

Warp Product Family User Guide

USER GUIDE

Warp Product Family



© 2019 BADU Networks All rights reserved.

Software Version: we-4.3-c16

Disclosures

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR BADU REPRESENTATIVE FOR A COPY.

FCC disclosures for Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

FCC compliance for Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Badu could void the FCC approval and negate your authority to operate the product.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. BADU AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL BADU OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF BADU OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

WarpEngine, *WarpEngine-X*, *WarpGateway*, *WarpGateway-B*, *WarpAdmin*, *WarpManager*, and *WarpTCP* are registered trademarks of Badu Networks and/or its affiliates in the United States and certain other countries.

Badu and the Badu Logo are trademarks of Badu Networks, Inc. and/or its affiliates in the U.S. and other countries. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Badu and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Screenshots and images in this document may be slightly different than your screens. Depending on the version of the software you have installed, and the browsers (and shells) you use, your screen may not perfectly match what is presented in this document. However, every effort has been made to present accurate information in this document.

Table of Contents

Disclosures

Table of Contents

Introduction

System Requirements

Theory of Operation

Connecting to the Appliance

Status Page

Operating Modes

Filter Configuration

Interfaces Page

Performance Page

System Page

Diagnostics Page

Limited Shell Commands

Console Options

Known Issues

Contacting Badu Networks

Warranty Information

Introduction

Congratulations! You have just purchased the best solution on the market for optimizing jittery networks. Using Badu's *Warp* family of products, you can expect impressive optimization of network traffic performance for your platform's Internet connectivity. Following the installation and configuration of the appliance, you will enjoy the benefits of having greatly improved network speed for yourself and your customers. With this manual, you will become familiar with the process of setting up and performing ongoing management of Badu Networks' *Warp* products.

The appliance takes TCP streams arriving at the device, terminates them, and issues a transparent (if SNAT is disabled) stream to the destination. By applying stream termination, the appliance can take over the TCP congestion control on the outbound portion of the terminated stream as well as act as a better client for the server. The modifications are designed to drive more data and to provide increased throughput without changing the TCP protocol.

The system is designed to be highly available and recovers from unexpected errors or faults rapidly. If the system is configured in bypass mode, the system will allow traffic to flow without termination. Termination is on a per TCP session basis.

The following guide will help you through setup and configuration of the appliance.

System Requirements

The appliance comes as either a desktop unit (*WarpGateway*), or a 1U server with one or more physical NIC cards. This device requires a management connection (Gbit ethernet) as well as a network connection for each of the proxied interfaces. Typically during installation the operator would use a laptop or similar PC connected to the management eth0 interface.

The appliance shown below has 4 network ports in the back with the following functions.

eth0: Management port.

eth1: Reserved

eth2: Client side (downstream) interface

eth3: Server side (upstream) interface



Rear-View of a *WarpEngine* Appliance

By default, the system will start the *WarpAdmin* web service with an address of 10.10.10.10 on eth0. The sections that follow will walk you through accessing this web-based GUI and configuring the system.

Theory of Operation

Our proprietary congestion control algorithms can improve the throughput in networks where the throughput is limited by the protocol (such as TCP) and not by any physical or quality of service bandwidth constraint.

- All *Warp* products are configured between two physical or logical interfaces as pairs
- Network sessions are terminated and optimized unless there are specific bypass rules defined to cause them to be unoptimized
 - The outgoing connection utilizes Badu Networks' congestion control algorithms which expertly navigate congested networks
- All other traffic passing through the appliance is bypassed and not terminated, for example:
 - Multicast
 - UDP
 - Other protocols
- VLANs are supported with a logical proxy pair per VLAN
 - Traffic does not mix between VLAN interfaces

Some example network conditions that lead to significant TCP throughput improvements are:

- TCP traffic traveling through VPN tunnels
- Congested Wi-Fi networks
- Long distance connections

Connecting to the Appliance

After connecting a computer to the proxy on eth0/LAN1 with an IP address in the 10.10.10.x/24 subnet, navigate to the *Warp* Admin GUI at <https://10.10.10.10> on your web browser. This GUI will be used for configuring and managing the appliance. The first thing that will be displayed on the GUI is the login dialogue, which grants access to the management GUI. The management interface IP address and host name are included in the dialog box.

Note that the default MGMT address at 10.10.10.10 does not support any Layer 3 routing or VLANs. If connections are made in some other way, an alternate IP address should be configured on the MGMT section of the interface tab.

Default Credentials

Username: admin

Password: password

Note: It is highly recommended to change your password via the System Page after logging in with the default credentials



WarpTCP
JEFFTEST_6_VM
10.10.10.57

Username

Password

Sign in

Status Page

****NOTE** WarpAdmin only supports Chrome and Firefox browsers.**

To reach the Status page, you will need to successfully login. The Status page is segmented into two primary sections: Alarms and Performance Graphs.



Status Page

Alarms

- The system provides real-time notification alarms, which help aid users in monitoring and configuring the appliance.
 - Alarms can be viewed by using the scroll bar located on the right side of the section.
 - Alarms can be filtered by clicking on the filter icon at the top of each column.
- Filters**
 - Each column (except Messages) can be used to filter the alarms by clicking the desired filter icon.

Alarm #	Alarm Name	Severity	Type	Start	End	Message	ACK
<input type="checkbox"/>							

Action Dropdown

- By selecting alarms using the checkbox in the left column, you can apply the same action to multiple alarms. For example, you can acknowledge all selected alarms at once, instead of individually acknowledging them.
- You can also change the severity of selected alarms.

- **Severity**
 - There are 6 different severity levels:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
 - Warning (blue)
 - Information (white)
 - Cleared (green)
- **Date Range**
 - A date range can be entered by selecting the Start or End filters.

Filter ✕

Ascending ↑
Descending ↓

Range Start: 📅

Range End: 📅

Close
Apply

Date Range Window

Setting New Hostname:

You can set a new host name by clicking on the text in the center of the top bar (initially listed as "localhost.localdomain").

Setting a new host name will allow you to uniquely identify each machine on your network.

Note: This can be done from any page of the *WarpAdmin* interface.

Set New Hostname ✕

New Hostname:

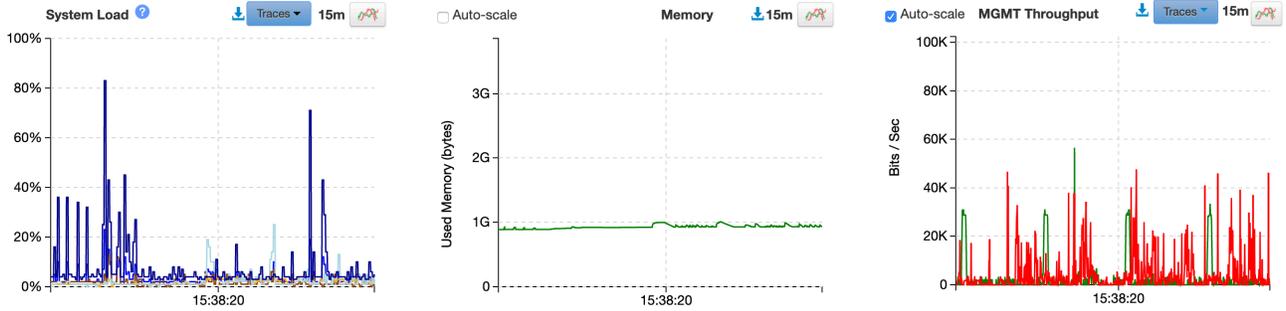
WARNING: Entering a new proxy hostname and clicking 'Set' WILL REBOOT the proxy immediately, after which the new hostname will be in effect.

Cancel
Set

1. Enter your new desired hostname (this is limited by standard DNS characters)
2. Press the Set button. Set

System Graphs

- These graphs include the CPU utilization & load average, memory utilization, and MGMT throughput.
- The data from the graphs is logged in a database for future review.
- Note that while the appliance is rebooted, there will be no data recorded.



Traffic Plots

Traffic that passes through the proxy can be logged and monitored real time. This feature is enabled in the Interfaces page and the resulting graphs are shown in the Status page.

Real time graphs can include:

- Total data through each physical interface
- Optimized traffic through each logical interface
- Number of sessions open per logical interface
- Number of sessions opened per second per logical interface
- Number of sessions closed per second per interface

Within each graph there are common functions:

- X axis time scale (slider)
- Select traces to graph
- Download current traces (download icon)
- Download historical data (clock icon). NOTE: Clicking the clock icon opens a separate tab where you can analyze historical data.



- On this page, use the bottom zoom area to highlight a specific range on the graph.
- Use the 'Re-sample' button to load more detailed data for the selection.
- Use the 'Previous' and 'Next' buttons to go to the previous selection.

Traces

- The Traces dropdown allows you to filter what results are displayed on the session rate graph.

- To enable a filter, select the checkbox next to that filter. Once the checkmark is selected, the associated information will be displayed on the graph.



Total Optimized Session Rate

- Downstream Open Sessions (LAN3)
- Downstream Closed Sessions (LAN3)
- Downstream Completed Sessions (LAN3)
- Upstream Open Sessions (LAN4)
- Upstream Closed Sessions (LAN4)
- Upstream Completed Sessions (LAN4)

Total Optimized Sessions

- Downstream Active Sessions (LAN3)
- Downstream Inactive Sessions (LAN3)
- Upstream Active Sessions (LAN4)
- Upstream Inactive Sessions (LAN4)

Total Throughput (LAN3 <-> LAN4)

- Downstream (LAN4 -> LAN3) Optimized
- Downstream (LAN4 -> LAN3) Unoptimized
- Upstream (LAN3 -> LAN4) Optimized
- Upstream (LAN3 -> LAN4) Unoptimized
- eth2 Rx - Total
- eth2 Tx - Total
- eth3 Rx - Total
- eth3 Tx - Total

Throughput Graph

The throughput graph shows both the total throughput through the Ethernet interfaces, as well as the portion which is proxied data. Note that any traffic that is not TCP such as UDP or other protocols would make up a significant portion of the difference. In addition the proxied data does not include the TCP headers per packet, while the ethernet interface data rate includes all bytes sent.

Performance Test Mode

This mode causes the system to optimize every other TCP flow, and bypass the other. As a result, interfaces with a large number of sessions can give a good indication of the average performance benefit.

