangle:**

1. Download VPN configuration files from Untangle Server.
2. Move the files to somewhere convenient, for example, the Desktop.
4. Double-click the downloaded Tunnelblick.dmg file; a window will appear.
5. Double-click the Tunnelblick icon in the window.
6. You will be asked for your computer administrator's password and then Tunnelblick will be installed into /Applications.

7. You will be asked if you wish to launch Tunnelblick. Click "Launch".

8. You will be guided through the process of installing your configuration files. (Note: Untangle configurations are "OpenVPN" configurations, not "Tunnelblick VPN Configurations").

The Tunnelblick icon will remain at the top right corner of the Menu Bar until/unless you quit. If you don’t quit, Tunnelblick will automatically launch the next time you log in. If you do quit Tunnelblick, you can relaunch it from /Applications at any time.

**To connect to the VPN:**

1. If Tunnelblick isn’t running, launch it from /Applications.

2. Click on the Tunnelblick icon in the top right corner of the Menu Bar and select Connect ‘office-mv’.

3. A "dark" tunnel shows no VPN connection is active, a "light" tunnel shows an active VPN connection. While attempting to connect, the tunnel goes from dark to light and back again repeatedly.

4. To view websites hosted inside the VPN you may need to do the following:
   1. click on "Details" in the Tunnelblick menu (see image below)
   2. select "Set Nameserver" (see 2nd image below)
   3. Disconnect and Re-Connect your VPN

**For help with Tunnelblick:**

Look at the documentation or post your problem on the discussion group.
Can I use OpenVPN on both of my WAN connections?

Yes, but you need to add a port forward from the secondary WAN IP to the primary WAN IP because Add the following port forward:

Matchers:

- Destination Address: <your secondary WAN IP address>
- Protocol: TCP and UDP checked
- Destination Port: 1194

To:

- New Destination: <your primary WAN IP address>
- New Port: 1194

After that, simply change the client to point at the second WAN's IP (or third etc). If you have your remote hosts and networks using a hostname to connect (ie "vpn.example.com") then you can do load-balancing and failover by having that hostname resolve to the appropriate IP you want the client to connect to.

My Untangle is in bridge mode, how do I setup the OpenVPN?

Setup: WAN-Router/Firewall (3rd party) -> Untangle (bridge mode) -> LAN

First of all, this is not an ideal scenario. You will need to make some changes on your network to get this to work properly. If you are unsure and want an easier OpenVPN solution, you might want to check out this post.
To make the OpenVPN work when the Untangle is in the bridge mode, you will need to make few changes on the edge router/firewall.

1) Port forward UDP 1194 to the Untangle. 2) Port forward https port (typically 443, if 443 is already utilized, pick something else), match is on the Untangle, config, administration, https port. 3) You can try the Packet Filter rule labeled ‘Route VPN traffic that would go through the Bridge’ at Config > Networking > Advanced > Packet Filter. If the Packet Filter rule does not work for you, you will need to create a static route on your router/firewall.

This is needed because typically when you have the Untangle in bridge mode, all the users on your LAN will have the edge Router/Firewall as their gateway. When the OpenVPN user tries to connect to a server on the inside, the Untangle doesn’t know how to route that traffic properly since it is not the gateway.

You may also need to configure OpenVPN to use the correct public external IP. (It may be necessary to redistribute your client configurations after making this change)

- If the hostname that looks up in DNS to the external IP, configure Untangle Server to use that hostname: Config > Administration > Public Address and specify the 'Use Hostname.'
- If you do not have a hostname that looks up externally, configure Untangle Server to use the external IP: Config > Administration > Public Address and choose ‘Use a Manually Specified IP.’

I am about to setup the OpenVPN, what is the best and the easiest way?

Check out the information here.

I want to setup site to site VPN, how would I do this?

We have a forum post outlining site-to-site VPN setup here.

When I try to send the OpenVPN client via the email option, my users do not receive the email.

First, make sure that your email settings are correct (Config > Email), then run the email test. If you are getting the email test, you should be able to get the OpenVPN client email as well. Your other option is to directly download the client from the Untangle and distribute it manually.

Clients can connect using OpenVPN, but the tunnel drops after 15-30 seconds. Why?

Check to see if you have any unused or disconnected interfaces set to Dynamic - if so, change these to static and retest.

OpenVPN connects, however I can not access anything?

Many things could cause this issue. Try pinging the Untangle's internal IP address (assuming you are not blocking ping). If you are able to ping the Untangle, that means
that the OpenVPN tunnel is up and functional. If that is working, check to see if Windows Firewall is running on the server you're trying to connect to - by default it will block access from non-local IPs.

**I can access resources via the IP address, how can I access them via their hostname?**

This depends on who is doing the DNS on the network: if you have an internal DNS server, you will need to go into the advanced tab of the OpenVPN, checkmark the export DNS, enable the DNS Override and input the IP address of the DNS server. If Untangle is doing DNS, just checkmark export DNS.

**How can I get DNS resolution working over my site-to-site tunnel?**

You'll need to go to Config > Networking > Advanced > Local DNS and add the IP of the DNS server on the far side of the tunnel, enter the domain in the Domain List column, and use the FQDN when accessing resources. Please note that you'll need to do this on both sides of the tunnel for it to work from either side.

**Can I use 3rd party like DD-WRT to connect?**

Unfortunately site-to-site tunnels are only supported Untangle to Untangle.

**Does OpenVPN support IPsec, PPTP, or any other types of VPN?**

As an endpoint we use OpenVPN, but you're free to use other VPN software by running a server behind the Untangle - we bypass IPSec traffic by default, so you shouldn't have issues with it.

**I need more help, what are my options?**

If you have a paid support subscription, please call or email us. If you do not have support, please use our forums - the more information you can provide the better, such as:

Site to Site or Site to Client VPN:

Untangle version:

Router mode or Bridge mode:

OpenVPN client's OS:

Describe the issue:

**I have Multi-WAN set up, does OpenVPN still work if my WAN fails?**

Not at this time. Currently OpenVPN only works with the Primary WAN.

**How can I restrict access to certain OpenVPN users?**

Exported address/host on the OpenVPN is for everyone, if you'd like to wall off resources from specific users you'll need to use the Firewall.
My OpenVPN user is connected remotely, can I force all the traffic through the VPN tunnel?

Untangle's implementation of OpenVPN uses split tunneling - only VPN traffic will traverse the tunnel; any non-VPN traffic will go out the normal WAN connection. We are aware OpenVPN supports full tunneling like PPTP, however Untangle does not support this option.

In a site-to-site configuration my software clients can talk to their server, but not other sites

Scenario: Multi-site VPN, site A (server), sites B and C (clients), software clients connecting to site A. A, B, and C and talk to each other because you are exporting A, B, C's networks under exported hosts/networks. The software clients can only access resources from site A.

If you want the software clients to also talk to B and C, you will need to add the address pool of the software clients to the exported hosts/networks.

My OpenVPN site to site is setup correctly, however I'm unable to pass traffic across the tunnel?

This is a very rare case, however this does happen from time to time. If you have site A with 1.2.3.4 and site B with 1.2.3.5, site to site VPN will not work, since both of them are in the same subnet or their gateways are the same. In order for the site to site VPN to work, each location needs to be completely different from the other location. You might need to ask your ISP to change one of your location's IP to a different subnet.

Is there a way to setup a password for the OpenVPN users?

Yes, if you right click on the OpenVPN icon on the client's PC there is an option for a password - this password is only used when launching the client.

What does Warning...files...no longer available... mean?

If you recieve the following message when you try to download the VPN Client:

Warning The files that you requested are no longer available, please contact your network administrator for more information

...your VPN Client key is no longer valid. Ask your Untangle Server administrator to resend the VPN Client key.

I have found this by searching for OpenVPN on my favorite search engine, I need help?

This is for Untangle's implementation of the OpenVPN - if you do not have an Untangle installation, you would need to try somewhere else for support (or maybe try us out!).
Why is the incorrect DNS Suffix pushed out to my clients?

The DNS Suffix is set **when the client is created** - you **can not** change this later, you'll need to delete and recreate the user and redistribute the client. Whatever suffix you want pushed out to your clients, set it in Config > Networking > DNS Server, make sure the DNS Server is turned on, then create your clients. You can turn off the DNS Server after you create the clients if you wish. If the DNS server is turned off when you create them, your clients will get the suffix example.com. Some users are reporting that this only works correctly if the DNS Server is set to **On** all the time.

**Can I use OpenVPN with my smartphone?**

Yes, you can. You'll just need to install and run a VPN client that supports OpenVPN. Android's build-in VPN client won't import the files unless you convert them, but if your phone is rooted you can use the application OpenVPN Settings on the Android Market.
Configuration Backup

Untangle's Configuration Backup enables you to respond quickly to hardware failures and disasters (fire, storm, etc).

Each night, your Untangle Server uses a phone-home feature to request a nightly backup. Upon request from your Untangle Server, Untangle Network's data center performs a backup of your server's configuration, with the exception of report data. The Untangle Server's interface shows you what day and time the backup event occurred and if the backup was successful or unsuccessful.

**WARNING:** Configuration Backup is not active until it appears in your rack and its power light is green. It can only provide protection when enabled.

**Settings**

The Status tab will inform you of the last successful backup - there is nothing to configure.

**Event Log**

Use the following terms and definitions to understand the Spyware Blocker Event Log:

<table>
<thead>
<tr>
<th>timestamp</th>
<th>The time the event took place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>The action which took place (e.g. backup).</td>
</tr>
<tr>
<td>result</td>
<td>The result of that action (e.g. success).</td>
</tr>
<tr>
<td>details</td>
<td>Any pertinent details.</td>
</tr>
</tbody>
</table>

**Configuration Backup FAQs**

**How do I know if my Untangle Server is performing backups?**

You can use the event log, specifics are listed here.

**How do I retrieve my own backups, if I have the Configuration Backup module installed and running?**

You will need to login to the http://store.untangle.com After logging in, please click my subscriptions on the left hand side. Your backups will be listed per UID on the right hand side "View Backups".
Once you click the View Backups, you will get this page:

Please pay close attention to the date - as this represents the date when the backup was taken: 25-04-2010 06-17-56 (this one is from April 25th, 2010) Please ignore the other numbers like 06-17-56.

Which backup should I use?

Typically, we suggest the latest backup or a backup just prior to the failure.

When I click View Backups, it tells me that No backups are available?
A few things could cause this:

1. Brand new install, and the Untangle server has not performed the nightly backup.
2. You don't have the Configuration Backup module installed or turned on.
3. Something is wrong with your network like DNS, IP address, and etc.

**How do I manually perform the backup?**

Log in to the Untangle, config, system, and backup. We suggest backing up to the file, meaning, log into the Untangle via a PC, and backup the config to the PC.

**How do I restore?**

Here is the general procedure for restoring your system:

1. Have your old and the new UID (Untangle ID) handy.
   1. We realize that if your old system crashed that it is tough to get the UID, however you can retrieve it from your store account.
      1. Login to store.untangle.com with your credentials.
      2. On the left hand side, select My Subscriptions.
3. You should see all your subscriptions with UID. If you don’t then your subscriptions were purchased under a different store account. Please contact support.

2. Retrieve your backup file from the store

3. Install the new HW with the latest Untangle software.
   
   1. Install the Open Source package
   
   2. Also install the trial of any paid applications you had installed previously.

4. Do the configuration restore if you want to restore the settings from the old box. (config, system, restore)

5. Under certain conditions, reboot is required.

6. Do the subscription transfer from the old server to the new.

Note: If you are using just the Open Source package, you may not have a store account. Typically, the store account is created when you are purchasing the paid subscription.

**Can I restore from a different version’s backup, example 6.2 backup to 7.2?**

We officially support within the same version. 6.2 backup should restore to another 6.2 server, however, most of our users also have reported that older backups do restore to the newer versions. General rule is to stay within 1 or 2 versions. Example: 7.1 backup should work with 7.2.

**How come the usb restore method does not work?**

That is correct, please use the network method to restore. Login to the Untangle from a network PC that has the backup file, config, system, and restore.

**What is the correct file extension for the backup?**

The config backup file should have the .backup file extension.
Report Tool

Untangle Server generates Untangle Reports, and makes them available through:

- Online
- Email summary
- CSV file (for further data analysis)

Reports can be viewed on the Untangle Server, or email summary reports can be emailed to report recipients. While the emailed report provides a significant amount of information on your network traffic, you cannot drill down to get extreme granularity. When this is needed, you should use the emailed report as a guide so that you can identify specific instances for further analysis with online reporting and/or with CSV-based report data.

Please note that upon a new Untangle server installation, Untangle Reports are unavailable until after the first full day of server usage.

Settings

The Settings tab allows you to change how the Reports are generated.

Status

The View Reports button, which is available after the first full day of server usage, will open a new window (IE) or tab (firefox) to display the current report.

Generation

Email

The Add button will provide entry fields for adding another email address to received the reports that are generated.

- **Email Address:** A valid email address to receive the reports. Sometimes the reports might be caught by SPAM filters so check quarantines if reports are not received.

- **Email Reports:** Whether or not to send reports. This checkbox is useful for temporarily turning on/off reports to specific users.

- **Online Reports:** This checkbox allows the email address of a user to log in the online reports page to view reports. The password field must be set along with this checkbox to allow access.

- **Password:** Along with the Online Reports checkbox, entering a password will enable a user to login with the email address and this password to view reports.

- **Confirm Password:** Confirms password from above field.
Email Attachment Settings

Online reports have CSVs (comma separated value spreadsheets) which contains all the data used for generating the tables and graphs in the reports. The CSVs enable admins to perform further analysis on the traffic patterns.

- **Attach Detailed Report Logs** checkbox enables the sending of CSVs in a zip file with the emailed reports.

- **Attachment size** field limits the size of the CSVs attached to the email. As CSVs are added to the attachment zip field, once the size of the zip file reaches the size entered in this field, no more CSV files are added. This field is mostly used when the receiving email server limits the size of attachments. Limiting the size of the attached file will prevent the report email from being bounced at the receiving email server.

Daily Reports

- The checkbox is for enabling of daily reports. The reports are generally generated around 1-2am server local time.

Weekly Reports

Weekly reports are a complete summary of the past 7 days. Each day checked will generate a report for the previous 7 days from that day. For example checking Sunday and Wednesday will generate a report on Sunday for the previous Sunday through Saturday traffic and on Wednesday, the report will be previous Wednesday through Tuesday traffic.

**WARNING:** *Retention Data* should be at least 7 days to get this full report.

Monthly Reports

This type of report contains all the traffic for the previous 30 days.

**WARNING:** *Retention Data* should be at least 30 days to get this full report.

Data Retention

Data Retention is the amount in days of traffic data is kept. If desired, you may change Data Retention from its default setting (7 days) to a value of your choosing. This value controls how much time report data is kept on disk. This data is used to generate per host/user/email reports on the fly. Please note that increasing the number increases
the amount of disk space that is needed for data storage, and could have negative effects.