The activation and de-activation of this mode is immediate and does not require a reboot. A popup and red text are present when switching into Performance Test Mode. Note that existing long-running sessions will finish with the mode they were started; enabling/disabling this mode does not affect them.

WARNING: Performance Test Mode will cause external test metrics (such as speed test websites) to report worse performance. This is expected because only half of the traffic will be optimized. Use with caution.

Performance Test Mode

Auto-scale **Throughput (Ip_0 - IPv4)** 50% Bypass

Auto-scale

- The Auto-scale tool will scale your graph's Y-axis according to the maximum height in the data. This tool is helpful when trying to analyze graph data, that might not reach or come close to the maximum of the Y-axis (1G, 10G).
- To enable Auto-scale, select the checkbox. Once the checkmark is displayed, the graph will be scaled.

Operating Modes

Operating Modes

This section describes the operating modes and provides detailed information for their configuration. Multiple logical pairs or proxies can be configured for each physical pair using VLANs. Each of the operating modes enables different features and requires different changes to the equipment in the surrounding network. The simplest to configure is **Transparent** mode (formerly Bridged Gateway), followed by **Bridge** mode, and finally **Gateway** mode. The following table gives the features and requirements for each mode. For all of these modes the appliance terminates the session and then establishes another session downstream. The data within the packet is buffered while waiting to be sent down stream, but it is not modified in any way. As a result, the appliance can support encrypted traffic such as HTTPS. This method of breaking the session allows the use of our proprietary congestion control algorithms while transmitting to the downstream device. If there is jitter in the downstream network that causes standard TCP algorithms to back off, our *Warp*TCP has the opportunity to do well. From the perspective of the client and server, there is no way to tell that the appliance is present other than comparing the packet sequence numbers at the client and server.

Item	Transparent	Bridge	Gateway
IP addresses required for Proxy	0	1	2
DHCP support	No	Yes	Yes
Routing changes on Gateways	No	No	Yes
Route traffic only on the appliance subnet	No	Yes	No
Inline management access	No	Yes	Yes
Source NAT	No	Yes	Yes
Filter Configuration Rules	Yes	Yes	Yes
SMB + IP Broadcast support (Windows® Share)	Yes	Yes	No
Forward Broadcast and Multi-cast traffic	Yes	Yes	No

Windows is a registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Base Pair

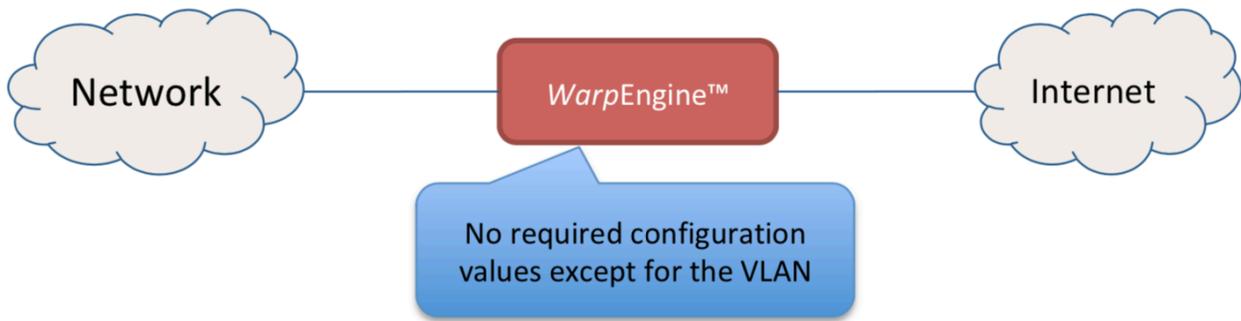
There is always one base pair present by default. To configure additional VLANs, you will need to click the "Add Logical Pair" button.

IPv4 & IPv6

Each pair includes a section for the physical layer, the IPv4 layer, and the IPv6 layer. The IPv4 and IPv6 layers can be enabled or disabled on a per logical pair basis. The configuration options are the same between IPv4 and IPv6, but some IPv6 options are currently disabled as they are not yet supported (including DHCP, MGMT, SNAT, SSH).

Transparent Mode

Transparent mode offers the simplest configuration, while limiting the features supported by the appliance. Examples where this configuration are particularly useful is in enterprise or carrier networks where the appliance is located between two routers or gateways and when IP Addresses are not available for the appliance.



Within *WarpAdmin*, the Transparent configuration is selected per logical pair. All fields in this mode are optional. The system will automatically determine what its neighboring gateways are, and configure itself accordingly. Click the "Add Logical Pair" button to add an additional logical pair for each VLAN on the network.

Name: Ip_2 (VLAN - 1)
Transparent ?

Downstream

Physical Layer

Interface: LAN3.1

MSS:

VLAN Name:

VLAN ID:

VLAN Priority:

Pair Name:

MTU:

Interface: LAN4.1

MSS:

VLAN Name:

VLAN ID:

VLAN Priority:

Optimize Unconfigured VLANs:

Upstream

+ MAC Filter Configuration
Active Filter Rules: 0

IPv4 Layer

Enabled

Idle Session Timeout (Mins):

User Notes

+ IPv4 Filter Configuration
Active Filter Rules: 0

+ IPv4 Redirect Configuration (Beta)
Active Redirect Rules: 0

IPv6 Layer

Enabled

Idle Session Timeout (Mins):

User Notes

+ IPv6 Filter Configuration
Active Filter Rules: 0

+ IPv6 Redirect Configuration (Beta)
Active Redirect Rules: 0

Optional Fields:

- **MSS:** The maximum TCP data payload size
- **VLAN Name:** A user defined name for this VLAN

- **VLAN ID:** The VLAN ID for this interface
- **VLAN Priority:** VLAN priority on this interface
- **Pair Name:** A user defined name for the proxy logical pair
- **MTU:** The desired MTU or Ethernet payload size. If left blank, the system will use the default value of 1500 bytes.
- **Optimize Unconfigured VLANs:** Check box to optimize VLAN traffic not specified in a logical pair
- **Idle Session Timeout (Mins):** How long to wait before timing out an idle TCP session

When the [Verify Configuration](#) button is pressed, the configuration of the proxy is validated. The question mark to the right of mode dropdown shows a list of the necessary conditions for a valid configuration.

Filter Configuration

See full details and examples in the section on [Filter Configuration](#)

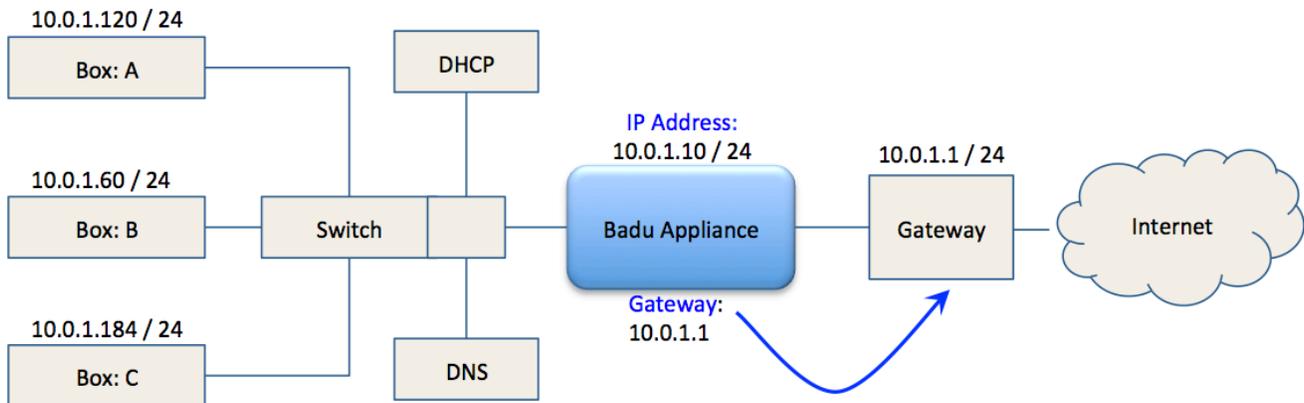
Redirect Configuration (Beta)

Used for routing all traffic to a particular IP address or set of IP addresses.

Bridge Mode

When using Bridge mode the system will route traffic between the two interfaces within a single subnet. An example network is shown below:

Example Bridge Network configuration



In order to route traffic, the proxy needs to have an [IP address](#) associated with the bridge, as well as a [gateway](#) that indicates where outbound traffic should be sent. The other fields in the blue section of the UI are optional configuration settings. The areas in grey, which are labeled "Upstream" and "Downstream" clients are used to help correctly configure the system. These should be filled out and then click the verify configuration button. This will check to see if the given configuration is successful.

Downstream	Upstream
Physical Layer	
Pair Name: <input type="text" value="ip_6"/>	Interface: br
MTU: <input type="text" value="1500"/>	MSS: <input type="text" value="MSS"/>
VLAN Name: <input type="text" value="ip_2_vlan_10_server"/>	MAC Address: <input type="text" value="00:00:00:00:00:00"/>
VLAN ID: <input type="text" value="10"/>	
VLAN Priority: <input type="text" value="0"/>	

+ MAC Filter Configuration Active Filter Rules: 0

IPv4 Layer	
Enabled <input checked="" type="checkbox"/>	
Source NAT: <input type="checkbox"/>	IP Address: <input type="text" value="CIDR Address"/>
SNAT Addresses: <input type="text" value="CIDR Address"/>	Gateway: <input type="text"/>
MGMT Port: <input type="text"/>	DHCP: <input type="checkbox"/>
Idle Session Timeout (Mins): <input type="text" value="120"/>	MGMT: <input type="checkbox"/>
	SSH: <input type="checkbox"/>
	SSH Port: <input type="text"/>

User Notes

+ IPv4 Filter Configuration Active Filter Rules: 0

+ IPv4 Redirect Configuration (Beta) Active Redirect Rules: 0

IPv6 Layer	
Enabled <input checked="" type="checkbox"/>	
Source NAT: <input type="checkbox"/>	IP Address: <input type="text" value="CIDR Address"/>
SNAT Addresses: <input type="text" value="CIDR Address"/>	Gateway: <input type="text"/>
MGMT Port: <input type="text"/>	DHCP: <input type="checkbox"/>
Idle Session Timeout (Mins): <input type="text" value="120"/>	MGMT: <input type="checkbox"/>
	SSH: <input type="checkbox"/>
	SSH Port: <input type="text"/>