**Reports Retention**

This controls how long the static reports are kept on the server. Each report uses a small amount of disk space.

**Name Map**

The Untangle Server makes Reports available through email and online. Emails on the recipient list with 'Email Reports' enabled will receive email summary reports. Top-level information presented in the email report is identical to that provided online, though the online report provides the capability to get information at a deeper level.

In order to maintain the name to IP Address to a specific device, it's recommended to also add those IP addresses as static reference in **Config -> Networking -> DHCP Server -> Add Static** in the DHCP list.

Directory Connector can provide this functionality automatically.

**To replace IP addresses with names:**

1. From **Reports**, click the **Settings** button.
2. Click the **Name Map** tab.
3. Click the plus (Add) button above the table. A new row appears in the table.
4. Specify the Name Map (IP address) and user name, and click the **Save** button.

**Viewing Reports**

**Email Summary Reports**

The Untangle Server makes Reports available through email and online. Emails on the recipient list with 'Email Reports' enabled will receive email summary reports. Top-level information presented in the email report is identical to that provided online, though the online report provides the capability to get information at a deeper level.

**Online Reports**

**To access Reports from Untangle Client:**

1. Click on the **Settings** button on **Reports**.
2. From Reports, click the View Reports button.

To access Reports directly with a browser:

1. In a browser, type https://PublicAddress/reports where PublicAddress is either the public hostname or public IP address of the Untangle Server. For example, https://10.0.0.1/reports. If a non-standard HTTPS port is used, the port number must also be entered. As an example, if port 8443 is used for remote admin and report viewing, you would enter https://10.0.0.1:8443/reports.

2. Specify your login and password. The Untangle Reports home page displays. If you do not have a valid login, contact your administrator.

As mentioned previously, online reports allow you to analyze reporting data in granular detail. In reports provided for each app, data contained in email reports is limited to that which is included under the Summary Report for each product (referring to the above graphics). All products have one or more tabs that contain event data for the product, which you are already familiar with in the Untangle rack. This allows you to refer to the specific event that causes the user/host/site to show up in the report.

In addition, the online Summary Report contains hyperlinks which allow you to drill down for further information. Using the sample below, each user who shows up on the pie chart (left) is shown also in the table (right), with a colored tile to help you locate them in the pie chart, and a hyperlink that allows you to analyze their usage at a deeper level. Following that link, you can see their usage on an hourly basis, on a daily basis, their acceptable web usage, unacceptable web usage, and bandwidth used.

Another major enhancement shows up near the top of each table. Immediately under the label Key Statistics is an icon. Clicking on the icon causes your Untangle server to collect data used in the report and store it into a CSV file, which you can download and have immediately available to you for analysis as you see fit. While many of the downloadable data sets appear trivial by themselves, they allow you to study in depth when used in conjunction with corresponding event data.
External Report Viewing

If you wish to access the online version of Untangle Reports from a location external to the Untangle server, click the **Config** tab at the left of your screen, followed by **Administration**. The **Administration** screen will open in the main part of your screen. Under **External Administration**, check the **Enable External Report Viewing** checkbox.

Configuration of reports is fairly simple. There are a few options to control which reports are generated and what data they contain. There are also a few parameters to control how long data and old reports are kept on the server.
Email

Reports Recipients and Users

<table>
<thead>
<tr>
<th>Email Address (Username)</th>
<th>Email Reports</th>
<th>Online Reports</th>
<th>Change Password</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:dominic@juntangle.com">dominic@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:dominic@juntangle.com">dominic@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:krembo@juntangle.com">krembo@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:lromio@juntangle.com">lromio@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:nromio@juntangle.com">nromio@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:stromio@juntangle.com">stromio@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:tromio@juntangle.com">tromio@juntangle.com</a></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Email Attachment Settings

- Attach Detailed Report Logs to Email (CSV Zip File)
  - Attachment size limit (MB): 10

Daily Reports

Daily Reports are generated at midnight and covers events from the previous 24 hours, up to, but not including the day of generation.

Generate Daily Reports: ✔ Every Day

Weekly Reports

Weekly Reports are generated at midnight and covers events from the previous 7 days, up to, but not including the day of generation.

Generate Weekly Reports: ✔ Sunday
  - Monday
  - Tuesday
  - Wednesday
  - Thursday
  - Friday
  - Saturday

Monthly Reports

Monthly Reports are generated at midnight and covers events from the previous 30 days, up to, but not including the day of generation.

Generate Monthly Reports: Never
  - First Day of Month
  - Everyday
  - Once Per Week

Data Retention

Limit Data Retention to a number of days. The smaller the number the lower the disk space requirements and resource usage during report generation.

Limit Data Retention: 7

Reports Retention

Keep old reports on the server for this number of days.

Reports Retention days: 30

Reports Settings

Blitz Networking Systems - c/Caldes de Montbui 118 - 17003 - Girona - Spain +34 972486160 - ventas@blzwall.com - http://www.blzwall.com
Reports FAQs

Why am I not receiving Untangle Reports?

- If your Untangle Server is turned on, it's possible that the reports have not yet been sent. Reports are emailed on a daily basis. Wait up to 24 hours to receive your first report email. Go to Specifying When Untangle Server Generates Untangle Reports.

- If you have been using the Untangle Server for more than 24 hours, verify that you configured the Untangle Server with your outgoing mail server settings. Go to Configuring Server Email Traffic.

Why am I not receiving the Detailed Report through email?

Beginning with Untangle 7.0, a new report engine is being used. The reports are more detailed than they have been in the past, but you can only receive maximum detail by using online reports.

What is the difference between event logs and Reports?

Event logs contain the underlying data from which the Untangle Server generates Untangle Reports. However, there are a few differences. Event logs provide real-time information whereas Untangle Reports provide next-day information. Moreover, the event logs show activity by IP address; Untangle Reports are more user-friendly because they show activity by user.

Can I email Reports to anyone?

Yes, as outlined in Emailing Recipients Untangle Reports, you can email reports to anyone. That user does not need administrator privileges. There is no limit on the number of users that receive the Untangle Reports.

I just upgraded my Untangle box. My reports are missing. Why?

The next time that scheduled reports are run, the top-level report index gets rebuilt according to the new standard. If you run reports daily, please allow 24 hours before reports are available. If you only run weekly or monthly reports (and not daily), please allow one reporting cycle.

The key statistics does not appear to match the data in the graph. Why?

The 24-hour graphs show an average of all days covered by the reports. In other words, it shows what a "typical" day looks like. The actual max and avg of any given day could be far greater or less than the "typical" day.

The spam/phishing stats don't seem to add up. Why?

You may notice that some reports may report a certain number of phish/spam email, but the event log and CSVs show a different number. This is because the graphs show the actual number of emails, but the event log and CSVs treat each recipient as an
individual email so per-user/host reports are correct. So, for example, if a single spam email is sent to two users it will only be counted as one in the reports, but two in the event log/CSV file.

**Timestamp (date) column is not displayed properly after I export reports to CSV file. Why?**

If you are using MS Excel to view the exported CSV file, you can change the format of the cell (first column) to a Date format.

**What is the others column when looking at the charts in Reports?**

When looking at the top 10 of a Reports chart, Others is made up of everything else not listed - in the following example, we can see the top 9 sites visited by users in a day. Others is there to give us a baseline, for example if we saw one or two users with a larger percentage than Others, we’d probably want to do some investigating as to why that user is pushing more web traffic than a large portion of the organization (relative to total organization size).
### Setting Up Your Network

Most of these options are available under the Config > Networking tab of the GUI and are broken down by section. Features and settings listed under **Advanced Mode** may require you to be in advanced mode to access them:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Standard Mode</th>
<th>Advanced Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>• Network Configuration Modes</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Changing the Configuration Mode</td>
<td></td>
</tr>
<tr>
<td>Networking Basics</td>
<td>• About Untangle Server’s Network Interfaces</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• About NAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• About DMZ</td>
<td></td>
</tr>
<tr>
<td>Network Configuration</td>
<td>• Configuring Untangle Server’s External IP Address (Standard Mode)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modifying Data Transfer Mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Swapping Network Interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adding Network Cards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Removing Network Cards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Testing Internet Connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network Troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Port Forwards</td>
<td>• About Redirecting Network Traffic</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Redirecting External and Internal Traffic</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Topics</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>External Aliases</strong></td>
<td>• Routing Traffic To Untangle Server From Another External Network (Standard Mode)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Routing Traffic To Untangle Server From Another External Network (Advanced Mode)</td>
<td></td>
</tr>
<tr>
<td><strong>Hostname Configuration</strong></td>
<td>• About Untangle Server’s Hostname</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Configuring Untangle Server To Use Dynamic DNS</td>
<td></td>
</tr>
<tr>
<td><strong>DHCP Server</strong></td>
<td>• About DHCP</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Assigning Network Computers Static IP Addresses</td>
<td></td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>• Configuring Untangle Server as DNS Server</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Mapping Computer Hostnames To IP Addresses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Using DNS Entries To Reduce Load on Untangle Server</td>
<td></td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>• About Untangle QoS</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enabling UntangleQoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitoring Untangle QoS</td>
<td></td>
</tr>
<tr>
<td><strong>Multi-WAN</strong></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• About Multi-WAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What you need</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuring Multi-WAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• About WAN Balancer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• About WAN Failover</td>
<td></td>
</tr>
<tr>
<td><strong>Packet Filter</strong></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• About Packet Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adding Packet Filter</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Rules</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Overrides</td>
<td>• About File Overrides&lt;br&gt;• Adding File Overrides</td>
<td></td>
</tr>
<tr>
<td>Bypass Rules</td>
<td>• About Untangle Virtual Machine&lt;br&gt;• Creating User Bypass Rules&lt;br&gt;• Bypass Rules vs. Protocol Control</td>
<td></td>
</tr>
<tr>
<td>Route Management</td>
<td>• About Untangle Server's Routing Table&lt;br&gt;• Routing Network Traffic</td>
<td></td>
</tr>
<tr>
<td>Static ARP Management</td>
<td>• About ARP Entries&lt;br&gt;• Adding ARP Entries&lt;br&gt;• Spoofing Untangle Server's Mac Address</td>
<td></td>
</tr>
</tbody>
</table>
Network Configuration Modes

The Untangle Server has two distinct network configuration modes, **Standard Mode** and **Advanced Mode**. When initially installed, the Untangle Server is configured in Standard Mode, which can be configured for many common deployments. If Standard Mode features are not sufficient, you can switch the Untangle Server to Advanced Mode. The two modes offer the following services and features:

<table>
<thead>
<tr>
<th>Service/Feature</th>
<th>Standard Mode</th>
<th>Advanced Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address Translation (NAT)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DMZ</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Port Forwarding</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Domain Name Service (DNS)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Static Route Management</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Packet Filtering (Netfilter)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Bypass Rules</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ARP Management</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>File Overrides</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Changing the Configuration Mode**

**Warning:** You need to know what happens if you’re currently in advanced mode:

<table>
<thead>
<tr>
<th>Basic → Advanced</th>
<th>Advanced → Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Untangle Server preserves all your settings when you switch from Standard Mode to Advanced Mode.</td>
<td>The Untangle Server preserves all your the settings that exist in basic mode when you switch from Advanced Mode to Standard Mode. In other words, the Untangle Server deletes all settings that do not exist in basic mode. So, back up your configuration.</td>
</tr>
</tbody>
</table>
To change the Untangle Server's mode:

Before You Begin:
If your Untangle Server is currently in Standard Mode and simply want to experiment with Advanced Mode, back up your configuration as this change deletes your existing settings.

1. From the Navigation pane, choose Config > Networking.

2. Do one of the following:
   - If you are currently in standard mode, click the Status tab, click on the Advanced drop-down menu button, then click on the Switch to Advanced Mode button.
   - If you are currently in advanced mode, click on the Advanced drop-down menu button, then click the Configuration Wizard link from the Configuration Level window.
Networking Basics

About Untangle Server's Network Interfaces

Untangle Server's Interfaces

To configure your interfaces, go to:

- Configuring Untangle Server's External IP Address (Standard Mode)
- Configuring Untangle Server's Interfaces (Advanced Mode)

The Untangle Server supports up to 7 physical interfaces, though a typical Untangle Server includes the following interfaces:

- Internal
- External
- DMZ (Optional)

These interfaces do not need separate IP addresses. In the default configuration, they are all bridged and share the same IP address. Traffic is transparently captured and forwarded to the correct interface.

When the Untangle Server operates as a router, the internal interface has its own address. This address serves as the default route (gateway) for internal machines. In this case, the external and DMZ interfaces are still bridged and share the same IP address. If multiple interfaces are bridged, you can specify aliases.

So why does one need more than the three, typical interfaces? Good question. Additional interfaces can be configured as Internal or DMZs, but you don't really need additional interfaces. However, because you can apply policies by interface, additional interfaces provide you more flexibility. Here are a couple of reasons, and both involve scanning traffic:

- Scanning traffic differently depending on the DMZ. You might want two DMZs, one DMZ that manages an internal Web Server and another DMZ that manages an external Web Server, and you want to scan the traffic differently for each DMZ. Well, you can do this now that the Untangle Server supports multiple DMZs. You can also create different policies for each DMZ.

- Scanning traffic differently depending on business unit. Some companies use a different internal interface for each business unit so that an Administrator can treat traffic differently for each business unit. Using racks is a much easier way to achieve this goal, but some companies have internal policies that state that the traffic must be on different physical network interfaces.
About NAT

Network Address Translation (NAT) is a Router feature. This feature configures the Untangle Server to allow multiple machines on your internal (protected) network to share access to an external network (usually the Internet) through a single IP address.

When NAT is enabled, the administrator must provide the Internal IP Address and Internal Subnet. The Internal IP Address is the IP address of the Untangle Server as seen from the internal network and the Internal Subnet is the subnet mask of the Internal IP Address.

Note: When NAT is disabled, none of the fields on the NAT tab are modifiable.

After NAT has been configured, the administrator should configure the Dynamic Host Configuration Protocol (DHCP) feature on the Untangle Server. To configure DHCP, see the discussion in About DHCP.

- If you do not plan to use the Untangle Server to provide DHCP services for some or all of the machines within your internal network and instead, plan to set up NAT functionality on these machines, you must manually set the gateway address and subnet mask of these machines.

- If you do not plan to use the Untangle Server to provide NAT services for your internal network, you must do one of the following:
  - Ensure that you have a machine outside of the Untangle Server (on the external network) to provide NAT services.
  - Define an IP address pool. The IP addresses in this pool must be routable on the external network. If the external network is the Internet, these IP addresses must be public IP addresses.

About DMZ

DMZ is the "demilitarized zone" for the network. This is often an area where public servers are placed such that they can be reached from outside and they are separated from the internal private network.