User Notes

+ IPv6 Filter Configuration Active Filter Rules: 0

+ IPv6 Redirect Configuration (Beta) Active Redirect Rules: 0

Required Fields:

- **IP Address:** The IP address for the proxy (CIDR notation only)

Optional Fields:

- **Gateway:** The IP address that data is routed to if the IP address is not in the bridge's local subnet.
- **MSS:** The maximum TCP data payload size
- **MAC Address:** Define a custom MAC address to use for the bridge interface
- **DHCP:** Enables the proxy IP address to be provided by a DHCP server.
- **MGMT:** Enable management through this logical pair
- **SSH:** Enables SSH access to the limited shell on this interface
- **SSH Port:** If the SSH checkbox is selected, you must specify a port for SSH.
- **Pair Name:** A user defined name for the proxy logical pair
- **MTU:** The desired MTU or Ethernet payload size. If left blank, the system will use the default value of 1500 bytes.
- **VLAN Name:** A user defined name for this VLAN
- **VLAN ID:** The VLAN ID for this logical pair
- **VLAN Priority:** VLAN priority on this logical pair
- **Source NAT:** Enable source NAT on the proxy (**NOTE: This only applies to traffic originating on the downstream side**)
- **SNAT Addresses:** Specify multiple source addresses to use for source NAT-ing (separated by comma or return). Addresses must be specified in CIDR notation.
- **MGMT Port:** If Management is enabled on the logical pair, it is accessible on this port number. To access MGMT on this port, go to <https://logical pair IP address:MGMT port/login.html> in your browser
- **Idle Session Timeout (Mins):** How long to wait before timing out an idle TCP session

When the [Verify Configuration](#) button is pressed, the configuration of the proxy is validated. The question mark to the right of mode dropdown shows a list of the necessary conditions for a valid configuration.

Filter Configuration

See full details and examples in the section on [Filter Configuration](#)

Redirect Configuration (Beta)

This function allows the user to redirect traffic traveling through the appliance to another IP address or fully qualified domain name (FQDN). This can be used as a load balance function. If a domain name is used, you can specify a custom DNS TTL.

If more than one entry is added, the system will use a Round Robin algorithm to send traffic to each IP address.

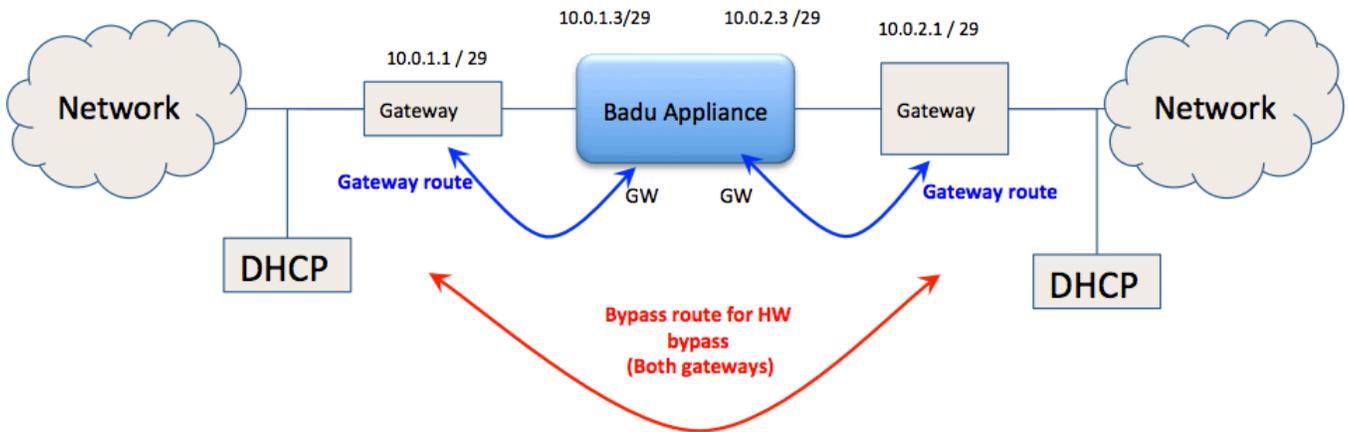
Gateway Mode

Gateway mode allows the most control over the networking environment. However, it also requires the most changes to the network surrounding the appliance. The requirements are as follows:

- Two IP addresses
- Routing changes on each of the Downstream and Upstream Gateways
- Bypass routing is required if the Proxy has a Bypass Network card.
 - Specifically when the bypass NIC turns into a wire, the routing between the gateways needs to be valid.

In the example network below, the appliance is placed between two gateways in a network. The Gateway and IP addresses are shown above the appliance. The routes that need to be added to the two gateways for network operation are shown in blue, while the rules that need to be added for HW bypass operation are indicated in red.

Example deployment in Gateway mode



Within *WarpAdmin*, the configuration is defined for each logical pair. The fields in Gateway mode are essentially a superset of all of the fields used by the different modes.

Downstream		Upstream	
Physical Layer			
Interface: eth2.5		Interface: eth3.5	
MTU: 1500	Pair Name: ip_1	MTU: 1500	
MSS: MSS		MSS: MSS	
MAC Address: 00:00:00:00:00:00		MAC Address: 00:00:00:00:00:00	
VLAN Name: ip_1_vlan_5_client		VLAN Name: ip_1_vlan_5_server	
VLAN ID: 5		VLAN ID: 5	
VLAN Priority: 0		VLAN Priority: 0	

+ MAC Filter Configuration Active Filter Rules: 0

IPv4 Layer		
Enabled		
IP Address: 172.16.2.10/24	Source NAT: <input type="checkbox"/>	IP Address: 172.16.3.10/24
Gateway: 172.16.2.1	SNAT Addresses: CIDR Address	Gateway: 172.16.3.1
DHCP: <input type="checkbox"/>	MGMT Port: <input type="text"/>	DHCP: <input type="checkbox"/>
MGMT: <input type="checkbox"/>	Idle Session Timeout (Mins): 120	MGMT: <input type="checkbox"/>
SSH: <input type="checkbox"/>		SSH: <input type="checkbox"/>
SSH Port: <input type="text"/>		SSH Port: <input type="text"/>

Traffic on VLAN 5

+ IPv4 Filter Configuration Active Filter Rules: 1

+ IPv4 Redirect Configuration (Beta) Active Redirect Rules: 0

+ IPv6 Filter Configuration	Active Filter Rules: 0
+ IPv6 Redirect Configuration (Beta)	Active Redirect Rules: 0

Required Fields:

- **Downstream IP Address:** The IP address for the eth2 interface (CIDR notation)
- **Upstream IP Address:** The IP address for the eth3 interface (CIDR notation)

Optional Fields:

- **Downstream Gateway:** The IP address that data is routed to for traffic coming from upstream (if destination is outside the local subnet).
- **Upstream Gateway:** The IP address that data is routed to for traffic coming from downstream (if destination is outside the local subnet).
- **MTU:** The desired MTU or Ethernet payload size. If left blank, the system will use the default value of 1500 bytes. **If this is mismatched on either side of the appliance, indeterminate results (including failure of traffic to flow through the appliance) may result.** When troubleshooting, carefully check MTU sizes on both sides of the appliance.
- **MSS:** The maximum TCP data payload size
- **MAC Address:** Define a custom MAC address to use for the interface
- **VLAN Name:** A user defined name for this VLAN
- **VLAN ID:** The VLAN ID for this logical pair
- **VLAN Priority:** VLAN priority on this logical pair
- **DHCP:** Enables the IP address to be provided by a DHCP server.
- **MGMT:** Enable management through this logical pair
- **SSH:** Enables SSH access to the limited shell on this interface
- **SSH Port:** If the SSH checkbox is selected, you must specify a port for SSH.
- **Pair Name:** A user defined name for the proxy logical pair
- **Source NAT:** Enable source NAT on the proxy (**NOTE: This only applies to traffic originating on the downstream side**)
- **SNAT Addresses:** Specify multiple source addresses to use for source NAT-ing (separated by comma or return). Addresses must be specified in CIDR notation.
- **MGMT Port:** If Management is enabled on the logical pair, it is accessible on this port number. To access MGMT on this port you need to set the browser to `https://logical pair IP address':MGMT port'/login.html`
- **Idle Session Timeout (Mins):** How long to wait before timing out an idle TCP session

When the [Verify Configuration](#) button is pressed, the entered configuration is validated. The question mark to the right of mode dropdown shows a list of the necessary conditions for a valid configuration.

Filter Configuration

See full details and examples in the section on [Filter Configuration](#)

Redirect Configuration (Beta)

This function allows the user to redirect traffic traveling through the proxy to another IP address or fully qualified domain name (FQDN). This can be used as a load balance function. If a domain name is used, you can specify a custom DNS TTL.

If more than one entry is added, the system will use a Round Robin algorithm to send traffic to each IP address.

If the "Enable Interface as Destination" box is checked, it will enable that interface to accept traffic and will then redirect that traffic to the specified server(s). This can be useful when Source NAT is enabled.

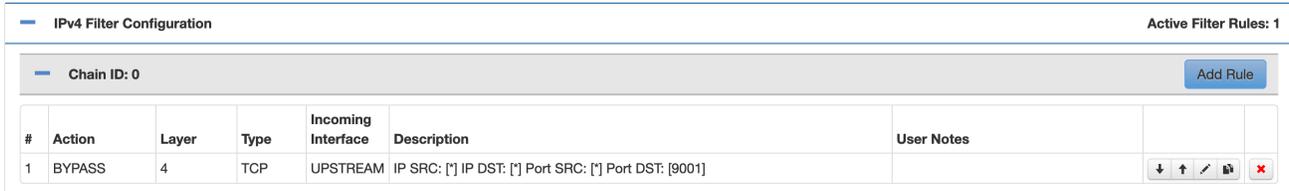
IPv4 Redirect Configuration (Beta) Active Redirect Rules: 0

Redirect IP Address or FQDN	DNS TTL (sec)	
<input checked="" type="checkbox"/> Enable Interface as Destination: <input type="text" value="Redirect IP Address or FQDN"/>	<input type="text"/>	<input type="button" value="Add"/>

Filter Configuration

Filter Configuration Rules

The Filter Configuration rules can be used to choose which flows should be optimized and which ones should be dropped or ignored. Separate filters can be added for each logical pair that is configured.



The screenshot shows the IPv4 Filter Configuration interface. At the top, it says "IPv4 Filter Configuration" and "Active Filter Rules: 1". Below that, there is a section for "Chain ID: 0" with an "Add Rule" button. The main part of the interface is a table with the following columns: #, Action, Layer, Type, Incoming Interface, Description, and User Notes. There is one rule listed with the following details:

#	Action	Layer	Type	Incoming Interface	Description	User Notes
1	BYPASS	4	TCP	UPSTREAM	IP SRC: [*] IP DST: [*] Port SRC: [*] Port DST: [9001]	

Within the filter configuration section, it is possible to add rules for layers 2, 3, & 4. You can also add certain specialty rules:

TCP Options: Only applies to Riverbed™ traffic.

GTP Filtering: If your license allows it, you will also have to option to create rules for filtering GTP Tunnels.

Prioritization/DSCP: Mark certain traffic with DSCP bits for prioritization. **This setting can affect throughput; use with caution!**

Bandwidth Hinting: Suggest a target bandwidth for the specified traffic. This option is only for use with specific applications that require it. It is not recommended to be configured to operate on all traffic through the Proxy, as it may limit overall performance. When used, its use should be narrowed in scope as much as possible to specific IP addresses, subnets, or VLANs.

Click **Add Rule** and choose your options for rule type and desired filter parameters. Port ranges can be specified using a hyphen or colon (e.g., **80-90** or **100:120**).

Within each rule, the conditions are logically ANDed so that the a packet must match all of the conditions to apply. Another way to say it: most fields are optional, so the more information you add, the more restrictive your rule becomes. **Since TCP has a return path for each session, the return path rule is automatically added, but not shown.**

Please use the **Incoming Interface** field to specify whether the rule should apply to sessions coming from upstream or downstream. The incoming interface may be on the client side of the appliance (i.e., "downstream") or the server side of the appliance (i.e., "upstream").

Filter Configuration



Layer 4 ▾

Insert Position 1 ▾

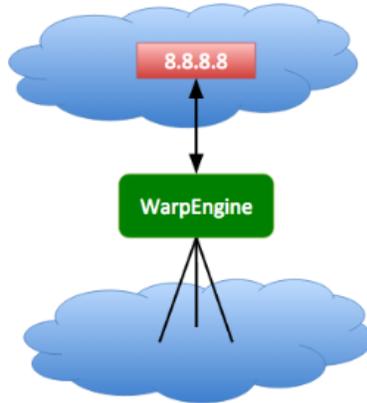
Incoming Interface	<input type="text" value="Upstream"/>
Type	<input type="text" value="Select Type"/>
Action	<input type="text" value="Select Action"/>
Source IP (CIDR)	<input type="text" value="*"/>
Destination IP (CIDR)	<input type="text" value="*"/>
Source Port	<input type="text" value="*"/>
Destination Port	<input type="text" value="*"/>
Notes	<input type="text"/>

Rule type can be selected using the drop-down menu in the top left corner. You will only be allowed to select a type that corresponds to the active logical pair section. The insert position near the top right allows you to specify where to insert your new rule. This is helpful if you have a large number of rules in place. Commonly matched rules should be placed near the top of your list.

Example Configurations:

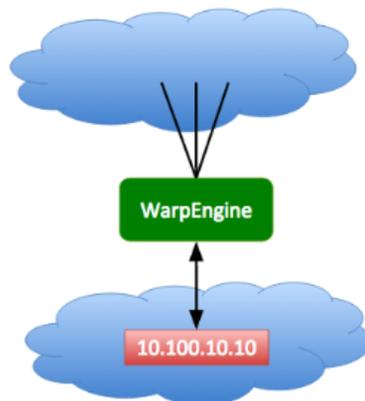
Bypass Source IP

- **Select: Layer 3**
 - Enter Source IP to bypass
 - 8.8.8.8/32
- **Result:** All packets in sessions initiated by 8.8.8.8 will pass through the appliance untouched.



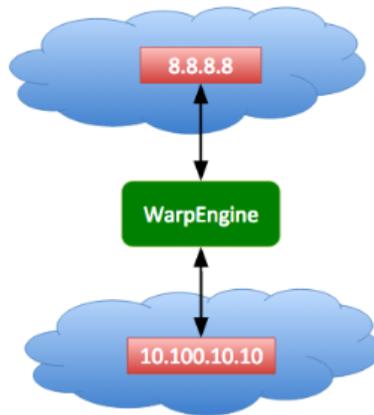
Bypass Destination IP

- **Select: Layer 3**
 - Enter Destination IP to bypass
 - 10.100.10.10/32
- **Result:** All packets in sessions destined for 10.100.10.10 will pass through the appliance untouched.



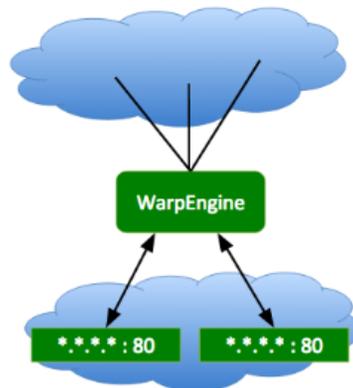
Bypass Source & Destination IP

- **Select: Layer 3**
 - Enter Source & Destination IP addresses
 - Source IP: 8.8.8.8/32
 - Destination IP: 10.100.10.10/32
- **Result:** All packets in sessions initiated by 8.8.8.8 going to and from 10.100.10.10 will pass through the appliance untouched.



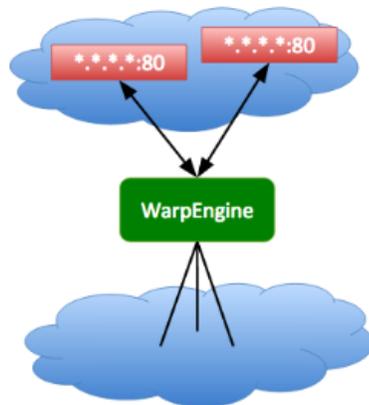
Bypass Source Port

- **Select: Layer 4**
 - Enter Source port to bypass
 - Port: 80
- **Result:** All packets in sessions originating from port 80 will pass through the appliance untouched



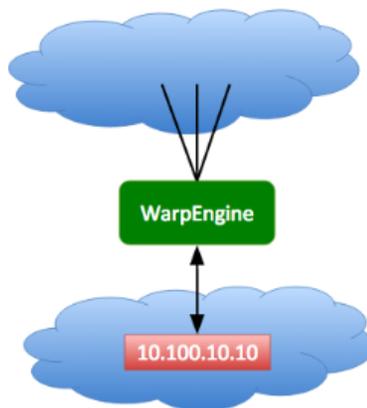
Bypass Destination Port

- **Select: Layer 4**
 - Enter Destination port to bypass
 - Port: 80
- **Result:** All packets in sessions going to port 80 will bypass the appliance and not be optimized



Bypass Both Destination & Source Ports

- **Select: Layer 4**
 - Enter both Source & Destination ports to bypass
 - Destination Port: 80
 - Source Port: 81
- **Result:** All packets in sessions originating from port 81 and going to port 80 will bypass the appliance, and not be optimized.



Interfaces Page

****NOTE** WarpAdmin only supports Chrome and Firefox browsers.**

The Interfaces Page is used for setting up the appliance to operate within your network configuration.

The Tabs at the top of the page include the Management tab, as well as each of the physical interface pairs.

At the far right there is a subnet calculator to help you calculate IP address ranges for different subnets.

All fields require the config to be SAVED before any changes will be applied. The one exception is enabling/disabling software bypass mode.

MGMT Tab

Under the from the top down there is a grey box indicating the physical properties of the interface, followed by the the system configuration, DNS servers, and associated management server information box.

Warp Management Interface

Physical Interface	
Name	eth0
Type	Twisted Pair, Intel Corporation 82540EM Gigabit Ethernet Controller
Link Status	
MAC Address	08:00:27:8d:9c:63
Speed (Mbps)	1000

Fixed Management Addresses ?

Type	Enable	DHCP	IP Address (CIDR)	Gateway	VLAN ID	VLAN Name	Physical Port	Delete
Local (IPv4)	<input type="checkbox"/>		10.10.10.10/24				eth0:M	
IPv4		<input type="checkbox"/>	<input type="text" value="10.10.10.57/24"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	eth0	<input type="button" value="X"/>
IPv6			<input type="text" value="CIDR Address"/>	<input type="text"/>				<input type="button" value="X"/>

Management On Proxied Interfaces

IP Address (CIDR)	Gateway	Port	VLAN ID	VLAN Name	Physical Port
-------------------	---------	------	---------	-----------	---------------

DNS Servers

User Notes

The information in the Management interface box represents the hardware information for this Ethernet port .

- **Fixed Management Addresses:** By default, the management interface has 10.10.10.10/24 available on eth0. If desired, this can be disabled by unchecking the "Enable" box. In addition, the user can add an additional IP address to work with the user's management network.
- **Inline Management Addresses:** It is possible to connect to the *WarpAdmin* through one of the proxied logical pairs on a specific port (in certain operating modes). The IP address and port are selected on the interface configuration tab and then displayed here after saving.
- **DNS Servers:** If you are using DHCP for your management interface, you may get a DNS server added automatically. You can add additional DNS servers by clicking the Add button. (Normal proxy operation does not require any DNS servers to be present. This is only for specific features such as redirecting to a URL.)
- **Verify Configuration:** In order to help with the configuration of the management interface this utility checks for common mistakes and connectivity, to verify that the configuration is set up correctly.
 - The window next to the verify configuration section displays warnings and errors from the verification check. In addition, the help button next to the Fixed Management Addresses displays all of the items that are necessary for a valid management configuration.
- **User Notes:** Optional user notes can be saved here.
- **Save:** Any changes made to the management interface page are not saved until this button is selected. Changes require a reboot.
- **Cancel:** Clear changes without saving.

NOTE: The management port (eth0) should **never** be plugged in to the same network as the proxy interfaces (eth2/eth3). If this happens, the network routing won't work, and you may see unpredictable network behavior.