If you set the DMZ interface to bridged with external. To put servers on the DMZ simply give them one of the public IPs available on your public network and plug them in on the DMZ interface.
Network Configuration

Configuring Untangle Server's External IP Address (Standard Mode)

This topic is for Standard Mode only. If you are in Advanced Mode, go to Configuring Untangle Server's Interfaces (Advanced Mode).

To configure the Untangle Server's external IP Address:

1. From the **Navigation pane**, choose **Config > Networking**.
2. Click the **Network** tab.
3. From the **Config Type** drop-down list, select how you want the Untangle Server to obtain its IP address:
4. Specify where you want to direct the traffic:

<table>
<thead>
<tr>
<th>Dynamic</th>
<th>If selected, the Untangle Server uses the DHCP server to obtain network settings and displays them in the boxes below. You can request a renewal of the DHCP Lease via the <strong>Renew DHCP Lease</strong> button.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>If selected, you must manually set the IP Address and Netmask. Configure the network settings as you would for any system on the network. Default Route (sometimes referred to as a gateway), primary DNS server and, optionally, a secondary DNS server are only configurable on the external interface.</td>
</tr>
<tr>
<td>PPPoE</td>
<td>If selected, you've identified that your Internet Server Provider uses PPPoE for authentication—to authorize you to connect to the Internet. If you have PPPoE questions, go to PPPoE FAQs.</td>
</tr>
</tbody>
</table>
5. Click the **Save Settings** button.
6. Click the **Run Connectivity Test** button. The test reports its findings: success or failure.
Configuring Untangle Server's Interfaces (Advanced Mode)

This topic is for Advanced Mode only. If you are in Standard Mode, go to Configuring Untangle Server's External IP Address (Standard Mode). To learn about the differences between these modes, go to Network Configuration Modes.

To configure the Untangle Server's interfaces:

1. From the Navigation pane, choose Config > Interfaces.
2. Click the Edit link for the interface that you want to configure.

   1. Click the Add (+) button. A new row appears in the table.
   2. From the Config Type drop-down list, select how you want the interface to obtain its IP address:
      - Static
      - DHCP
      - Bridge
      - Dynamic (DHCP)
      - Other

3. Click the Add (+) button. A new row appears in the table.
4. From the Config Type drop-down list, select how you want the interface to obtain its IP address:
### Static
If selected, you must manually set the IP Address and Netmask. Configure the network settings as you would for any system on the network. Default Route (sometimes referred to as a gateway), primary DNS server and, optionally, a secondary DNS server are only configurable on the external interface.

### Dynamic
If selected, the Untangle Server uses the DHCP server to obtain network settings and displays them in the **Current** column. You can override these settings using the **Override** column. You can request a renewal of the DHCP Lease via the **Renew DHCP Lease** button.

### Bridge
If selected, bridges any two interfaces. A common use is when you want to bridge the Untangle Server's DMZ interface to the Untangle Server's external interface. It's not uncommon for the DMZ to have an internal IP address; in fact, the main reason you might want to bridge the DMZ to the External is so that you don't need to assign the DMZ its own external IP addresses. In this case, Config Type is bridge, and Bridge To is External (static).

### PPPoE
If selected, you've identified that your Internet Server Provider uses PPPoE for authentication—to authorize you to connect to the Internet.

- PPPoE is supported on the external interface for users connecting to their ISP via PPPoE.
- Select the **use peer DNS** check box to use your ISP's DNS servers when the PPPoE connection is established.
- You can request a renewal of the DHCP Lease via the **Renew DHCP Lease** button.
- If you have PPPoE questions, go to PPPoE FAQs.

5. **(Optional/Internal Interface)** Specify NAT policies.

6. **(External/Internal Interfaces)** To increase network performance, specify a MTU for the interfaces. This setting is not available for PPPoE configuration type.

7. Change the transmission rate/mode. The default is auto or autonegotiation.

8. Click **Save**.

9. Test the Internet connection.
Creating NAT Policies (Advanced Mode)

For every source address that you specify, you must first assign these public IP addresses to the Untangle Server as outlined in Routing Traffic To Untangle Server From Another External Network (Advanced Mode).

There are a few reasons why you might want to create a NAT policy:

- **Sending mail.** Since the volume of mail per IP address is an important metric, have the mail server use a different IP address than the rest of the users to reduce the amount of outbound mail that gets marked as spam.

- **Logging.** You might want to separate the external behavior of some group of users from another group.

To create a NAT policy:

1. From the **Navigation pane**, choose **Config > Networking > Interfaces**.
2. Click the **Edit** for the internal interface.
3. Specify the IP address of the Internal Interface and the Source Address, then click **Save**.

For example, let's assume your Untangle Server has an internal interface with IP address and netmask of 192.168.1.102/32. Let's also assume that your Untangle Server has three external IP address:

- 1.2.3.1
- 1.2.3.2
- 1.2.3.3

If you want the packets for the internal network to appear to come from 1.2.3.2, add a NAT policy for 192.168.1.102/32 with a Source Address of 1.2.3.2.

- By default the Source Address is auto, which means packets will go out the primary (first) IP address. In this case, 1.2.3.1 is the primary (first) IP Address, so by default all traffic appears (on the Internet) to come from that address, having a Source Address of 1.2.3.1.

- Auto also means NAT is enabled as opposed to just passing through the internal addresses, which won't work for most network configurations, especially cable/DSL.

Determining Status of Network Connections

An external and internal interface are required for your Untangle Server to function correctly. Optionally, you can install a DMZ interface.
To determine status of a network connection:

1. From the **Navigation pane**, choose **Config > Networking**.
2. Click the **Interfaces** tab. The Physical Interface column lists the status for each network card.
   - Some interfaces may report unknown if they are working but cannot detect a signal in software properly.
   - If a MAC address is listed, then a network card is installed. If you want to add a network card, go to Adding Network Cards.
   - If the interface indicates connected, then the interface has a network connection. Otherwise, the interface indicates disconnected. If you want to fix a network connection, go to Testing Internet Connection.

Swapping Network Interfaces

To swap the Untangle Server's interfaces:

1. From the **Navigation pane**, choose **Config > Networking**.
2. Click the **Interfaces** tab.
3. Drag and drop the Mac addresses for the interfaces that you want to swap.

Adding Network Cards

To add a network card:

1. Physically install the network card.
2. Log on to the Untangle Server, and choose **Config > Networking**.
3. Click the Interfaces tab. The network card that you just installed does not appear in the list of interfaces.
4. Click **Refresh**.
   - If the Untangle Server detects that you installed a network card, a message appears as shown in Figure, Installing Interfaces: Interface Change Detected.
Installing Interfaces: Interface Change Detected

- If the Untangle Server does *not* detect that you installed a network card, a message appears as shown in Figure, Installing Interfaces: *No Interface Change Detected*.

5. Click **Save**.

6. Return to the **Interfaces** tab. The network card that you installed now appears in the list of interfaces.

Removing Network Cards

**To remove a network card:**

1. Physically remove the network card.

2. Log on to the Untangle Server, and choose **Config > Networking**.

3. Click the Interfaces tab. The network card that you just removed still appears in the list of interfaces.

4. Click **Refresh**.

- If the Untangle Server detects that you removed a network card, a message appears as shown in Figure, Removing Interfaces: Interface Change Detected.
Removing Interfaces: Interface Change Detected

- If the Untangle Server does not detect that you removed a network card, a message appears as shown in Figure, Installing Interfaces: No Interface Change Detected.

5. Click **Save**.

6. Return to the **Interfaces** tab. The network card that you removed no longer appears in the list of interfaces.

**Testing Internet Connection**

**To test your Internet connection:**

1. From the **Navigation pane**, choose **Config > Networking**.
2. Click the **Interfaces** tab.
3. Click on the **Test Connectivity** button. If successful a message appears as shown in Figure, Testing Internet Connection.
Testing Internet Connection

Ping Test

To perform a Ping Test:

1. From the **Navigation pane**, choose **Config > Networking**.
2. Click the **Interfaces** tab.
3. Click on the **Ping Test** button. A window opens as shown in Figure, Ping Test.
4. Enter the IP address or website URL that you wish to ping and click the **Run Test** button. The results of the ping test will be shown in the window.
Modifying Data Transfer Mode

You cannot change the speed at which network interfaces send data over the network—the Half/Full Duplex and 10/100 settings. The speed is set at 100 Mb/s full-duplex and cannot be turned off.

When interfacing with old hardware, you might need to downgrade a given port from its default Auto-Negotiate setting to a more limiting setting. However, networking hardware that requires a transfer rate limitation (100/10 Mbps) or that cannot auto-negotiate has not been readily available for several years, so Untangle Server doesn't want to clutter your interface if there is no benefit.
Port Forwards
Redirecting Network Traffic

You can redirect traffic across any of the Untangle Server's network interfaces. You can configure the Untangle Server to redirect network traffic that matches certain criteria.

The Untangle Server enables redirects from one IP address to another IP address, or from a specific source to a destination. More specifically, port forward rules apply if the Untangle Server has NAT enabled. Port Forwarding enables you to retain the security that NAT provides, yet still enable users to access certain services on your network. Port forward rules redirect traffic from an external IP to an internal computer.

The Untangle Server evaluates the port forward rules in the order that they are listed in the table, starting with the first rule in the table. For each new connection, the Untangle Server evaluates the traffic against active rules until a match (if any) is found. When a match is made, traffic is redirected as specified by the rule.

Keep in mind that your ISP can block ports using its router, and not the Untangle Server. The Untangle Server has no control over your ISP's router. If your ISP is blocking the ports required by a particular program, configure the program to use a different port, if possible. Sometimes programs allow you to set the port that it uses, then use some port that is not being blocked by your ISP. There is no way to get a list of ports that your ISP blocks, though perhaps a quick Internet search might do the trick; otherwise, you need to try one port at a time, until you find one that isn't being blocked.

Troubleshooting

If you're having trouble getting port forwarding to work you can follow the Port Forward Troubleshooting Guide.

Redirecting External and Internal Traffic

To learn about port forwarding, go to About Redirecting Network Traffic. There are two common scenarios in which you might want to use port forwarding:

- You want a web server to handle all web traffic. Redirect web traffic (port 80) from the external IP address (1.2.3.4) port 80 to your web server (192.168.1.100) in your internal network.
- You want a FTP Server to handle all FTP requests. Redirect FTP requests (port 21) from the external IP address (1.2.3.4) port 21 to your FTP server (192.168.1.101) in your internal network.

To create an advanced redirect rule:

Before You Begin:

1. Glance at the example outlined in Example: Redirecting FTP Traffic
2. From the Navigation pane, choose Config > Networking.
3. Click the Port Forward tab.
3. Click the add (+) button. The Edit window launches.

4. Select the **Enabled** checkbox if it isn't already. This flag Enables/disables a rule's redirect functionality. Checking the enable rule box enables the rule and enables the Untangle Server ability to redirect traffic matching this active rule. Unchecking the enable rule box disables the rule.

5. In the **Description** text box, provide a description of the traffic type and the traffic's destination. For example, FTP to Small Business Server.

6. In the **Type** drop-down lists, specify conditions to describe the traffic that you want to redirect. To add more conditions, click the **Add** button.

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Destination IP address of the traffic if the traffic is not redirected. You indicate a wildcard by not specifying the value. To learn about IP address syntax, go to Networking and Web Address Syntax.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Local</td>
<td>The traffic is destined to any of the Untangle Server's IPs.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Original destination port of the traffic in Port Matcher syntax.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Network protocol of the traffic to forward. Valid values are TCP, UDP, PING or TCP &amp; UDP.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source IP address of the traffic in IP Matcher syntax.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Interface from which the Untangle Server receives traffic. Valid values are External, Internal, or DMZ. For information about the Untangle Server's network interfaces, see the discussion in Network Interfaces.</td>
</tr>
</tbody>
</table>

7. Specify where you want to direct the traffic:

<table>
<thead>
<tr>
<th>New Destination</th>
<th>IP address of the host that will receive the traffic. To learn about IP address syntax, go to Networking and Web Address Syntax.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Port</td>
<td>Port on the host that will receive the traffic. To learn about port syntax, go to Networking and Web Address Syntax.</td>
</tr>
</tbody>
</table>

8. Click **Save**. A new rule appears in the table.
Example: Redirecting FTP Traffic

In the following example, all FTP traffic that reaches the Untangle Server's external interface is directed to a Small Business Server on the internal network. Note that the passive port range of 5500-5700 has been forwarded, this must also be configured on your FTP server software.

Redirecting FTP Traffic Rule 1

| Enabled: | ![Checkbox] |
| Description: | FTP to SBS |

If all of the following conditions are met:

- Source Interface: External
- Destination Local: TCP
- Destination Port: 21

Forward traffic to the following location:

- New Destination: 192.168.254.20
- New Port (optional): 21
Redirecting FTP Traffic Rule 2
External Aliases

Untangle provides the ability for a company to route many different public IP addresses through a single Untangle Server, so that within the LAN, all these IP addresses can be handled according to your business needs.

If you have more than one public IP address (64.233.167.99, google.com), you can assign the secondary addresses as external aliases (64.233.167.83, gmail.com). The Untangle Server can provide protection, handling for both the primary address assigned to the Untangle Server as well as any aliases that you specify.

Routing Traffic To Untangle Server From Another External Network (Standard Mode)

This topic is for Standard Mode only. If you are in Advanced Mode, go to Routing Traffic To Untangle Server From Another External Network (Advanced Mode). In order to create NAT policies, you must be in Advanced Mode.

- If your Untangle Server is a bridge, you can create an external address alias to allow the Untangle Server to route traffic for a network other than the network that is defined by the Untangle Server’s external IP address.

- If the Untangle Server is a router, you can create an external address alias to allow the Untangle Server to receive traffic for more than just the network of the Untangle Server’s external interface.

To create an external address alias:

1. From the Navigation pane, choose Config > Networking.

2. Click the Network tab.

3. In the Configuration for the External Interface section, click on the External Aliases button. The External Aliases window launches.

4. Click the plus (+) button. A new row appears in the table.

5. In the new row, specify the address and netmask of the additional external network. The netmask may be entered in dot notation such as 255.255.255.0 or CIDR but will be displayed in CIDR notation after it is set.

6. Click Save.

Routing Traffic To Untangle Server From Another External Network (Advanced Mode)

This topic is for Advanced Mode only. If you are in Standard Mode, go to Routing Traffic To Untangle Server From Another External Network (Standard Mode).
For more complex deployments:

- If your the Untangle Server is a bridge, you can create an external address alias to allow the Untangle Server to route traffic for a network other than the network that is defined by the Untangle Server's external IP address.

- If the Untangle Server is a router, you can create an external address alias to allow the Untangle Server to receive traffic for more than just the network of the Untangle Server's external interface.

- If you want to create a NAT policy as outlined in Configuring Untangle Server's Interfaces (Advanced Mode), each source address must be assigned to the Untangle Server.

**To create an external address alias:**

1. From the Navigation pane, choose Config > Networking.
2. Click the Interfaces tab.
3. Click the Edit link for the external interface. A new window launches.
4. Click the plus (+) button. A new row appears in the table.
5. In the new row, specify the address and netmask of the additional external network. Express the netmask as a CIDR prefix.
6. Click Save.
Hostname Configuration

Hostnames are needed to identify devices on the network. By default, the Untangle Server’s hostname is untangle.example.com. The idea is for you to replace this name with a hostname of your choosing. Make sure that the hostname resolves publicly.

Configuring Untangle Server To Use Dynamic DNS
If your Untangle Server receives a dynamic IP address from your ISP (as opposed to a static IP address), consider using Dynamic DNS. Dynamic DNS enables the Internet to translate a dynamic IP address to a static hostname. Without Dynamic DNS, you must update your Untangle Server’s network configuration each time your ISP changes the IP address of your Untangle Server.

A hostname is also useful when you use Quarantine Digests because this feature embeds URL information into its report(s).

To specify Dynamic DNS for the Untangle Server:

Before You Begin:

- Retrieve the Untangle Server’s external IP address. Go to Determining Untangle Server’s External IP Address.
- Request a hostname for your Untangle Server. Register with a Dynamic Domain Name Service (DDNS) vendor such as DynDNS at http://www.dyndns.com or one of the services listed at Free DNS. Complete the service provider’s registration, and record the following information, which you need to configure the Untangle Server as shown in Figure, Configuring Untangle Server To Use Dynamic DNS:
  - Account Name. Account name that you used to register for the dynamic DNS service.
  - Password. Password that you used to register for the dynamic DNS service.
  - Host Name and Domain Name. The Internet host name and domain name that you registered with the DDNS service provider.

Caution: Do not download and configure any third-party dynamic DNS clients (for example, the DynDNS Client Updater). The Untangle Server has its own client. If you install DynDNS Client Updater, that client will conflict with the Untangle Server’s dynamic DNS client.

1. From the Navigation pane, choose Config > Networking.
2. Click the Hostname tab.
3. Do one of the following:
   - (Standard Mode) In the Hostname field, type the hostname that you registered with your dynamic DNS service provider. If you have more
than one hostname, you must be in Advanced Mode to list more than one hostname.

- **(Advanced Mode)** In the **Hostname** field, type the hostname(s) that you registered with your dynamic DNS service provider.

4. Select the Enabled check box, specify your dynamic DNS service provider, then type your account information. Congratulations! You should now be able to contact your Untangle Server from the Internet using its hostname.

![Configuring Untangle Server To Use Dynamic DNS](image-url)
DHCP Server
Dynamic Host Configuration Protocol (DHCP) configures the Untangle Server to automatically assign dynamic or static IP addresses to machines within the internal network.

A few support details:

- The Untangle Server supports DHCP on the Internal interface, and will support the DMZ interface in advanced mode.
- The Untangle Server doesn't support multiple address pools.

In Advanced Mode
In Advanced Mode, you can specify that the DHCP Server serve up a different gateway, netmask, and change the lease time in seconds.

- If you do not plan to use the Untangle Server to provide DHCP services for some or all of the machines within your internal network and, instead, plan to set up NAT functionality on these machines, you must manually set the gateway address and subnet mask of these machines.
- If you do not plan to use the Untangle Server to provide NAT services for your internal network, you must do one of the following:
  - Ensure that you have a machine outside of the Untangle Server (on the external network) provide NAT services.
  - Define an IP address pool. This pool is a group of IP address from which the Untangle Server can assign to network clients. Without an address pool, network clients cannot access the network. The IP addresses in this pool must be routable on the external network. If the external network is the Internet, these IP addresses must be public IP addresses. The Untangle Server doesn't support multiple address pools.

Assigning Network Computers Static IP Addresses
If a computer on your internal network receives a dynamic IP address from the Untangle Server, and you want VPN clients to connect to that computer, you must assign a static IP address to that computer.

To assign a static IP address to an internal network computer:

Before You Begin: Wait for the network computer to join the internal network.

1. From the Navigation pane, choose Config > Networking.
2. Click the DHCP Server tab. There are two tables, and the interface automatically takes you to the Static DHCP Entries.
o **Static DHCP Entries.** Lists all the computers to which you've assigned static IP addresses.

o **Current DHCP Entries.** Lists all the computers that are receiving DHCP service from the Untangle Server.

3. Do one of the following:

   o If the computer is currently on the network, in the **Current DHCP Entries** table, locate the computer that currently has a dynamic IP address and that requires a static IP address, then, in the **Add Static** column, click the **plus (+) symbol** for that computer. The row immediately moves to the **Static DHCP Entries** table.

   o If the computer is not currently on the network, in the **Static DHCP Entries** table, click the **Add** button, then assign the IP address manually.

**Note:** It is best practice not to assign a static IP address from the middle of a DHCP address pool. An address pooling scheme should be defined that incorporates servers, printers, dynamic workstation addresses and static workstation addresses.

4. Click **Save**.

**Next Step:** If you want users to access this computer by hostname (thereby preventing users from having to remember the computer's IP address), map that computer to a host name. Go to Mapping Computer Hostnames To IP Addresses.
DNS Server
Configuring Untangle Server as DNS Server

Your Untangle Server can be the telephone book—the Domain Name Service (DNS) server—for your internal (protected) network. To reduce load on the Untangle Server, the Untangle Server caches DNS lookups locally.

To configure the Untangle Server as a DNS server:

1. From the Navigation pane, choose Config > Networking.
2. Click the DNS Server tab. There are two tables:
   - Static DNS Entries.
   - Automatic DNS Entries.
3. Select the Enabled check box.
4. In the Domain Name Suffix field, type the domain name suffix, which is the domain name suffix (for example, acme.com) of your organization. The domain name suffix is used to ensure that a computer on the internal network can be accessed by its fully-qualified hostname (for example, host1.acme.com).

Caution: If the Domain Name Suffix field is not filled in, problems might occur when certain versions of Microsoft Windows servers attempt to resolve a hostname.

Next Step: To add DNS entries, go to Mapping Computer Hostnames To IP Addresses.

Using DNS Entries To Reduce Load on Untangle Server

If you are port forwarding traffic to your web server that hosts your company's website, map the web server's hostname to the private IP address (for example, 192.168.1.50). Sure, you can access your company website without such an entry because it has a public IP address, but it's more efficient to access the web server directly using its internal IP address. If you type in www.mycompany.com in your browser, your request is going to go out through the Untangle Server to the Internet, then back in through the Untangle Server.

Mapping Computer Hostnames To IP Addresses

The Untangle Server can be a DNS server for your internal network. If a client on your network receives a dynamic IP address from the Untangle Server, the Untangle Server automatically adds a DNS entry to the DNS Server Configuration table for this client. If you have a computer on the internal network that does not have a DNS lookup entry, map that computer's hostname to an IP address so that:

- Other computers on the internal network can access that computer.
- Network users can access it by hostname rather than IP address (sometimes called internal aliases). A hostname is easier to remember than an IP address.
To map a computer's hostname to IP address:

**Before You Begin:**

- Configure Untangle Server as a DNS Server.
- Assign the computer a static IP address, if it doesn't already have one.

1. From the Navigation pane, choose Config > Networking.
2. Click the DNS Server tab.
3. Click the add (+) button. A new row appears in the table.
4. In the new row, specify the computer's hostname(s), static IP address, and description.
5. Click Save.
6. (Optional) To make this mapping available to VPN clients, go to OpenVPN and select the export DNS check box:

   ![Exporting DNS for VPN Clients]

**Local DNS**

This page allows you to forward individual domain queries to specific DNS servers instead of asking the upstream DNS servers.

Example: If you add "untangle.local" and 10.0.0.41, it will ask 10.0.0.41 to answer any queries for *.untangle.local.
QoS Configuration

Quality of Service (QoS for short) is a mechanism to ensure high-quality performance to latency and bandwidth sensitive applications. It allows for the prioritization and differential treatment of traffic based on rules. Most often this is used to improve the performance of latency and bandwidth sensitive applications and traffic (like VOIP) at the cost of less important traffic such as peer-to-peer.

QoS can greatly improve the performance of the network traffic and important protocols, especially when the upload or download bandwidth is saturated. However, QoS can also be detrimental to network performance if configured incorrectly. It is advised to read this section in its entirety before enabling QoS.

QoS settings can be found at Config > Networking > Advanced > QoS.

Settings

Enabled

The Enabled checkbox controls whether QoS is enabled. The default setting is unchecked, which means QoS is disabled and no rules have any effect. Before enabling QoS the Bandwidth Settings of each WAN interface must be set.

Default Priority

The Default Priority is the priority assigned to traffic which matches no QoS rule. The default setting is Medium. It is advised to leave this setting at Medium as this provides several priorities both above and below by which to prioritize special traffic.

WAN Bandwidth

WAN Bandwidth is the most critical setting to configure correctly if QoS is to operate correctly. Measure your available upload and download bandwidth several times using a bandwidth measurement tool such as speedtest.net. Make sure the rest of the network is idle when measurements are taken to avoid interference with the test measurements.

Set the limit to 85-95% of the average measured speed of each WAN interface.
Finding the right settings for the WAN Bandwidth may take some experimentation. If the bandwidth limit is set too high QoS will have no effect at all. If the bandwidth setting is too low, traffic will be unnecessarily limited to a lower bandwidth.

Why limit bandwidth to less than is actually available? So QoS can do the queueing of packets and provide differential preference. When the link is not saturated all packets are sent immediately; no waiting is required. However when the link is saturated often packets build up in a queue. If the download/incoming link (often also called ingress) is saturated, packets will be queued at the ISP. If the upload/outgoing link (also called egress) is saturated then the packets will be queued at the modem.

For outgoing packets the modem will normally write packets to the WAN on a first-come-first-serve basis. This means that the packets will be sent to the WAN in the order they were received from the internal network. This can lead to delays of all traffic when the link gets saturated. This is not ideal because latency and bandwidth-sensitive applications are delayed just as much as non-critical, non-interactive applications that are not as important.

Similarly for incoming packets, the ISP will queue packets coming to the network until they can be sent. The ISP does not know what is considered important traffic and what is low priority. Traffic is normally sent on a first-come-first-serve basis and all traffic is treated equally.

By limiting the bandwidth in QoS the packet queue is maintained within the Untangle Server and keeps the packet queues in the modem and at the ISP empty. Because the queue is maintained within the Untangle Server (the new bottleneck) this allows differential treatment to traffic. High priority traffic can skip in front of lower priority traffic giving it more bandwidth and lower latencies.

Tip: Remember traffic only receives preferential treatment when the set bandwidth limit is saturated. For testing it is useful to start several downloads while testing the performance of high priority traffic.

QoS Rules

QoS Rules are built-in rules to provide priorities for some typically important packets and traffic.

Ping Priority: Default
DNS Priority: Very High
SSH Priority: Very High
TCP Control Priority: Very High
Gaming Priority: Default

Ping Priority sets the priority of ping (echo request and echo reply) packets. This can be useful for testing the performance at different priorities.
**DNS Priority** sets the priority of DNS traffic used for name resolution. Setting this at a higher priority than other traffic usually leads to a better, more responsive internet experience.

**SSH Priority** sets the priority of SSH traffic. Setting this at a higher priority than other traffic gives better SSH performance for administrators who use SSH.

**TCP Control Priority** sets the priority of special TCP traffic, such as SYN and FIN packets. Setting this at a higher priority than other traffic usually leads to a better, more responsive internet experience and quicker session initiation.

**Gaming Priority** sets the priority of gaming traffic. This is useful for users with an Xbox, Wii, or Playstation. Giving this a higher priority can improve the responsiveness of online games.

**QoS Custom Rules**

**QoS Custom Rules** provide a simple way to create custom rules to prioritize or de-prioritize certain traffic. By default, rules exists for VOIP traffic (which is also bypassed by default).

*Note:* Custom Rules only match on *Bypassed* traffic. Non-bypassed traffic can be prioritized using the Bandwidth Control application.

**QoS Priorities**

The **QoS Priorities** section allows customization of how each priority is treated and how they are prioritized relative to other priorities.

*Note:* It is recommended to keep the default values.
Limits and Reservations

**Download Limit** can be any value between 1% to 100%. It limits the maximum amount of download bandwidth available to this priority under any circumstance.

**Upload Limit** can be any value between 1% to 100%. It limits the maximum amount of upload bandwidth available to this priority under any circumstance.

**Download Reservation** can be any value between 1% to 100%. It guarantees the minimum amount of bandwidth available to this priority should it be needed under any circumstance.

**Upload Reservation** can be any value between 1% to 100%. It guarantees the minimum amount of bandwidth available to this priority should it be needed under any circumstance.

For example: By default the *Medium* priority is limited to 100% of the download bandwidth and is guaranteed at least 12% of the download bandwidth. By default the *Medium* priority is limited to 100% of the upload bandwidth and is guaranteed at least 12% of the upload bandwidth.

### The 7 Priorities

The 7 priorities in the default configuration can be thought of as two sets. The top four priorities: *Very High, High, Medium* and *Low* can all consume all the bandwidth available if no higher priority class wishes to use it. The bottom three priorities *Limited, Limited More,* and *Limited Severely* are always limited regardless of other priorities’ bandwidth consumption, because their download and upload limits are set to less than 100%.

Some amount of bandwidth is always guaranteed (by the reservation) to each priority. This is to prevent any priority from being fully starved and being disconnected from the internet because higher priorities are using all the bandwidth. When a higher class is not using its reservation, the leftover is re-assigned to the lower classes based on the ratio of their reservations.
Examples

Below are a few examples going from simple to more complex.

1) The network is completely idle except for one Medium priority download. This download is given all the available bandwidth and happens at full speed because no other priorities are using any traffic and the Medium download limit is 100%.

2) The network is completely idle except for one Low priority download. This download is given all the available bandwidth and happens at full speed because no other priorities are using any traffic and the Low download limit is 100%.

3) The network is completely idle except for one Limited More priority download. This download is given only half the available bandwidth because the reservation of Limited More is only 50%. The other 50% remains unused.

4) The network is fully saturated and all seven priorities have several active downloads running. All Very High Priority downloads equally split 60% of the download bandwidth (the Very High reservation). All the other priorities split their reservations in a similar fashion all the way down to Limited Severely which splits the 1% reservation between all Limited Severely Sessions.

5) One Medium priority download and one Low priority download are running simultaneously. Because the other priorities are not using any of the reservations the left over is split relative to the Medium and Low reservations (5:12 or roughly 1:2.5). As such the Medium priority download runs roughly 2.5 times faster than the Low priority download and together they consume all available bandwidth. (example: Low priority runs at 100kB/sec while the Medium runs at 250kB/sec and the total available bandwidth is 350kB/sec)

6) Two Limited Severely downloads are taking place simultaneously. All sessions in the same priority share the resources of that priority so the two sessions split the priority's resources. Because all other priorities are not in use the two split the bandwidth limit (10%) and each download runs at 5% of the total available bandwidth.