There are three primary management scenarios:

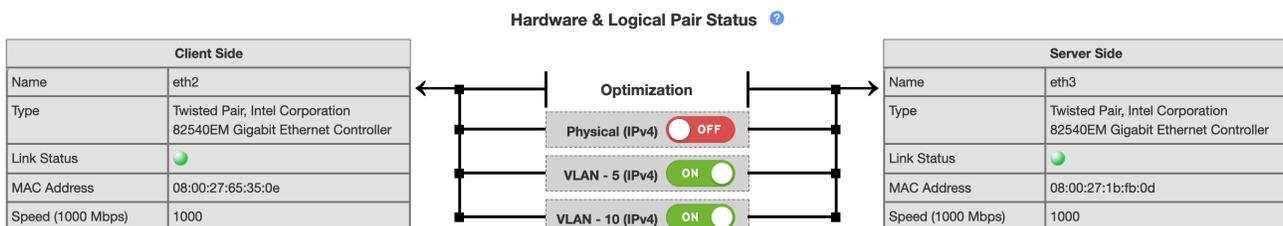
1. **No remote management is required.** Do not plug in the management (eth0) port, and do not check the MGMT box on the proxied interface.
2. **Remote management is required, but there is no dedicated management network.** Do not plug in the management (eth0) port, but **DO** check the MGMT box on the proxied interface. Access the GUI at the proxy interface IP with the specified port number (from the main network).
3. **Remote management is required, and there is a dedicated management network.** Plug in the management port (eth0) into the management network and select DHCP or enter a static IP for the fixed management. Do not check the MGMT box on the proxied interface. Access the GUI at the management interface IP (from the management network).

Proxied Pair Tab (eth2 <-> eth3)

In the middle of the screen, there is a pull-down menu that allows the user to select the global modes of operation for the proxy, including:

- **WarpTCP:** Normal proxying mode
- **Software Bypass:** All traffic is routed through the device, but TCP sessions are not terminated and no acceleration happens. This function works immediately; saving the configuration is not required.
 - **NOTE:** Enabling software bypass disables proxying of *new* sessions. Existing sessions will continue to be proxied. Likewise, sessions started while software bypass is enabled will be bypassed until session completion, even when software bypass is disabled.
- **Hardware Bypass** (if supported by the hardware): The two Ethernet or fiber cables in the pair are physically connected together by the NIC removing the proxy from the network.
 - When bypass NICs are installed, hardware bypass mode is enabled by default.
 - **NOTE:** If you are using an Inline Mgmt Address, switching into HW Bypass will cause you to lose access to *WarpAdmin*.

You can also enable software bypass by clicking the appropriate VLAN/pair toggle button in the middle of the screen. Green indicates Optimization mode, and red indicates Bypass mode.



For each physical pair of interfaces (eth4 <-> eth5, etc.) there is a tab for defining its operation. The tab is separated into two different sections, the first relating to the physical interface (as seen above) and the second relates to the configuration of logical

pairs. Each logical pair implements an independent proxy. The physical interfaces are referred to as upstream and downstream sides of the appliance. The upstream side is usually associated with the server, and is the external port when Source NAT is used.

Physical Port Fields

- **Name:** The name of the physical interface
- **Type:** The type of physical interface
- **Link Status:** Red for not connected, Green for link detected.
- **MAC Address:** MAC address for the physical interface
- **Speed:** The link speed that the interface has negotiated.

Watchdog Mode

In the event of a system failure, the watchdog will set the interfaces into the selected mode of operation.

- **Bypass:** Keep sending traffic as the Badu appliance becomes a wire (link stays up)
- **Disconnect:** Drop the interface links so other devices are aware and stop sending traffic
- **Disabled:** The watchdog is not enabled.

Power Loss Mode

Selects the mode of operation when the power to the box is lost: Bypass or Disconnect. Note that when the box is booting, or shutting down it will also go into this state.

LLCF

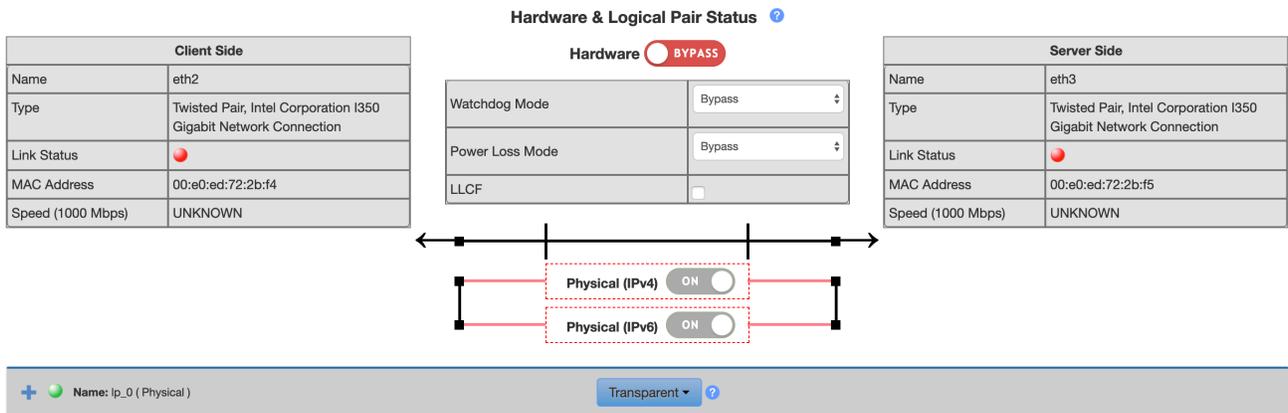
This enables the Link Loss Carry Forward feature. When enabled, if one of the network ports link fails it will drop the link on the other network port.

****NOTE**** Watchdog Mode, Power Loss Mode, and LLCF options will only be displayed if the hardware supports it. Any changes to these options require a reboot via the "Save" button at the bottom of the interfaces page.

Logical / Proxy Configuration:

In this part of the configuration, individual proxies are configured and added or deleted. **There will always be one base pair on the appliance. This pair cannot be deleted.**

Each logical pair can be individually Enabled/Disabled. To disable a logical pair means that all traffic on that pair will be dropped. The details of each mode are covered in the [Operating Modes](#) section of the user guide.



Key Functions:

- **Add Logical Pair:** Add an additional logical pair (up to 30 logical pairs can be added)
- **Apply:** Save and apply the current configuration
- **Cancel:** Cancel any changes made to the current configuration

Bonding Interfaces

If your *Warp* appliance has additional network interface pairs, you can configure them as standalone pairs. Each pair will cause a new tab to appear on the Interfaces page.

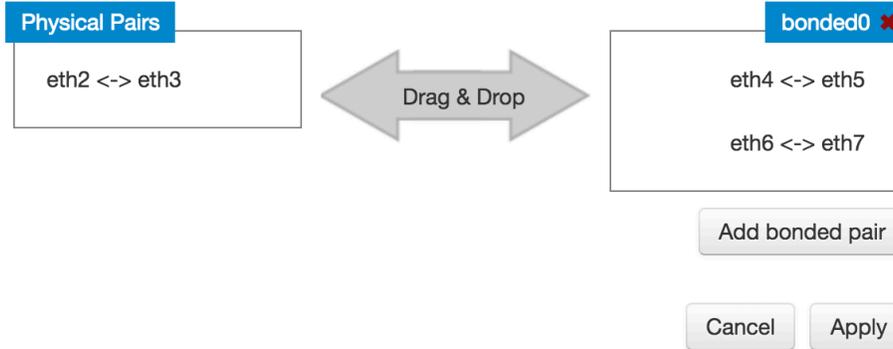


When multiple pairs are available, you will see a **Bonding** button appear next to the subnet calculator. When you click the Bonding button, a popup window will appear, allowing you to bond interfaces. Two physical pairs are required to create a bonded pair.

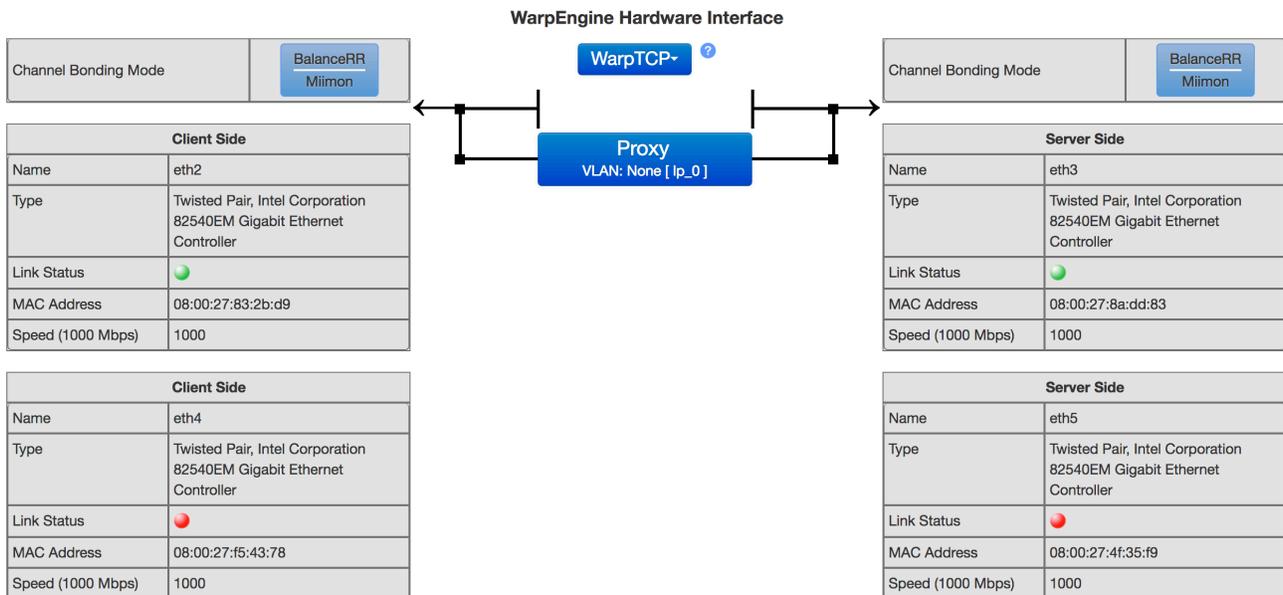
Bonding configuration



Note: Use drag and drop to bond the pairs



After applying your bonded pair selections, the tabs on your Interfaces page will be updated accordingly. You will also see additional bonding options displayed above the typical proxy configuration sections.