7) There are two WAN interfaces and WAN Balancer is balancing traffic across the WANs. One Medium priority download is happening on WAN1 and one Low priority download is happening on WAN2. The Medium priority download is given 100% of the WAN1’s bandwidth and the Low priority download is given 100% of WAN2’s bandwidth.

8) There are two WAN interfaces and WAN Balancer is balancing traffic across the WANs. One Medium priority download is happening on WAN1 and one Limited More priority download is happening on WAN2. The Medium priority download is given 100% of the WAN1’s bandwidth and the Limited More priority download is given 50% of WAN2’s bandwidth.
Using Priorities

The top four priorities are used for differentiating between normal and important traffic. Giving interactive or important applications and traffic higher priority can greatly improve the internet experience when the link is busy, but allows for all traffic to use resources that are available at any time.

The bottom three "limited" priorities are usual in "punitive" situations where the goal is to restrict traffic regardless if there is more bandwidth available. It is also useful in locations when bandwidth is paid for on a usage basis or bandwidth quotas are being used.

Special Notes

- Any given TCP download uses upload bandwidth to communicate to the sender that the data is being received. Usually this upload bandwidth is only a little, but sometimes if there is very little upload bandwidth available it can actually be the limiting factor in the total rate of the download. The receiver can only communicate with the sender to tell it that data is being received sporadically and as such the sender will slow down. This is especially common with assymetric links, especially if other uploads are in progress.

- Because packets are often approximately 1500 bytes (the MTU size), the lower priorities must either send the packet or not send the packet. Splitting the packet and sending a portion is not an option. As such the packet will be sent to prevent starvation but may actually exceed the 1% reservation at times. This is especially true on small links with very little bandwidth. As such the granularity of the limits and reservations on small links may be slightly skewed.

- WANs are treated completely seperately. Rules run on all traffic, regardless of which WAN the traffic is going out. However the bandwidth setting on each WAN is separate and they are treated as separate resources that are divided amongst traffic independently.

- All sessions within the same priority are given equal treatment using Stochastic Fairness Queueing or SFQ.

QoS Statistics

QoS Statistics is a status readout of recent activity. The Statistics are reset at reboot and when settings are saved. It is useful for diagnosing which rules are being matched and that the proper priorities are getting assigned. It is also useful to test the total usage of each priority.
QoS Statistics

The statistics are broken up by WAN interface. For example, *External - Outbound* shows the priority byte counts of all traffic going out the External WAN while *External - Inbound* shows the priority byte counts of all traffic coming in the External WAN.

QoS Current Sessions

*QoS Current Sessions* shows a table of all current active sessions and the assigned priority of each.

This is useful for testing to assure that priorities are being given the correct priority.

*Note*: Sessions are assigned priorities at creation time. When rules are changed active sessions will keep their current priority - only new sessions will be run against the new rules.
QoS FAQ

How are multiple WANs handled?

WANs are treated completely separately, but the same set of rules are evaluated on all traffic. The bandwidth settings of each WAN must be set correctly and independently, but there is no need to maintain separate rule sets beyond that.

Why is my internet slow when I enable QoS?

Likely because your WAN bandwidth settings are too low. Check out the WAN Bandwidth section for more help on setting these values.

QoS is not helping my high priority applications. Why?

This is likely because your WAN bandwidth settings are too high and QoS is having no effect or you simply do not have enough bandwidth to support your high priority applications regardless of low priority traffic. Check out the WAN Bandwidth section for more help on setting the bandwidth values.

Why do custom rules only match bypassed traffic?

Non-bypassed traffic is handled differently because it goes through the Untangle network stack - not the normal Linux packet flow. You can use the Bandwidth Control application to assign priorities to non-bypassed traffic.

Does QoS work on non-WAN interfaces?

No. Only WAN interfaces have limits and are subject to QoS manipulation. If you have a DMZ with local servers all communication between that network and the internal network is not subject to QoS.

Does QoS work with PPPoE interfaces?

No. PPPoE uses a special interface and is not supported by QoS.
**Multi-WAN**

**About Multi-WAN**

This is the capability to configure your network to simultaneously connect to the outside world with two (or more) different connections provided by two different ISP’s. There may be many reasons why you would want to do this, but the most common are:

- Load Balancing
- Failover
- Increasing available bandwidth beyond what is offered by a single ISP.

While you can run all normal internet traffic across all WAN connections, you **cannot** currently do the following operations on any secondary WAN connections:

- Remote Administration
- OpenVPN
- PC Remote
- Remote Access Portal

**What you need**

![A simple multi-WAN connection](image-url)
Setting up Multi-WAN is simple, but there are a few requirements in order to get started.

- First, you need two internet connections provided by your ISPs.
- Second, you must have at least three network interface cards installed in your Untangle server.
  - If you are not using a DMZ in your local network, the DMZ interface will be converted to a second WAN connection.
  - If you are using a DMZ connection, you must add an additional interface card to be able to provide internal, DMZ, and multiple WAN connections.
- Last, you must configure the second WAN connection. We'll do that next!

**Configuring Multi-WAN**

There are three network configuration steps necessary to set up Multi-WAN. In the following example, we will convert the DMZ interface to a second WAN interface. A printscreen is provided for each. You can click on each printscreen to see a full-size graphic if needed.

- Go to **Config -> Networking** and verify you are in **Advanced Mode** (upper right corner).
- Click on the **Interfaces** tab. You will see the installed interface cards. Note that the external interface has the **wan** notation.
- Click on **Edit** for the DMZ interface.
- Select the **is WAN interface** checkbox, then enter the **Primary IP address, netmask, default gateway and DNS address**. Click **Save** when done.

At this point, Multi-WAN configuration is done and route tables can be used to direct specific internal traffic to either one of the two WAN interfaces. The additional Load Balancing and Failover modules provide the most useful implementation of the Multi-WAN network configuration. These modules provide for automatic traffic distribution across available WAN's and traffic redirection in case of Internet connectivity failure on a WAN.

**Multi-WAN FAQs**

**I just ran the Setup Wizard and I was not asked any questions about my WAN connections. How do I set up multiple WANs?**

It's not part of a basic installation. Here's how to setup Multi-WAN.

**Why won’t OpenVPN use both of my WAN connections?**
The OpenVPN configuration files specify only the WAN address that is listed as your External interface.

**Can I use Remote Access Portal on both of my WAN connections?**

No. Remote Access Portal will only function on your primary WAN connection.

**Can I use PC Remote on both of my WAN connections?**

No. PC Remote will only function on your primary WAN connection.

**Can I use Remote Administration on both of my WAN connections?**

No. Remote Administration will only function on your primary WAN connection.

**Do I have to buy another certificate now that I have multiple WAN connections?**

Only if the additional external WAN connection(s) would be used for an additional domain name. If you are only using one domain name, your existing certificate is all you need.

**Does Untangle multi-WAN support give me a bonded connection?**

No. A bonded connection combines the bandwidth of multiple internet connections from a single ISP into a single physical connection, and often requires additional hardware at each end of the connection.

**I have 2 IP addresses from my ISP, why can’t I get Multi-WAN to work?**

Your ISP may give you two or more IP addresses, but if the addresses share the same physical WAN internet connection, you have just one WAN.

**I have 2 WAN connections from 2 different ISP’s, but I can’t get Multi-WAN to work.**

Check to see if the IP addresses are in the same subnet. If so, this will not work. You need to get one ISP to give you a different IP address.

Each WAN interface needs to be in a different subnet.

**I have installed and configured WAN Balancer and/or WAN Failover and nothing is happening. What should I do?**

Check your Multi-WAN setup to make sure that you've set this part up properly.

**I have 2 WAN's and I want to put all my FTP traffic on one and all my HTTP traffic on the other. Can I do it?**

As a general rule, no. If you can define the external destination of all FTP traffic, you may be able to use Static NAT to accomplish this.
I have a destination web site that requires authentication from a specific WAN interface. Can I do it?

Yes, by adding a static route in Config -> Networking -> Advanced -> Routes traffic to a specific target IP or IP range can be force to use a specific WAN interface. In routes table enter the following information.

- Target = destination IP or IP range
- Netmask = destination netmask
- Gateway = The gateway of the WAN interface you wish the traffic to the traffic to use.
Packet Filter

About Packet Filter

Packet Filter configures the linux firewall called IP tables/Netfilter. The Untangle Server provides a Firewall, but each meets a different set of needs.

Use Packet Filter instead of Firewall only if:

- You wish to filter what is available on the Untangle Server. For example, you wish to block certain services on the server itself (administration, ssh, etc)
- You need advanced use-cases that may not be supported in Firewall

Adding Packet Filter Rules

Untangle Server provides a default list of *system packet filter rules* for IP tables/Netfilter:

- **Enabled.** These rules are enabled by default, and represent those rules that enabled by default when the Untangle Server’s router is in basic mode.
- **Disabled.** These rules are useful in advanced configurations, though not needed by default.

If the system packet filter rule that you need does not exist in the default list, you can add a custom packet filter rule (called *user packet filter rules*). Untangle is curious about the rules that users add to the Untangle Server, so contact Untangle Technical Support to let us know when you add custom rules so that Untangle can determine if those rules need to be added to the default list--to make life easier for all users. Thank you!

**To add a custom packet filter rule:**

1. From the Navigation pane, choose **Config > Networking**.
2. In From the **Advanced** drop-down menu, select **Packet Filter**.
3. In the **User Packet Filter Rules** table, click the add button. An Edit window appears. The rule is enabled (On) by default.
4. Provide an optional description for the rule. Follow the contention for the list of default rules.
5. Specify the packet filter instructions. If you have specific questions, refer to the IP tables man page.
   a. Select a target (action):

| **Pass**    | This action permits a packet to traverse the firewall just as if the firewall weren't present. |

Blitz Networking Systems - c/Caldes de Montbui 118 - 17003 - Girona - Spain- +34 972486160 - ventas@blzwall.com– http://www.blzwall.com
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject</td>
<td>This action has the same result as Drop, except that the sender is sent an ICMP &quot;port unreachable&quot; error message.</td>
</tr>
<tr>
<td>Drop</td>
<td>This action prohibits a packet from passing, and does not send a response to the sender.</td>
</tr>
</tbody>
</table>

b. Select the type.

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Matches the IP address of the host that sent the traffic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Address</td>
<td>Matches the destination IP address of the session.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Matches the destination port (server port).</td>
</tr>
<tr>
<td>Destined Local</td>
<td>Matches traffic destined to any of the the Untangle server's IPs or aliases.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Matches the transport or network protocol that the traffic uses.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Matches the network interface on the Untangle Server that first receives the traffic.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Matches the IP address of the host that created the session (client).</td>
</tr>
<tr>
<td>Source Mac Address</td>
<td>Matches the Mac Address of the client NIC that sends the traffic (N.B. dash notation, not case sensitive e.g. 00-3E-22-0B-9F-F7 and 00-3E-22-0B-9F-F7 are both valid)</td>
</tr>
<tr>
<td>Source Port</td>
<td>Matches the source port (client port). <strong>Note:</strong> This is normally a random number chosen by client. Do not use unless you know what you are doing.</td>
</tr>
</tbody>
</table>

6. Click **Update**. The new rule appears as a row in the table.
Bypass Rules
About Untangle Virtual Machine

In most cases, you don't need to know that there is an Untangle Virtual Machine (UVM). However, there is no "getting around" this component in the context of bypass rules.

Bypass rules enable specific traffic to bypass the UVM. The UVM is an Untangle Server process—a Java virtual machine, that processes all traffic that reaches the Untangle Server. By default, whether your Untangle Server is a bridge or gateway, the Untangle Server traffic always passes through the UVM, then on to the racks.

Traffic can never reach the racks without first going through the UVM. So, if the traffic doesn't pass through the UVM, then it never makes its way to the racks. Traffic that has a bypass rule (e.g. VoIP) enters an interface and goes directly to Linux kernel, then exits another interface; in this case, the Linux kernel, not the UVM, processes the traffic.

Creating User Bypass Rules

When you create a bypass rule, you're really creating a user bypass rule. There are two types of bypass rules:

- **User bypass rules.** Bypass rules that do not exist by default, and that you can add yourself.
- **System bypass rules.** Bypass rules that exist by default (e.g VoIP), and that come preconfigured with the Untangle Server.

Untangle is curious about the rules that users add to the Untangle Server, so contact Untangle Technical Support to let us know when you add bypass rules so that Untangle can determine if those rules need to be added to the default list—to make life easier for all users. Thank you!

Bypass rules enable you to use technology that wouldn't otherwise work in an Untangle Server environment because the traffic requires special handling: it either depends on Windows protocol (for example, IPSEC/PPTP) or it is time-sensitive (for example, VoIP). To deal with such special handling, bypass rules instruct specific traffic to bypass the Untangle Virtual Machine (UVM). However, in the case of VoIP, the Untangle Server is preconfigured with a default bypass rule, so VoIP works "out of the box" without the typical VoIP performance and reliability problems.

A bypass rule is commonly used for high priority protocols such as SIP, which is used for VoIP. The Untangle Server bypass rules support SIP and Asterisk sessions only. SIP is an application protocol that establishes VoIP sessions between caller and sender. Underlying SIP is usually UDP or TCP transport protocols. There are many VoIP software applications that support SIP and Asterisk. The Untangle Server bypass rules don't support sessions such as RTP and H323, which Microsoft Netmeeting uses to make VoIP calls.
To create a bypass rule:

1. From the Navigation pane, choose **Config > Networking**. The Network Configuration page launches.

2. From the Advanced drop-down menu, select **Bypass Rules**.

3. Specify how you want the Untangle Server to identify the traffic, then click **Save**. Here are few examples:
   - **VoIP traffic.** SIP uses either TCP or UDP protocol and usually on port 5080, 5060, or 5061.
   - **PPTP VPN connections.** PPTP uses TCP and usually on port 1723.
   - **IPSEC VPN connections.**

<table>
<thead>
<tr>
<th>Source Address</th>
<th>The IP address of the host that sent the traffic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destined Local</td>
<td>Any external interface or external IP address on the Untangle Server. You don't need to specify a value because &quot;any&quot; is the value by default.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The IP address of the host that will receive the traffic.</td>
</tr>
<tr>
<td>Source Port</td>
<td>The port on the Untangle Server that first receives the traffic.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>The network interface on the Untangle Server that first receives the traffic.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The transport or network protocol that the traffic uses.</td>
</tr>
</tbody>
</table>

**Next Step:** To improve QoS, enable Untangle QoS. Bypass rules DO NOT bypass the QoS system because QoS is handled outside of the Untangle virtual machine. If you are using Bypass rules for the sole reason of latency and priority, add a corresponding QoS rule, marking the same traffic as High.

**Bypass Rules vs. Protocol Control**

You can use both bypass rules and Protocol Control because they serve two, completely different functions:

- Use Protocol Control to implement policies.
- Use bypass rules to ensure that specific traffic bypasses the Untangle Virtual Machine (UVM).
Route Management

About Untangle Server’s Routing Table

The Untangle Server’s Route Management tool consists of two tables:

- **Static Routes.** Shows the static routes that you manually added.
- **Active Routes.** Shows the Untangle Server’s “live” routing table.

The Active Routes—the routing table—is what is used to determine where the Untangle Server must send packets based on their destination IP address. When you configure the Untangle Server’s interfaces, the Untangle Server adds a default list of entries to the Active Routes table, assuming the Linux kernel supports the interfaces. The default list is the default gateway to the Internet, plus one entry for each subnet configured for an interface, signifying that this subnet can be reached on this interface.

Routing Network Traffic

In some deployments, hosts might not directly connect to the Untangle Server, yet the traffic from one host needs to be directed to another host. Using static routes, you can configure the Untangle Server to direct traffic that is destined for a network to a specific host.

The Untangle Server evaluates rules in the order that they are listed, starting with the first rule in a table. For each new connection, the Untangle Server evaluates the traffic against active rules until a match (if any) is found. When a match is made, traffic is routed as specified by the rule.

**To create a static routing rule:**

**Before You Begin:** Ensure that your Router is in Advanced Mode.

1. From the **Navigation pane**, choose **Config > Networking**.
2. In the **Advanced** drop-down list, select **Routes**.
3. In the **Static Routes** table, click the add (+) button. A new row appears in the table.
4. In the new row, specify the static routing rule:

<table>
<thead>
<tr>
<th>Target/Netmask</th>
<th>These fields specify the network that will have its traffic routed. Valid values are in IP address/netmask format.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>This field specifies the host that receives traffic that is routed from the specified network. Valid values are in IP address format.</td>
</tr>
</tbody>
</table>
5. Click **Save**.
Static ARP Management
About ARP Entries

Each computer on your network has an IP address, but a computer's network interfaces have MAC addresses, not IP addresses. When on the same subnet (on the Untangle Server), if Computer A wants to send data to Computer B, it needs to know two things:

- Destination IP address for Computer B
- MAC address for Computer B

ARP (Address Resolution Protocol) is a protocol that associates a computer's IP address and MAC address so that Computer A has all the information it needs to communicate with Computer B. Basically, using an ARP broadcast, Computer A shouts out What's the MAC address for IP Address 216.27.180.1?, then Computer B shouts back, That's me! My MAC address is 00:90:1A:40:AA:4D. Talk to me baby!

Like other routers, the Untangle Server can automatically make this translation if Computer A and Computer B are on the same segment. But, sometimes you don't want to use this automatic mapping; you'd rather have fixed (static) associations between an IP address and a MAC address. The Untangle Server provides you the ability to add static ARP entries to:

Protect your network against ARP spoofing. An unauthorized computer can sniff around, waiting for the right ARP request. Then, responds with its own MAC address, claiming to have the IP address of an important server or router.

Prevent network confusion as a result of misconfigured computers. A host that has been misconfigured with the ip address of another router or server will confuse all the other computers on its subnet. A host with a static ARP entry for the true router or server will not be confused. Don't forget to clear the misconfigured client's cached ARP table.

Enable computers to talk to primitive network devices. Some devices don't speak the ARP protocol, so their MAC addresses must add as ARP entries so that they can communicate with other network computers. This situation is rare these days.

Adding ARP Entries

As outlined in About ARP Entries, there are specific reasons why you might not want to use dynamic ARP. The Untangle Server provides you the ability to add static ARP entries to bypass dynamic ARP.

To add an ARP entries:

1. Retrieve the IP address and MAC address of the device that requires the ARP entry.
   - From Windows Server command prompt, run ipconfig/all command.
   - From Solaris and Linux command prompt, run ifconfig -a command.
2. From the Navigation pane, choose Config > Networking.
3. In the Advanced drop-down list, select ARP.
4. Click the Add button. A new row appears in the Static ARP Entries table.
5. Specify the IP address and MAC address of the device, then click Save.

If the entry is for a misconfigured client, clear the client’s ARP table. For ARP to be efficient, each computer caches IP-to-MAC address mappings to eliminate repetitive ARP broadcast requests. There are various public scripts that use the arp command to do the trick.

From any network computer, test that the entry is working. From a command prompt, run `arp -a` command.
Untangle Configuration

These options are available under the Config tab of the GUI and are broken down by section:

Administration

<table>
<thead>
<tr>
<th>Tab</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Accounts</td>
<td>• About Administrator Accounts</td>
</tr>
<tr>
<td></td>
<td>• Creating, Deleting or Editing an Administrator's Account</td>
</tr>
<tr>
<td></td>
<td>• Resetting the Password for Administrator's Account</td>
</tr>
<tr>
<td></td>
<td>• Enabling Remote Access To Untangle Server</td>
</tr>
<tr>
<td></td>
<td>• Restricting Remote Access To Untangle Server</td>
</tr>
<tr>
<td>Public Address</td>
<td>• About Untangle Server's Public (Internet) Address</td>
</tr>
<tr>
<td></td>
<td>• Specifying Untangle Server's Public (Internet) Address</td>
</tr>
<tr>
<td>Certificates</td>
<td>• About Digital Certificates</td>
</tr>
<tr>
<td></td>
<td>• Generating a Self-Signed Certificate</td>
</tr>
<tr>
<td></td>
<td>• Using an SSL Certificate</td>
</tr>
<tr>
<td>Monitoring</td>
<td>• About Monitoring</td>
</tr>
<tr>
<td></td>
<td>• Enabling SNMP Monitoring</td>
</tr>
<tr>
<td></td>
<td>• Enabling Syslog Monitoring</td>
</tr>
<tr>
<td>Skins</td>
<td>• Specifying a Skin</td>
</tr>
<tr>
<td></td>
<td>• Changing the Skin</td>
</tr>
</tbody>
</table>
Admin Accounts
About Administrator Accounts

Administrators are users who are able to launch the Untangle Server's interface, the Untangle Client, to administer the Untangle Server. End-users, individuals who browse the web and receive email, do not need to log on to the Untangle Server.

Creating, Deleting or Editing an Administrator's Account

To add an administrator account:

1. From the Navigation Pane, click the Config tab > Administration.

2. In the Admin Accounts area, click the add (plus) button to the left of the table, adding a new (blank) row to the table.
   - Description - The full name of the user, such as Emma Scott or Jun Wang.
   - Login - A login name, such as escott or jwang.
   - Email - The user's email address. You can leave this field blank.
   - Password - The user's admin password.

3. Click the Save button. The new account is now active.

To delete an administrator's account:

1. From the Navigation Pane, click the Config tab > Administration.

2. In the Admin Accounts area, click the delete (X) button to the right of the account that you want to permanently delete.

3. Click the Save button.

To change the password for an administrator's account:

1. From the Navigation Pane, click the Config tab > Administration.

2. In the Admin Accounts area, highlight the account (row) that you want to change, click on the change password icon, type the new password, then confirm new password field.

3. Click the Save button.
Resetting the Password for Administrator's Account

If you forgot the password for admin, you must reset the password. If you created any additional administrator accounts, when you reset the default administrator's account, the Untangle Server deletes all the administrator accounts that you created. After you reset the password, the Untangle Server informs you of the newly-assigned password.

To reset the password for an administrator's account:

1. Ensure that the Untangle Server is turned on.
2. Connect a monitor, keyboard, and mouse to the Untangle Server. The monitor displays the Untangle Client.
3. In the Navigation bar, click the Recovery Utilities button.
4. When the Recovery window appears, click the Yes button. A terminal window appears.
5. Scroll to Reset Administrative Accounts, and hit Enter. The following question appears: Reset administrative accounts to factory defaults (admin/passwd)?.
6. Select Yes. The Untangle Server resets the password and informs you of the newly-assigned password. Once you log in to the Untangle Server using that newly-assigned password, the Untangle Client forces you to assign a new password.

Enabling Remote Access To Untangle Server

External Access is access whereby someone can connect to the Untangle Server and applications from outside the protected network. Someone from the DMZ is considered outside. All traffic passes over a secure (SSL) connection. External access using http and https is always enabled, but can be disabled.

Internal Remote Administration is access whereby someone can connect to the Untangle Server and applications from within the protected network either through http or https. Internal access using http and https is always enabled, and cannot be disabled.

To enable external access to the Untangle Server:

1. From the Navigation Pane, click the Config tab > Administration.
2. In the External Administration area, select the Enable External Administration check box.
3. Do one of the following:
If you want to restrict access from a set of computers, click the **Restrict external access to these external IP address(es)** radio button, and provide the IP addresses and netmask for the computers.

If you do *not* want to restrict access from a set of computers, click the **Allow external access from any IP address** radio button.

4. Click the **Save** button.

5. If your Untangle Server is a bridge and not a router, do the following:
   
   a. Click the **Public Address** tab.
   
   b. Select the **Use Manually Specified IP** radio button.
   
   c. Type in the IP Address of the router.
   
   d. If **port 443** is in use by another system, choose a different port; otherwise, accept the default and click **Save**. If you do not know which port to use, accept the default.
   
   e. Click the **Save** button.
   
   f. Go to your router and create a rule to all traffic destined for port 443 to the Untangle Server.

*Next Step:* Ensure that you can log on remotely. Go to Logging On To Untangle Server.

---

**Restricting Remote Access To Untangle Server**

**To restrict external access to the Untangle Server:**

1. From the **Navigation Pane**, click the **Config** tab > **Administration**.

2. In the **External Administration** area, clear the **Enable External Administration** check box.

3. Click the **Save** button.
Public Address
About Untangle Server's Public (Internet) Address

Is your Untangle Server behind an existing router? If so, that router provides Internet access to your network, and not your Untangle Server. Therefore, the Untangle Server needs to know the IP address for that router because some applications send URL links that require the correct external address. For example, the public address is used in Quarantine Digest emails and report emails so the user can always use the URL that is embedded inside the email. (If you have offsite employees, you'll want to read this FAQ: Why can't my off-site users get their Quarantine Digests.)

Specifying Untangle Server's Public (Internet) Address

- If you have Router (w/NAT) -> Untangle -> Local Network, specify the public address of the router and add a port forward to the router, in order to access the Untangle Server from the links in the Quarantine Digest emails (go to About Untangle Server's Public (Internet) Address).

You can set up an Untangle Server behind a router or other network device that redirects or port forwards traffic (Redirecting External and Internal Traffic) to the Untangle Server, but there really is no need for the router because the Untangle Server can do everything (and more) than the router. But, if there is a reason you need this configuration, simply have the router redirect all traffic on its IP address for port 443 to the Untangle Server's port 443. In such a scenario, the Untangle Server's address is not the address used from the Internet (the public address). In this case, from outside the corporate network, you cannot access the Untangle Server unless you specify, on the Untangle Server, the IP address and port that will be used for Internet access.

Note: The default port for external access is 443. It is permissible to use a port other than 443 on the Untangle Server, but the device performing redirection must honor 443 as the external mapping.

- If you have Untangle (w/NAT) -> Local Network, and it has a dynamic address, use something like Dyndns to get a Dynamic DNS entry so that you can always use the Untangle Server's hostname.

To change Untangle Server's public address:

1. From the Navigation Pane, click the Config tab > Administration.
2. Click the Public Address tab.
3. Select the Use Manually Specified IP radio button.
4. Specify the IP address and port that will be used for Internet access to the Untangle Server, and click the Save button.

Next Step: If you want to enable remote access to the Untangle Server, go to Enabling Remote Access To Untangle Server.
Certificates
About Digital Certificates

Your Untangle Server uses digital certificates when using SSL. Without a properly installed and signed certificate, users who browse to the Untangle Server receive warning messages from their browser as shown in Figure, Browser Error: Unknown Certificate Authority. To prevent this annoyance, install a certificate. Go to Preventing Web Browser Errors (Unknown Authority). The Administrative Console, as well as the Quarantine features use SSL for user interaction.

Digital Certificates are used by a web server to identify itself as demonstrated in the following example:

If you visit amazon.com to purchase a book, the checkout procedure performs the following actions associated with the transaction:

1. You are redirected to a secure web site which uses SSL.

2. The transaction page (checkout) is painted on your screen, including product information and any cookie/session-based information pertaining to the purchase.

3. You enter in the remaining information necessary to complete the transaction.

4. SSL encrypts your web session to prevent any malicious parties from intercepting your personal information.

5. Your browser requested Amazon.com's Digital Certificate to make sure you were in fact visiting amazon.com. Your browser is asking Amazon for proof of identity. You can think of the digital certificate as a driver license or a passport.

6. The web server authenticates. Your browser knows that you typed www.amazon.com, and expects the web server to return a certificate which declares this is www.amazon.com. Since a Digital Certificate is easy to create, your browser verifies that the certificate is authentic. This is done by examining the digital signature on the digital certificate against a list of known certificate authorities.

All browsers come with a list of certificate authorities, along with information to validate when those authorities sign web server certificates. The digital certificate for www.amazon.com is signed by a Certificate Authority named Verisign. When Amazon presented its certificate to your browser, your browser went through the following steps:

1. Visited a web site with the address www.amazon.com and requested its digital certificate.

2. Examined the returned certificate and found that it claimed to be for a site called www.amazon.com. If the address you entered into your browser did not match the name of the certificate, the browser would have issued a warning that the name of the certificate does not match the visited site.
3. Found that this certificate was signed by an authority named Verisign. The browser then went through its list of pre-installed Certificate Authorities and found an entry for Verisign. Otherwise, the browser would have issued a warning that the certificate was signed by an unknown authority.

4. Verified the signature on Amazon's certificate was in fact the signature of Verisign. Otherwise, the browser would have issued a warning that the signature was invalid.

Unlike with Amazon, a new Untangle Server installation causes the browser to issue warnings because the Digital Certificate that the Untangle Server uses is not signed by a known Certificate Authority. The initial (default) certificate is a self-signed certificate, which is equivalent to not signed by anyone known to the browser. Again, to prevent this annoyance, install a certificate. Go to Preventing Web Browser Errors (Unknown Authority).

**Preventing Web Browser Errors (Unknown Authority)**

Browser Error: Unknown Certificate Authority

To prevent the annoying web browser errors as outlined in About Digital Certificates, do one of the following:

- When you receive the error message, select the **Accept this certificate permanently** radio button.
- Generate a self-signed certificate.
- (Recommended) Use an SSL certificate from a CA.

**To install a digital certificate:**

Obtain a digital certificate by doing one of the following:

**Generating a Self-Signed Certificate**

A self-signed certificate isn't ideal.

**To generate a self-signed certificate:**

*Before You Begin:* Ensure that your Untangle Server's hostname is known to the Internet. Go to Specifying Untangle Server's Public (Internet) Address.