- **Channel Bonding Mode:** Shows the currently selected bonding mode and link monitoring option.

To change the selected bonding mode and link monitoring options, click the blue button in the Channel Bonding Mode box. You will see the following dialog window:

Configure Bonding Details



Bonding Policy:

Packets per Slave	<input type="text" value="1"/>
Resend IGMP	<input type="text" value="1"/>

Link Monitoring:

MII Link Monitoring Frequency

Down Delay ms.

Up Delay ms.

• Bonding Modes

• **Balanced Round Robin**

- **Packets per Slave (ms)**: Number of packets to transmit through a slave before moving to the next one. 0 is random. Default is 1. Range is 0 to 65535.
- **Resend IGMP**: Number of IGMP membership reports to be issued after a failover event. Default value is 1. Range is 0 - 255. Value of 0 means don't send.

• **Active Backup**

- **Active Slave**: New active slave. Either name or empty string. Name requires interface and link to be up in order to become active slave. If an empty string is specified, the current active slave is cleared, and a new active slave is selected automatically.
- **Primary Reselect**: Designed to prevent flip-flopping between the primary slave and other slaves. Values are below. Default is **Always**.
 - **Always**: The primary slave becomes active slave when ever it becomes available.
 - **Better**: Primary slave becomes active when it become available only if speed and duplex are better than the current slave.
 - **Failure**: Primary slave becomes the active slave only if the current active slave fails and the primary slave is up.
- **Arp All Targets**: Quantity of **Arp IP Targets** that must be reachable in order for the ARP monitor to consider a slave as being up. For value of **Any** it considers the slave up only when any of the **Arp IP Targets** is reachable. For value of **All** it considers the slave up only when all of the **Arp IP Targets** are reachable. Default is **Any**.
NOTE: The "Arp All Targets" option is not available when using Miimon Link Monitoring mode.
- **Fail Over MAC**: Whether active-backup mode should set all slaves to the same MAC address at enslavement (traditional behavior), or, when enabled, perform special handling of the bond's MAC address in accordance with the selected policy. Values are listed below. Default is **None**.
 - **None**: Disables **Fail Over MAC**, and causes bonding to set all slaves of an active-backup bond to the same MAC address at enslavement time.
 - **Active**: "Active" **Fail Over MAC** policy indicates that the MAC address of the bond should always be the MAC address of the currently active slave. MAC address of the bond changes during a failover. Requires gratuitous ARP and possibly an up delay if miimon is used.
 - **Follow**: "Follow" **Fail Over MAC** policy causes the MAC address of the bond to be selected normally (normally MAC address of the first slave added to the bond). Policy is useful for multiport devices that either become confused or incur a performance penalty when multiple ports are programmed with the same MAC address.
- **Number of Gratuitous ARPs**: Number of Gratuitous ARPs sent after a failover event. Range is 0 to 255. Default is 1.

- **Primary Device Slave:** String interface name specifying which slave is the primary device. Specified device will always be the active slave while it is available. No Default. Optional; not a required parameter.
- **Resend IGMP:** Number of IGMP membership reports to be issued after a failover event. Default value is 1. Range is 0 - 255. Zero means don't send.
- **802.3ad**
 - **System Priority:** Specifies the system priority. Range is 1 - 65535. Default is 65535.
 - **Mac-address for the actor:** Mac-address for the actor in protocol packet exchanges (LACPDU). Cannot be NULL or multicast. Default is master's MAC address.
 - **802.3ad aggregation:** 802.3ad aggregation selection logic to use. Options are Stable, Bandwidth, and Count. Default is Stable.
 - **Stable:** Active aggregator is chosen by largest aggregate bandwidth. Re-selection of the active aggregator occurs only when all slaves of the active aggregator are down or the active aggregator has no slaves.
 - **Bandwidth:** Active aggregator is chosen by largest aggregate bandwidth. Re-selection of the active aggregator occurs when a slave is added to or removed from the bond, any slave's link state changes, any slave's 802.3ad association state changes or when the bond's administrative state changes to up.
 - **Count:** Active aggregator is chosen by largest number of ports (slaves). Re-selection of the active aggregator occurs when a slave is added to or removed from the bond, any slave's link state changes, any slave's 802.3ad association state changes or when the bond's administrative state changes to up.
 - **Port-key:** Port-key has three parts – 00 Duplex, 01-05 Speed, 06-15 User-defined. Values are from 0 to 1023. Defaults is 0.
 - **LACPDU packets rate:** Rate in which link partner is asked to transmit LACPDU packets. Options are **Slow** in which LACPDU packets are sent every 30 seconds, or **Fast** in which LACPDU packets are sent every second. Default is **Slow**.
 - **Number of links active before asserting carrier:** Number of links that must be active before asserting carrier. Default is 0. 0 and 1 are the same.
 - **Hash policy:** Selects the transmit hash policy to use for slave selection. Default is **Layer 2**. Options are Layer 2, Layer 2+3, Layer 3+4, Encap 2+3, and Encap 3+4.
- **Active Load Balancing**
 - **Active Slave:** New active slave. Either a name or empty string. Name requires interface and link be up in order to become active slave. If an empty string is specified, the current active slave is cleared, and a new active slave is selected automatically.
 - **Primary Reselect:** Designed to prevent flip-flopping between the primary slave and other slaves. Values are below. Default is **Always**.
 - **Always:** The primary slave becomes active slave when ever it becomes available.
 - **Better:** Primary slave becomes active when it become available only if speed and duplex are better than the current slave.
 - **Failure:** Primary slave becomes the active slave only if the current active slave fails and the primary slave is up.
 - **Resend IGMP:** Number of IGMP membership reports to be issued after a failover event. Default value is 1. Range is 0 - 255. Zero means don't send.
 - **Learning packets interval:** Number of seconds between instances where the bonding driver sends learning packets to each slaves peer switch. Default value is 1. Range is 1-0x7ffffff.
 - **Primary device slave:** String interface name specifying which slave is the primary device. Specified device will always be the active slave while it is available. No Default. Optional; not a required parameter.
- **Link Monitoring**
 - **Miimon**
 - **MII link monitoring frequency:** MII link monitoring frequency in milliseconds. Determines how often link state of each slave is inspected for link failures. Value of zero disables MII link monitoring. Default is 0.
 - **Down delay (ms):** Time, in milliseconds, to wait before disabling a slave after a link failure has been detected. Option is only valid for the miimon link monitor. Default is 0.
 - **Up delay (ms):** Time, in milliseconds, to wait before enabling a slave after a link recovery has been detected. Option is only valid for the miimon link monitor. Default is 0.
 - **Arp Interval (not available in Transparent mode)**

Note: If multiple logical pairs are configured, ARP Interval monitoring will only be performed on the base pair.

 - **Arp Interval:** ARP link monitoring frequency in milliseconds. Regular traffic is generated via ARP probes issued for the addresses specified by the **Arp IP Target** option.
 - **Arp IP Target:** IP addresses to use as ARP monitoring peers when **Arp Interval** is > 0. These are the targets of the ARP request sent to determine the health of the link to the targets. Default is no addresses. Max is 16 and must be separated by a comma.
 - **Arp Validate:** Specifies whether or not ARP probes and replies should be validated in any mode that

supports arp monitoring, or whether non-ARP traffic should be filtered (disregarded) for link monitoring purposes. Values are listed below.

- **None:** No validation or filtering is performed.
- **Active:** Validation is performed only for the active slave.
- **Backup:** Validation is performed only for backup slaves.
- **All:** Validation is performed for all slaves.
- **Filter:** Filtering is applied to all slaves. No validation is performed.
- **FilterActive:** Filtering is applied to all slaves, validation is performed only for the active slave.
- **FilterBackup:** Filtering is applied to all slaves, validation is performed only for backup slaves.
- **Use Carrier:** miimon should use MII or ETHTOOL ioctls vs. netif_carrier_ok() to determine link status. Default is **1**. Value of 0 means use the deprecated mode.
- **All slaves active:** Duplicate frames (received on inactive ports) should be dropped (0) or delivered (1).

Once you have configured all of your bonding options, you can configure the logical pair as normal.

Performance Page

The Performance Page is designed to give greater insight into the traffic and performance of your network.

In order to determine what type of benefit the appliance is providing, a baseline is needed for comparison. When you capture performance data, you will be capturing both a baseline of unoptimized traffic and a sample of optimized traffic. The resulting data will then be shown in a series of graphs.

Time to capture (minutes): Total run time: 0h 0m 0s

Note: You have to allow at least 5+ minutes to capture performance data.

Capturing Performance Data

- With traffic running through the appliance, click the button "Capture Performance Data"
 - This will put your appliance into performance test mode, where sessions will be alternated between optimized and unoptimized.
 - You will not be allowed to toggle optimization on or off during this capture.
 - If you enable hardware bypass while the baseline capture is running, the capture will be stopped.
 - A timer will be displayed so you know how long the capture has been running.
- You can click "Stop Recording" to stop the capture at any time

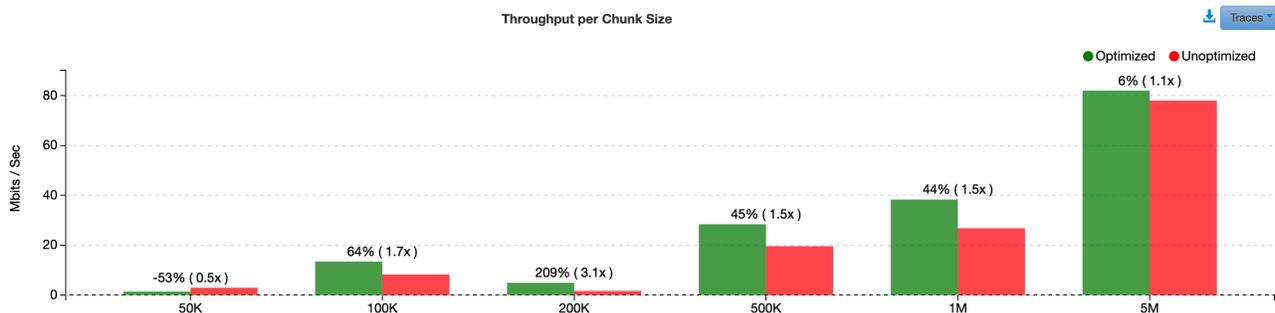
Discarding Data

- To delete the data you have captured, click the "Discard All Data" button.