1. From the *Navigation Pane*, click the *Config* tab > *Administration*. The Administration Config window appears.

2. Click the *Certificates* tab.

3. In the *Generation* section, click the *Generate a Self-Signed Certificate* button. The Generate Self-Signed Certificate window appears.

4. Specify the company's name and location information, and click the *Proceed* button. You do not need to provide the hostname because the Untangle Server provides this information automatically.

**Using an SSL Certificate**

In order to use an SSL certificate from a third party, it is important to follow all of the following steps.

1. change the hostname of your untangle box
2. generate a new self-signed certificate
3. generate a new CSR (verify that the information is correct).
4. submit CSR to third party CA
5. install returned certificate & any intermediate certificates from the certificate authority.
Create a Certificate Signature Request

A Certificate Signature Request (CSR) is a standard digital document accepted by all certificate authorities as the initial step in the process of obtaining a digital certificate.

To create a CSR:

Before You Begin: Ensure that your Untangle Server's hostname is known to the Internet. Go to Specifying Untangle Server's Public (Internet) Address.

1. From the Navigation Pane, click the Config tab > Administration. The Administration Config window appears.

2. Click the Certificates tab.

3. Click the Generate a Certificate Signature Request button. The Certificate Signature Request window appears.

4. From the Certificate Signature Request window, click the Proceed button. The Untangle Client populates the window with several lines of text starting with ----- BEGIN NEW CERTIFICATE REQUEST ----- . This text is your CSR.

5. Save the CSR by selecting the text in the Certificate Signature Request window and by saving the text to a text file. You will need this information

Purchase a Public Key Certificate

Purchase a digital certificate from a well-known certificate authority (CA). Examples of CAs include Verisign and Thawte. Some Untanglers use GeoTrust. Many CAs charge varying fees for a digital certificate.

To purchase an SSL certificate:

1. Go to the website of a certificate authority, and purchase an SSL certificate.

2. Cut and paste the CSR that you created in Create a Signature Request into the form that your certificate authority provides.

   o The certificate authority might also request additional information to verify that you are the "owner" of the website for which you are requesting the certificate.

   o Afterward, the certificate authority returns a signed digital certificate for your Untangle Server.
Import a Public Key Certificate

To import a digital certificate from a CA:

1. From the Navigation Pane, click the Config tab > Administration. The Administration Config window appears.
2. Click the Certificates tab.
3. In the Generation section, click the Import a Signed Certificate button.
4. Install the certificate into the Untangle Server by copying and pasting the certificate into the Import Signed Certificate window, and click the Proceed button. The certificate was either emailed or received in a web browser.
5. If your CA provided a second, intermediate certificate, paste it into the bottom window.

Note: Some free or open-source CAs provide such certificates. To learn about intermediate ("chained root") certificates, go to SSL Certificates: Chained Root vs. Single Root.
Configuring Monitoring
Enabling SNMP Monitoring

SNMP is a protocol typically used by Managed Service Providers (MSPs) to monitor and manage systems. Untangle Server follows SNMP standards for its SNMP support. As such, Untangle Server should work with any SNMP monitoring tool so long as that tool adheres to the standard. When a tool has a unique implementation, Untangle provides the vendor connectors to work with Untangle Server. If you’d like to see Untangle produce an extensive monitoring tool, or you currently use a third-party tool that you love, let us know!

Please note that any applications requiring the installation of an agent to the Untangle box are not supported - if you install an agent (or any 3rd party software) onto an Untangle box we cannot support that installation.

Some examples of tools that work with Untangle Server (again, any tool that adheres to the SNMP standard should work with Untangle Server) are Cacti, Net-SNMP, Nagios, Level Platforms, Kaseya, MRTG, and Munin. Some of these tools provide just the yummy statistics and pretty graphs, and others provide additional features such as alerts.

Untangle Server supports access to its UTMs (Untangle Server’s software products; also called nodes by developers). In the future, Untangle Server will provide statistics on the Untangle Virtual Machine. Untangle Server does not support configuration operations at this time, but does support all monitoring operations, including traps.

To enable SNMP monitoring:

1. From the Navigation pane, choose Config > Administration.
2. Click the Monitoring tab.
3. In the SNMP area, click the Enable SNMP Monitoring radio button and, optionally, Enable Traps radio button. Traps are rarely used today, but Untangle Server provides this functionality for special configurations.
4. Type the appropriate configuration information, then click Save Settings.

| Community (Get) | This community is for a Get* operation, which is the most common method of communication. An SNMP community is the group to which devices and management stations running SNMP belong. The SNMP community defines where information is sent. The SNMP community acts as a password. Untangle Server will not respond to requests from management system that do not belong to its community. By default, this |
community is untangle.

<table>
<thead>
<tr>
<th><strong>System Contact</strong></th>
<th>Email address of the System Administrator that should receive SNMP messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Location</strong></td>
<td>Description of the system's location. Simply use the default if you don't want to specify a location.</td>
</tr>
</tbody>
</table>

**Community (Traps)**

This community is for a Trap or Inform operation, which is a rare method of communication. An SNMP community is the group to which devices and management stations running SNMP belong. The SNMP community defines where information is sent. The SNMP community acts as a password. Untangle Server will not respond to requests from management stations that do not belong to its community. By default, this community is untangle.

**Host**

The host name or IP address of the management system that is authorized to receive statistics from the Untangle Server.

**Port**

The default port for SNMP traps is 162.

---

**Enabling Syslog Monitoring**

Untangle Server supports the aggregation of syslog messages by being a syslog *sender*. To enable this support, simply install a syslog *receiver*, then enable syslog monitoring on the Untangle Server. Some syslog products are easier to set up than others. Kiwi, a third-party syslog daemon, is a favorite of many Untanglers using Windows, while those on *nix can use rsyslog.

**To enable Syslog monitoring:**

1. From the Navigation pane, choose Config > Administration. The Remote Admin Config windows launches.
2. Click the Monitoring tab.
3. In the Syslog area, click the Enable Syslog Monitoring radio button.
4. Type the appropriate configuration information, then click Save.

**Note:** Some syslog daemons define priority as a combination of facility and priority:
### Host
The host name or IP address of the Syslog daemon that is authorized to receive syslog messages from the Untangle Server. Do not set the Host to the Untangle box itself - this will result in the hard drive filling up very quickly and most likely crashing the box.

### Port
The typical port on which a Syslog daemon listens for UDP syslog messages is port 514. As such, the Untangle Server provides port 514 as the default. You can change this port if your Syslog daemon uses a different port.

### Facility
The facility that you would like to assign to the Untangle Server so that you can distinguish its syslog messages from other daemons, systems, or subsystems that submitted the error message. By default, Untangle Server select local 0, but you can change the facility to anything you want. Just make sure that it's not already being used.

Unfortunately, syslog doesn't allow you to create a custom facility with a descriptive name such as untangle, so you're stuck with the list of facilities that the Untangle Server (and all syslog senders) provide.

### Threshold
Another name for *priority*, and represents the importance of the message's content. The thresholds are listed in order of priority. The highest priority is emergency. The lowest priority is debug. Select the lowest priority messages that you want to receive. For example, if you want to receive all syslog messages with emergency, alert, and critical priorities, simply select critical. However, you can choose the lowest priority, allowing the Untangle Server to send all messages; then, you can configure your syslog daemon to filter out priorities.

5. Go to your syslog receiver to view your messages sent by the Untangle. Depending on the threshold that you specified, you might see messages immediately. If you don't see messages that you'd expect to see, let us know.
## Configuring Email Settings

<table>
<thead>
<tr>
<th>Tab</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Settings</td>
<td>• About Server Email</td>
</tr>
<tr>
<td></td>
<td>• Configuring Email Settings</td>
</tr>
<tr>
<td>From-Safe List</td>
<td>• About SafeLists</td>
</tr>
<tr>
<td></td>
<td>• Declaring an Email Sender as Safe</td>
</tr>
<tr>
<td>Quarantine</td>
<td>• About Quarantine</td>
</tr>
<tr>
<td></td>
<td>• Setting Time Period To Automatically Delete Quarantined Email</td>
</tr>
<tr>
<td></td>
<td>• Specifying Who Manages Quarantined Email</td>
</tr>
<tr>
<td></td>
<td>• Resending Quarantine Daily Digests</td>
</tr>
<tr>
<td></td>
<td>• Monitoring Quarantined Email</td>
</tr>
<tr>
<td></td>
<td>• Releasing Wanted Email and Purging Unwanted Email</td>
</tr>
</tbody>
</table>
Email Settings

About Untangle Server Email

The Untangle Server sends emails for several reasons:

- The Quarantine facility sends users a daily digest of the spams they received.
- The Quarantine allows users to "release" emails from the quarantine.
- The Reports sends daily summary reports to administrators about Untangle Server activity.

For these functions to work correctly, Email settings must be properly configured.

Configuring Email Settings

In order for the Untangle Server to send email, you must configure the Untangle Server with your outgoing mail server (also called SMTP server). If your company does not have its own outgoing mail server, consider that ISPs typically provide an outgoing mail server as part of their Internet service. This mail server accepts email messages.

- For someone that uses web email (for example, Yahoo or GMail), you may not even be aware that you have an ISP-provided email account.
- If you use ISP-provided email, and use a mail client like Outlook, Thunderbird or Mozilla mail to read your email, you at one time provided your email client the names of the incoming and outgoing mail servers. Your Untangle Server needs this information too.

To configure outgoing server email:

1. From the Navigation pane, click Config tab > Email. The Email Config window launches.
2. Click the Outgoing Server tab, and select the Send Email using the specified SMTP Server radio button.
3. Specify the following properties:

<table>
<thead>
<tr>
<th>Server Address or Hostname</th>
<th>The name of your SMTP mail server (for example, mail.mycompany.com or 4.79.181.14). Your company might have its own internal SMTP Email Server or use an Internet Server Provider’s SMTP Email Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Port</td>
<td>The standard port for sending email via SMTP is 25. You should only change this setting if you know your mail server is using a non-standard port.</td>
</tr>
<tr>
<td>Login/Password</td>
<td>For servers that use authenticated SMTP, which requires a username (for example, <a href="mailto:joesmith@sbcglobal.net">joesmith@sbcglobal.net</a>) and</td>
</tr>
</tbody>
</table>
password, specify the Login and Password. Otherwise, these can be left blank.

| Email From Address | Provides an email address for the sender, which is your Untangle Server. You can accept the default. |

4. Click the **Save** button.

5. Click the **Run Email Test** button, specify your email address, and click the **Proceed** button. If you receive an Untangle Server Test Message email, your Untangle Server is configured properly.
From-Safe List

About SafeLists

The concept of a safelist is the result of Spam filters that have high rates of false positives. False positives represent email that really isn't spam. Have you ever had a friend send you an automated email that says, "Joe, click on the link below so that you can be automatically added to my safelist"? Well, your friend knows that his Spam filter has a high rate of false positives so he wants to prevent email from you from going to his "quarantine". If you want to understand how false positives occur, read these sender tips.

Because Untangle Server's Spam Blockers don't have high rates of false positives, end-users cannot add users to their individual safelists unless email from those senders is quarantined. Basically, if you don't get false positives, you really don't need a safelist. Untangle Server is doing a good job, so why interfere, right?

Also, Untangle Server doesn't allow Administrators to set up a per user safelist unless the user has quarantine email. If a user doesn't have any quarantined email (theoretically, spam), then you don't need to add anyone to a safelist. Everything is making its way into the end-user's inbox, so no senders' emails are being quarantined. No need to worry!

Declaring an Email Sender as Safe

You can instruct the Untangle Server to always treat email from a given sender as wanted as opposed to unsolicited. The set of these good senders is a safelist. If you choose not to populate a safelist, there is no negative effect on the overall Untangle Server.

Populate a safelist based on emails that were incorrectly quarantined. As discussed in Releasing Wanted Email and Purging Unwanted Email, it's important to add the Untangle Server's Outgoing Mail Server to your safelist.

There are two types of safelists:

- **Global.** Apply to all your end-users.
- **Per User.** Apply to individual end-users.

As outlined in the Quarantine Digest page, your end-users can declare an email sender as safe too. From their Quarantine Digest, they simply click **Release** in the Action column, then select the email and click (Safelist) from the Safelist page.
Therefore, most of the time you'll only add senders to the Global safelist.

To declare an email sender as safe:

1. From the Navigation pane, click the Config tab > Email.

2. Click the From-Safe List tab, then do one of the following:

   - If you want to allow all users to receive email from the sender, in the Global area, specify the email address (johngmail.com) or domain (*.gmail.com) of that sender, then click Save.

   - If you want to allow a specific user to receive email from the sender, in the Per User area, specify the email address (johngmail.com) or domain (*.gmail.com) of that sender, then click Save.
Quarantine Configuration
As outlined in Creating Custom Policies, outgoing mail is not quarantined by default.

The Untangle Server has the ability to store emails suspected of containing unwanted content. This repository, a Quarantine, can then be reviewed to ensure no emails were mistakenly labeled as unwanted (sometimes called a false positive). The decision to quarantine emails is made by each Software Product (for example, Spam Blocker). There are two different types of users that have access to the Quarantine:

- **End user**: Person within the protected network who receives email. End users interact with the Quarantine using a web interface. End users can purge/release their own emails through a web interface, but cannot launch the Untangle Server's administrative interface.

- **Administrator**: Person with administrative privileges. The administrator uses the Untangle Server's administrative interface, Untangle Client, to control quarantined emails for many users.

The Quarantine stores emails that the Untangle Server suspects contain unwanted content (for example, Spam or phishing). This storage is done on a per-email address basis. For example, if escott@yourcompany.com receives three Spam emails in a day, those three emails are quarantined for escott. The collection of emails for a given address resides in an inbox.

If you specify that users receive a Quarantine Daily Digest, the Untangle Server emails users daily reports that contain a browser link to their specific Quarantine inbox. The daily digest emails are delivered in HTML format, such that they contain links to a web server. The web server is housed within the Untangle Server. From the Quarantine, users can manage their quarantined email. End users can release emails, causing them to be sent to their email clients, or delete them. In this way, the Quarantine Daily Digest emails enable end-users to maintain their inboxes.

You may also disable sending of Quarantine emails. If you elect to do this, users will not have the option to manage their quarantine. If you receive a huge volume of spam, you may need to modify the *Maximum Holding Time* if disk space is an issue for you.

Some users will choose not to act on (ignore) their digest emails. If a user ignores their inbox for many days (and receives many spams), their inbox will grow. This is not a concern, as the Untangle Server automatically deletes emails after a fixed period of time. This time period is configurable, as discussed in Setting Time Period To Automatically Delete Quarantined Email.

**Setting Time Period To Automatically Delete Quarantined Email**

By default, the Untangle Server deletes quarantined email every 28 days. However, you can decrease the holding period to free up disk space, or you can increase the holding period to retain quarantined email to give users more time to respond to quarantined email.
To change the holding period:

1. From the Navigation pane, click the **Config** tab > **Email**. The Email Config window appears.
2. Click the **Quarantine** tab.
3. In the **Maximum Holding Time** text box, specify the time period in days, then click **Save**.