Viewing the Benefit Data

Once you have a valid capture, you will be able to see information and statistics related to that data. There will be a graph that shows average throughput, broken out by data chunk sizes. To download a CSV file of the actual data behind the graph, click the download icon next to the Traces dropdown.

NOTE: The graph shows statistical estimates of performance benefits, based on sampling traffic. In order to get an accurate measurement, any bucket in the graph should have a minimum of 1,000 samples to ensure a statistically accurate benefit.



Scheduling Performance Data Captures

To schedule a performance data capture at a future date or on a recurring basis, you can use the scheduler underneath the graph. You can specify duration of the capture, along with time(s) of day and day(s) of the week. Your scheduled captures can be enabled or disabled as required. If a run is scheduled, the next scheduled run will be displayed as well.

Schedule: 12 a.m., 1 a.m., 2 a.m., 3 a.m., ... ▾ M, Tue, W, Th, ... ▾ **Duration:** 5 ▾ **DISABLED**

Next run scheduled for:

Current time: 2019/05/09 15:35:15 (America/Los_Angeles)

System Page

****NOTE** WarpAdmin only supports Chrome and Firefox browsers.**

The System Page is used for viewing system configuration, utilities, and software version.

System Information:

The System Information tab contains information about the appliance and the software that is installed on it.

Proxy Information Utilities Time and Date Database Advanced Options Administration SNMP Manager Alarm Modifications Accounts

Proxy Information:

Model:	WarpGateway	Licensed Features:	basic,vlan,2.5 Gbps,2
Serial Number:	10008	Expiration Date:	Sun May 02 2038 01:00:00 GMT-0700 (PDT)
Software:	4.2-b11 18515:1343	Proxy Uptime:	2 days 01:03:34
Admin:	18515:1343	Proxy Time:	05/17/2018 16:31:04 (GMT-7)
Kernel:	4.4.0-baduwartcp-180509.1258-fuzzybottom	Admin Time:	05/17/2018 16:31:04 (GMT-7)
BIOS Version:	BAR3NB04.1		

Hardware Information

The Hardware Information button will only be enabled for WarpEngine products. For WarpGateway products, the button is disabled.

Utilities

Under the systems page, the utilities tab supports different functions for managing firmware, configuration, and system control.

Utilities Tab

Proxy Information Utilities Time and Date Database Advanced Options Administration SNMP Manager Alarm Modifications Accounts

Firmware Partitions

Partition	Build Version	Active
Inactive: 4.2-b10.4	18510:1337	<input type="radio"/>
Active: 4.2-b11	18515:1343	<input checked="" type="radio"/>
Manufacturing: 4.2-b10.3.3	18430:1413	<input type="radio"/>

Select Partition ▾

Proxy Configuration

Import Export

System Control

Shutdown Reboot Factory Defaults

Utility Tab Inputs:

- **Firmware Partitions:** These are updated with a software update
 - **Partition:**
 - This is a list of all of the partitions on the box. There is an original read-only partition that will always be present. When the box is updated, 2 more partitions can be added. As a result, there will be a current partition, a previous partition, and the factory-installed partition. When an additional update is applied, the previous partition is replaced with the new partition, and the older partition is deleted. The factory installed partition is never removed.
 - In the event that the factory partition is selected, it behaves as if the box was updated to this partition. The factory partition is never actually active.
 - **Date:** The date each partition was installed.
 - **Active:** Green indicates the active partition. All others are grey.
 - **Select Partition button:** This selects which partition is currently active.
- **Proxy Configuration:** The configuration of the appliance can be exported or saved to a file for future use.
 - **Import:** Upload a configuration file to the appliance. This file would have come from a previous export from the pro
 - **Export:** Download the current proxy configuration. In the future it can be imported to recover the same state.
- **System Control:**
 - **Shutdown:** Turn off the appliance. This should be done prior to unplugging the box in order to prevent issues with the file system.
 - **Reboot:** Reboot the appliance
 - **Factory Defaults:** Clear the configuration and return to initial factory state. **Note that this includes clearing remote support keys; if you are currently using remote support, you will need to reconfigure your management interface and reapply your remote support bundle after the factory reset.**

Time and Date

This screen allows to set and manage the date and time on the proxy. Time can be set manually or via NTP. The time seen here is what will be used in any logged data.

Proxy Information Utilities **Time and Date** Database Advanced Options Administration SNMP Manager Alarm Modifications Accounts

NTP Server List

NTP Server	Delay/RTT (ms)	Offset (ms)	Reachable	Status	
<input type="text" value="IP Address"/>			<input type="radio"/>		<input type="button" value="Add"/>

Set date and time automatically with NTP:

Include WarpManager(s) as NTP server(s):

Current Proxy Time: 08/24/2018 23:24:15 (Universal)

Set New Time: Africa/Abidjan

- **NTP Server List:** Details about currently added NTP Servers. Note that multiple servers can be added by clicking the "Add NTP Server" button.
 - When the Reachable indicator is green, that means the time is synced.
- **Set date and time automatically with NTP:** Enable NTP time using the provided NTP servers.
- **Include WarpManager(s) as NTP server(s):** If your appliance is connected to a WarpManager, include the WarpManagers in the NTP server list.
- **Current Proxy Time:** Displays the current proxy time, with time zone.
- **Set New Time:** Manually set the time, date, and timezone on the Proxy.
- **Save:** Saves the configuration (requires reboot).
- **Cancel:** Discards changes without saving.

Data Storage

This section allows management of database storage limits and historical data.

File System Usage

Database: 454.14 MB / 1.88 GB

Age Limit Storage

Limits:

Alarm Age Limit (Days)	<input type="text" value="20"/>
Data Age Limit (Days)	<input type="text" value="20"/>

Note: Data age limit defines how many days at max the historic graph data will be kept in database. Min value is '1' day and max value is 10,000 days.

Historical Data Storage

Type	Recent Export	<input type="button" value="Delete all generated files"/>	Select Export	Cleanup DB
System Load				
Memory				
Sessions				
Throughput	WarpEngine--THROUGHPUT--15m--JEFFTEST_6_VM--2018-11-20--16-20-35.zip			
Alarms				
Traffic Capture				
SOS File				

- **File System Usage:**
 - **Database:** This is a bar indicating the amount of data used in the historical database vs the total available space in that partition. It only indicates storage that can be affected by the user. When the bar reaches 80% it turns yellow.
- **Age Limit Storage:**
 - **Limits:** User can specify the length of time (in days) that each item will be stored.
- **Historical Data Storage:** The most recently generated export file for each data type will remain available for future download. Clicking the red "X" button or the red button labeled "Delete all generated files" will remove these files.
 - **Trashcan:** This deletes all historical data of the corresponding type. A popup warns the user with OK / Cancel.
 - **Calendar:** This downloads the particular data type to a CSV file with headers for each column.
 - A popup allows the user to select a time or date range.
 - The popup also allows user to select data resolution; 15 minutes, 1 hour, or 24 hours.

Download: Data Range Selection - System Load



Start Date / Time:

End Date / Time:

08/24/2018 00:00



08/24/2018 23:59



Plot Data:

15 minutes 1 hour 24 hours

Data Resolution:

15 min plot - 1 second

1 hour plot - 5 seconds

24 hours plot - 90 seconds

Cancel

Download

Advanced Options

The options on this tab should not be modified unless directed by Badu support.

TCP Timestamp:	<input checked="" type="checkbox"/>
Timed Wait (sec):	<input type="text" value="10"/>

Save

Cancel

- [TCP Timestamp](#): Enable or disable TCP packet timestamps
- [Timed Wait \(sec\)](#): Specify the interval between closure and release of proxied sockets

Administration

This tab is used for accessing administrative functions for the appliance.

Proxy Information Utilities Time and Date Data Storage Advanced Options Administration SNMP Manager Alarm Modifications Accounts

Access Control:

Generate New SSH Key

Revoke SSH Key

SSH Port:

Current Key Expiration:

Software Control:

[Badu Networks Website](#)

License Request

Apply License

Upload Firmware Apply Firmware

Report Problems:

support@badunetworks.com

Generate SOS File

Activate Remote Support

Download System Logs

Firmware Update Procedure:

In order to update the latest firmware to the following:

1. Visit the Badu Networks licensing and update website: <http://license.badunetworks.com/>
2. Log in with your user name and password.
3. Download the latest software for your product
4. Choose
5. On the popup window, select your firmware update file and click either the Upload or Upload and Apply button

Upload Firmware Update



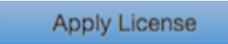
- a. If you choose "Upload" the file will be uploaded only. You will have to click the "Apply Firmware" button separately to actually apply the update. This option allows continuation of partial or interrupted uploads (useful on slow or unreliable connections). This is also useful to preposition the firmware, to make sure it is ready prior to a scheduled upgrade window.
- b. If you choose "Upload and Apply" the file will be uploaded and applied immediately.

Licensing Procedure:

In order to operate with high performance the *WarpAdmin* must be licensed with a valid license. Normally the License for a particular software update for the appliance is included in the zip file with the update. In this case when you update the software, the license will automatically be updated as well. However, in the event that you have received a custom patch from Badu Networks, you can still license the appliance using the method below.