**Setting Time Period To Automatically Send Quarantine Daily Digests**

By default, the Untangle Server sends Quarantine Daily Digest at 6am.

To change the sending time:

1. From the Navigation pane, click the **Config** tab > **Email**. The Email Config window appears.
2. Click the **Quarantine** tab.
3. In the **Digest Sending Time** drop-down list, change the time, then click **Save**.

**Specifying Who Manages Quarantined Email**

Untangle Server enables you to do the following:

- Enable Spam Blocker to quarantine email for some users and not for other users, and provide specific users the ability to manage their quarantined email themselves. To do so, you need to remove quarantinable addresses from the default configuration.

- Specify that a dedicated email account manage specific users quarantined email, or specify that a dedicated email account manage specific distribution list's quarantined email.

**To remove quarantinable addresses:**

In order for email recipients to manage their quarantined email, users must receive a Quarantine Daily Digest. If a user's email is quarantined, that user receives a Quarantine Daily Digest by default. The Quarantine Daily Digest contain a URL to the user's quarantine inbox. To learn more about this feature, go to About Quarantine.

When you configure Spam Blocker to scan and then quarantine email, it does so for all users—unless you specify otherwise. If you configure Spam Blocker to quarantine all users' email, and you want all users to manage their respective quarantined email, you do not need to do anything. However, if you do not want Spam Blocker to quarantine email for all users, and, instead, you simply want Spam Blocker to *mark* some users' email as spam, then perform the following procedure.

1. From the Navigation pane, click the **Config** tab.
2. Click the **Quarantine** tab.
3. In the **Quarantinable Addresses** area, delete the default row that contains the wildcard (*).

4. Create a table row for each user whose email you want Spam Blocker to quarantine, and specify users' email address in their respective table row. For all users not listed in the table, Spam Blocker simply marks the email as spam.

**Tip:** Depending on your Exchange Server, by default it might accept email from a spammer when the email is sent with the correct domain (@untangle.com)—but the wrong email address (for example, nosuchemployee@untangle.com). You might be inclined to use this list of quarantinable addresses to include all your company’s legitimate email accounts thereby rejecting all unknown email accounts. Before you do so, consider configuring your Exchange Server to reject such email as this technique will meet your needs and cut down on network traffic. Microsoft Exchange 2003 or later has a server setting that rejects email destined for unknown email accounts even when the domain is correct.

5. Click the **Save** button.

**To change who manages quarantined email:**

If you do not want specific users to manage their own quarantined email, or you do not want users to manage quarantined email for a distribution list (for example, sales@untangle.com) to which they subscribe, forward those users' or distribution list's quarantined email to a dedicated email account. That dedicated email account receives the Quarantine Digest for those users or distribution list.

1. From the Navigation pane, click the **Config** tab.

2. Click the **Quarantine** tab.

3. In the **Quarantinable Forwards** area, do the following:
   a. Create a table row for each user or distribution list.
   b. In the **distribution list address** column, specify one of the following:
      - The email address for the user that you do not want to manage quarantined email.
      - The email address for the distribution list.
   c. In the **send to address** column, specify the address that should manage the quarantined email. This **send to address** can be any dedicated email account. Consider creating one email account to manage all distribution lists' quarantined email, or assign a specific user's email address based on your company's workflow.

4. Click the **Save** button.
Resending Quarantine Daily Digests

If a user accidentally deletes the Quarantine Daily Digest, you can resend the Quarantine Daily Digest.

To resend digests:

1. From a browser, type in the Untangle Server’s External IP address followed by /quarantine. The Request Quarantine Digest Email window appears. For example:

   http://131.107.0.1/quarantine

2. Type in the email address of the user, then click Submit.

Disabling Quarantine Daily Digests

While Quarantine Daily Digests allow users to perform their own email maintenance, not all sites want digests to be sent to users.

To disable Quarantine Daily Digests:

1. From the Navigation pane, click the Config tab > Email. The Email Config window appears.

2. Click the Quarantine tab.

3. Uncheck the box sent to Send Daily Quarantine Digest Emails, then click Save.

Monitoring Quarantined Email

You can monitor email recipients quarantined email. To learn more about quarantined email, go to About Quarantine. You can also enable email recipients to monitor their own email as outlined in Specifying Who Manages Quarantined Email.

To browse the quarantine repository for unsolicited email:

1. From the Navigation pane, click the Config tab > Email. The Email Config window appears.

2. Click the Quarantine tab. In the User Quarantines area, the table lists quarantined email messages by email address (account address). This email address represents a user’s inbox.

3. In the table, select an email address, and click the Show detail button. The Email Quarantine Details window appears, and lists all the quarantined emails for the email address that you selected.

Next Step: To purge or release the emails, go to Releasing Wanted Email and Purging Unwanted Email.
**Releasing Wanted Email and Purging Unwanted Email**

You can manage email recipients quarantined email. To learn more about quarantined email, go to About Quarantine. You can also enable email recipients to monitor their own email as outlined in Specifying Who Manages Quarantined Email. However, you might need to maintain an end-user inbox if that user is on vacation.

**To release wanted email and purge unwanted email:**

*Before You Begin:* Locate the email that you want to release or purge. Go to Monitoring Quarantined Email.

1. (Important!) If this is an email that you want to release, then you must first add the *From Address* of your Outgoing Mail Server, the sender that releases email from quarantine, to your *Global* safelist. If you don't do so before you release the email, Spam Blocker will capture and quarantine the email again.

2. From the Navigation pane, click the **Config** tab > **Email**. The Email Config window appears.

3. Click the **Quarantine** tab.

4. In the **User Quarantines** area, select the email, then do one of the following:

   - Click **Purge Selected** button. The Purge selected button causes all emails within a given inbox to be deleted. This is the same as an end-user triggering a delete of all emails from the web application.

   - Click **Release Selected** button. The Release selected button causes all emails within a given inbox to be sent to the email address of the inbox. This is the same as an end-user triggering a release of all emails from the web application.
Local Directory
About User Access and User Authentication

The Untangle Server uses two types of user directories for two main purposes:

- **Local LDAP Directory:** A user directory stored on the Untangle Server. It can store the login, name, email, and password information on an unlimited number of users.

- **Active Directory (AD) Server:** A user directory that uses Microsoft's implementation of LDAP directory services for use in Windows environments.

These two directory types are used by the Untangle Server in the following ways. You might decide to use one method or, if you have an AD Server, you might use both methods. If your company hires temporary employees or contractors, and you do not want to update the AD Server with the temporary users, you can add the temporary employees to the Local LDAP Directory, and permanent employees to the Remote AD Server.

When a user attempts access with Remote Access Portal, the Untangle Server attempts authentication using the Active Directory Server, if specified:

- If the user does not exist, the Untangle Server attempts authentication using the Local LDAP Directory.

- If the user exists in the AD Server, but the password is incorrect, the User Directory will not attempt a lookup in the Local LDAP Directory.

- If no AD Server is specified, the Untangle Server uses the Local LDAP Directory.

For more information about Active Directory, go to Microsoft's Active Directory portal.

**Enabling LDAP Authentication**

**To add a user to the Local LDAP Directory:**

1. From the **Navigation Pane**, click the **Config** tab > **Local Directory**. The Local Directory Config window launches.

2. Click the green add (+) button to the left of the table.

3. In the new entry, provide the user's account information, then click the **Save** button.
## System Configuration

<table>
<thead>
<tr>
<th>Tab</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>• Enabling Remote Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>• Restarting Untangle Server</td>
</tr>
<tr>
<td></td>
<td>• Powering Off Untangle Server</td>
</tr>
<tr>
<td>Backup</td>
<td>• About Backups and Restores</td>
</tr>
<tr>
<td></td>
<td>• Backing Up Untangle Server's Configuration</td>
</tr>
<tr>
<td>Restore</td>
<td>• Restoring Untangle Server's Configuration</td>
</tr>
<tr>
<td>Protocol Settings</td>
<td>• Troubleshooting Email, Web, and FTP Traffic Problems</td>
</tr>
<tr>
<td>Regional Settings</td>
<td>• Changing Untangle Server's Timezone</td>
</tr>
<tr>
<td></td>
<td>• Specifying a Language Pack</td>
</tr>
<tr>
<td></td>
<td>• Uploading a Language Pack</td>
</tr>
</tbody>
</table>
Support
Enabling Remote Troubleshooting

There are two tools that Untangle Technical Support relies on to help you troubleshoot any system problems that you might encounter:

- Provide Untangle remote access to your Untangle Server.
- Enable data transmission related to problems with your Untangle Server.

To enable Untangle Technical Support remote access and data transmission:

1. From the Navigation pane, click **Config > System**.
2. Click the **Support** tab.
3. Select the **Allow** and **Send** radio buttons.

<table>
<thead>
<tr>
<th>Allow secure access to your server for support purposes</th>
<th>Provides Untangle Technical Support remote access to your Untangle Server. If you need Untangle Technical Support or their authorized representatives to troubleshoot problems with your Untangle Server, this may be required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send us data about your server</td>
<td>This allows your Untangle Server to send internal log messages to Untangle Technical Support in the event of unexpected conditions with your Untangle Server. This occurs through email, and no sensitive network information is transmitted.</td>
</tr>
</tbody>
</table>

4. Click the **Save** button.

Restarting Untangle Server

You can restart or reboot the Untangle Server without physical access to the system.

To reboot the Untangle Server:

1. From the **Navigation Pane**, click the **Config** tab > **System**.
2. On the "Support" tab, Under the **Manual Reboot** section, click the **Reboot** button.
Powering Off Untangle Server

Do not use the power button on the front of the Untangle Server or the emergency power switch on the back of the Untangle Server to power off the Untangle Server. These methods do not provide the Untangle Server a graceful shutdown. Instead, use the Untangle Server's direct-connect interface.

To power off the Untangle Server:

1. Connect a monitor, keyboard, and mouse to the Untangle Server. Your monitor displays the Untangle logo and Navigation bar.

2. In the Navigation bar, click the **Shutdown** button. The Untangle Server shuts down.

You can also shutdown Untangle without physical access to the system:

1. From the **Navigation Pane**, click the **Config** tab > **System**.

2. To Shutdown, click the **Shutdown** button under the **Manual Shutdown** section.
Backups and Restores

Untangle recommends that you back up your Untangle Server's configuration in case you need to restore it later. If you want Untangle to manage your backups, go to Configuration Backup.

While backup and restore should work between releases, it is advised to back up from and restore to the same release version. In other words, if you back up an Untangle Server 7.0.1 configuration and restore it to server running 7.3.1 it should work, but you should keep your network settings handy just in case.

Backing Up Untangle Server's Configuration

You can save a copy of your Untangle Server's configuration to:

- Untangle Server's hard drive.
- File on a local computer. This local computer must also be the same computer from which you intend to access the Untangle Server.

To back up your Untangle Server to a file:

1. Remote log in to your Untangle Server.
2. From the Navigation Pane, click the Config tab > System.
3. Click the Backup tab.
4. Click the Backup to File button.
5. Choose the file destination, and click Save. The backup file must have the .backup extension, but the actual file name any be any name. Choose file names that reflect the reason for the backup, such as BeforeOfficeMoveDowntown.backup or untangleserver_10_09_08.backup.

To backup your Untangle Server to the server hard drive:

1. From the Navigation Pane, click the Config tab > System.
2. Click the Backup tab.
3. Click the Backup to Hard Disk button. Untangle Server saves the data to a designated location, which Untangle Server remembers.

Restoring Untangle Server's Configuration
If you have an Untangle Gateway Lite, go to Restoring Untangle Gateway Lite Configuration.

You can restore your Untangle Server’s configuration from:

- Untangle Server's Hard Disk or USB key.
- File on a local computer. This local computer must also be the same computer from which you intend to access the Untangle Server.

To restore from Hard Disk:

*Before You Begin:* Ensure that you have the backup device (hard drive or USB key) that contains the backup configuration.

1. Using a keyboard, video and mouse, connect directly to the Untangle Server. When connected directly to the Untangle Server, a window with Untangle’s logo appears.
2. Click **Recover Utilities**. A confirmation window appears.
3. Click **Yes** to continue with the restore. The next screen offers a few options.
4. Select the **Backup & Restore** menu option. The Restore Method menu appears.
5. Select the **Local Hard Disk** menu option.
6. Insert the backup device, and click **OK**. The Restore Settings menu appears. If there is more than one backup on the device, the system prompts you to choose among the backups.
7. If prompted, from the Backup Image Selection Screen, select your backup.

*Caution:* The restore takes time. Do not power off the Untangle Server during the restore.

8. Click **OK**. The window displays many messages, and you can ignore them. When the restore completes, the Restore Successful window appears.

9. When the Restore Successful window appears, click **OK**. You can now exit all menus and return to the console desktop.

To restore from a local file that resides on your desktop:

1. Please make sure that your backup configuration file has the .backup file extension.
2. From the **Navigation Pane**, click the **Config** tab > **System**.
3. Click the **Restore** tab, then click the **Restore from File** button.
4. Choose the location of the .backup file.

Protocol Settings
Troubleshooting Email, Web, and FTP Traffic Problems

If you're having an email web or FTP traffic problem, and the cause isn't obvious, the first step is to rule out that the Untangle Server is NOT the cause.

Untangle Server's Software Products rely on HTTP, Mail, and FTP settings. By disabling these settings one at a time, you can troubleshoot your traffic problem.

To use protocol settings to troubleshoot:

1. From the Navigation pane, choose Config > System.
2. Click the Protocol Settings tab.
3. Disable one of the protocol settings:
   - HTTP. Web Override, Long URLs, Long Headers, Non-Http Blocking. Enable if you can't access a website.
   - FTP. Enable if you can't transfer files using FTP.
   - SMTP, POP3, or IMAP. SMTP, POP, IMAP, Timeouts. Enable if you can't send/receive email.
4. Click Save.
5. Perform the action that produced the problem initially. If you still observe the problem, the cause is probably NOT the Untangle Server.
Regional Settings

Regional settings help you customize your Untangle Server for your locale. You can set your timezone or specify a different language pack.

Changing Untangle Server’s Timezone

To change Untangle Server’s timezone:

1. From the Navigation pane, click Config tab > System.
2. Click the Regional Settings tab.
3. In the Timezone drop-down list, select the timezone in which the Untangle Server resides.
4. Click Save.

Specifying a Language Pack

During installation you chose a default language pack. You can choose a different language pack at any time. Language packs are available in two places, languages that are shipped with Untangle and language packs available for download from the Untangle site.

To change to a language pack shipped with Untangle:

1. From the Navigation pane, click Config tab > System.
2. Click the Regional Settings tab.
3. In the Language area, select a language from the drop-down list.
4. Click Save.