Licensing Steps:

1. Download License request

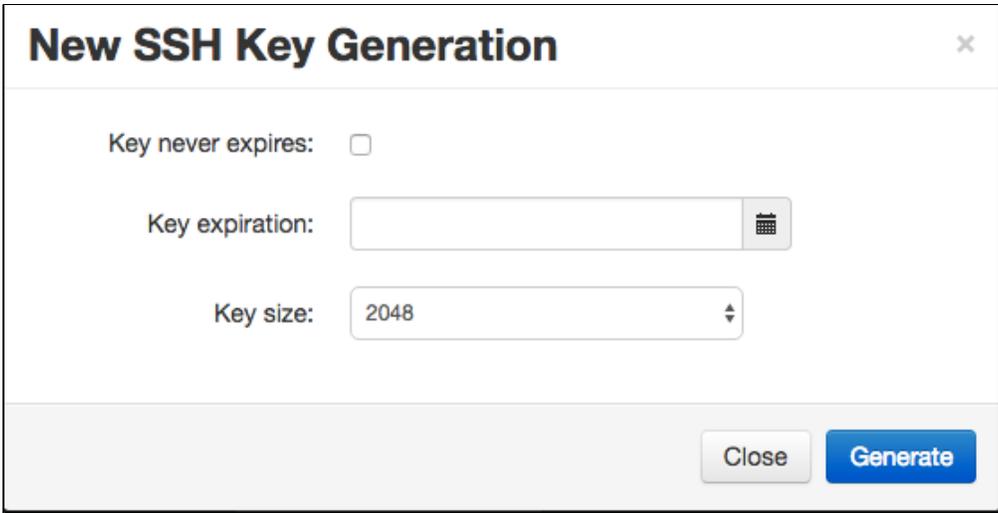
2. Log onto the Badu Networks Licensing and update website: <https://license.badunetworks.com/>
3. Choose request license tab -> Upload request
4. Upon success, download the license
5. Upload the license to the admin using 
6. Upon successful licensing a popup will indicate success. A short time later the license indicator will indicate that it was successful.

NOTE: When your license expires, traffic will be unoptimized for 30 days. If your appliance is still unlicensed after 30 days, it will begin slowing down traffic until a new license is applied.

Generate New SSH Key:



Creating a ssh key will allow the user to ssh into the machine and run a limited set of commands, which can assist in debugging network issues. The ssh key can be set to expire after a programmed period of time. SSH access is only provided through using a key and not a password. The ports that support ssh access are defined in the GUI.



The dialog box titled "New SSH Key Generation" contains the following elements:

- A checkbox labeled "Key never expires:" with an unchecked box.
- A text input field labeled "Key expiration:" with a calendar icon to its right.
- A dropdown menu labeled "Key size:" with "2048" selected.
- At the bottom right, there are two buttons: "Close" and "Generate".

1. Decide whether or not you would like the ssh key to expire at some time. If not then skip step 2 and select "Key never expires" checkbox. If so, proceed step 2.
2. Select the date that you would like the ssh key to expire. Use the calendar icon to select the desired expiration date.



3. Select the key size that you would like to associate with the ssh key.
 - a. The larger the key size is, the longer it takes to generate, but the more secure it will be.
4. Press the Generate button 
5. The Download SSH Key pop up will be displayed. Press the Download button to download the key.
 - a. The key will begin to download to your computer.



You can see all of the allowed commands in the [Limited Shell Commands](#) section.

Custom SSH Port

This field can be used to specify a custom SSH port.

SSH port: 

Current Key Expiration

This field can be used to reference the expiration date of your current ssh key.

Also you can download this ssh key at any time by pressing the key icon.



Current Key Expiration:

04:05:39 PM 05/21/16 (GMT-7)



Generate SOS File

Generate SOS File

In the event that something bad happens with the appliance software, a debug file can be created that gives information on the status of the box.

Select "Generate SOS File" to generate the SOS file and then e-mail it to support@badunetworks.com

Remote Support

The remote support function allows Badu Networks technicians to help solve issues by logging on remotely. In order to enable this support, please do the following:

- Configure the appliance with a default gateway so that it can reach the internet.
- Obtain a remote support key from Badu Networks, and upload the support key in the support key dialog as shown below.
 - The key will only be active for a limited time.
- Press the Activate button to activate the connection.
 - When the remote connection has been established the indicator next to the activate button will turn green.
- Once activated, the "Activate" button will change to say "Deactivate". Click the "Deactivate" button to disconnect the established session.
 - The indicator will turn yellow when a support key has been deactivated.

Log messages will be displayed in the remote support dialog shown below.

Remote Support

Support key 

Expires:

This requires the MGMT port to be to a network that can access the internet.

In order for the device to obtain remote support, it must have access to the internet through the management interface. This includes defining a default gateway for the management network. This remote support connection establishes a VPN connection between the appliance and the Badu Networks server.

SNMP

This option allows the user to configure the available SNMP options on the appliance. The screenshot below shows the different configuration sections available.

SNMP Notification Configuration Add

—
✕

Configuration Name

SNMP Version

Destination IP Address

Destination Port

Security Level

Security Name

Authentication Engine Id

Auth Password

Privacy Password

Authentication protocol

Privacy Protocol

Save
Cancel

Agent Users/Communities Add

+
BaduNetworks
✕

SNMP Agent Configuration Disable

Allowed IP Subnets for V2c (CIDR Notation) or * for All

Agent Listening IP Address

Agent Listening Port (UDP)

SNMP Notification Testing

Alarm Code

Notes

Identify Test Alarms as Test in Alarm Description

Test

SNMP Agent MIB-II Configuration ✎

SNMP sysName

SNMP sysContact

SNMP sysLocation

- **SNMP Notification Configuration**

- **Add:** Add a configuration for another outgoing connection
 - **Configuration Name:** The name of this particular configuration
 - **SNMP Version:** Version of the SNMP software (defaults to v3).
 - **Destination IP Address:** The IP address of the manager
 - **Destination Port:** The port that the manager uses for SNMP (defaults to 162)
 - **Security Level:** authPriv, noAuthPriv, noAuthNoPriv
 - **Security Name:** The login user name for the manager
 - **Authentication Engine ID:** A 2 – 32 char hex string which acts similar to an SNMP user name
 - **Auth Password:** The manager auth password
 - **Privacy Password:** The manager privacy password
 - **Authentication Protocol:** SHA or MD5

- **Privacy Protocol:** DES, AES128
- **Community Name (v2c only):** The community string that provides access to SNMP information
- **Testing:** This is used to artificially generate SNMP notifications. When a Proxy creates an alarm, it is sent as a notification to the manager. This alarm can then be re-issued to the NMS.
 - **Alarm Code:** Enter an arbitrary alarm code
 - **Notes:** Enter your alarm notes
 - **Identify Test Alarms as "Test" in Alarm Description:** Append the text "test" to identify this alarm as a test.
- **SNMP Agent Users/Communities**
 - **Add:** Add a configuration for authentication of incoming SNMP requests
 - **SNMP Version:** Version of the SNMP software (defaults to v3)
 - **Security Name:** The login user name for the NMS
 - **Security Level:** authPriv, noAuthPriv, noAuthNoPriv
 - **Auth Password:** The NMS auth password
 - **Privacy Password:** The NMS privacy password
 - **Authentication Protocol:** SHA or MD5
 - **Privacy Protocol:** DES, AES128
- **SNMP Agent Configuration**
 - **Edit:** Customize the parameters for accepting incoming requests
 - Allowed IP Subnet for V2c (CIDR Notation) or * for All
 - Agent Listening Port (UDP)
 - **Disable/Enable:** Button toggles listening state for incoming SNMP requests
- **SNMP Agent MIB-II Configuration**
 - **SNMP sysName:** Name to present for the system
 - **SNMP sysContact:** Contact person to present for the system
 - **SNMP sysLocation:** Location to present for the system

SNMP GET/Get-Next Object Support

The following public SNMP MIBs are supported for GET/Get-Next **READ-ONLY Access** using **SNMP v3 and v2c**

SNMPv2-MIB
 HOST-RESOURCES-MIB
 UCD-SNMP-MIB
 LM-SENSORS-MIB

Additionally, there are two private MIBs available that are specific to the Proxy. These can be downloaded from the license.badunetworks.com website.

BADUNETWORKS-SMI.MIB
 BADU-WARPTCP-NOTIFICATION.MIB

Here is a command line example that shows the LM Sensor information for a *Warp* product:

```

$ snmpwalk -v 3 -u BaduNetworks -l authPriv -A WelcomeBadu -a SHA -X
WelcomeBadu -x AES -m ~/Downloads/LM-SENSORS-MIB.MIB 10.254.20.186
.1.3.6.1.4.1.2021.13.16.2.1
LM-SENSORS-MIB::lmTempSensorsIndex.1 = INTEGER: 1
LM-SENSORS-MIB::lmTempSensorsIndex.2 = INTEGER: 2
LM-SENSORS-MIB::lmTempSensorsIndex.3 = INTEGER: 3
LM-SENSORS-MIB::lmTempSensorsIndex.4 = INTEGER: 4
LM-SENSORS-MIB::lmTempSensorsIndex.5 = INTEGER: 5
LM-SENSORS-MIB::lmTempSensorsIndex.6 = INTEGER: 6
LM-SENSORS-MIB::lmTempSensorsIndex.7 = INTEGER: 7
LM-SENSORS-MIB::lmTempSensorsIndex.8 = INTEGER: 8
LM-SENSORS-MIB::lmTempSensorsDevice.1 = STRING: Physical id 0
LM-SENSORS-MIB::lmTempSensorsDevice.2 = STRING: Core 0
LM-SENSORS-MIB::lmTempSensorsDevice.3 = STRING: Core 1
LM-SENSORS-MIB::lmTempSensorsDevice.4 = STRING: Core 2
LM-SENSORS-MIB::lmTempSensorsDevice.5 = STRING: Core 3
LM-SENSORS-MIB::lmTempSensorsDevice.6 = STRING: Core 4
LM-SENSORS-MIB::lmTempSensorsDevice.7 = STRING: Core 5
LM-SENSORS-MIB::lmTempSensorsDevice.8 = STRING: loc1
LM-SENSORS-MIB::lmTempSensorsValue.1 = Gauge32: 52000
LM-SENSORS-MIB::lmTempSensorsValue.2 = Gauge32: 49000
LM-SENSORS-MIB::lmTempSensorsValue.3 = Gauge32: 52000
LM-SENSORS-MIB::lmTempSensorsValue.4 = Gauge32: 48000
LM-SENSORS-MIB::lmTempSensorsValue.5 = Gauge32: 50000
LM-SENSORS-MIB::lmTempSensorsValue.6 = Gauge32: 49000
LM-SENSORS-MIB::lmTempSensorsValue.7 = Gauge32: 45000
LM-SENSORS-MIB::lmTempSensorsValue.8 = Gauge32: 74000

```

Manager

Manage connections for a *WarpManager*.

Proxy Information Utilities Time and Date Data Storage Advanced Options Administration SNMP **Manager** Alarm Modifications Accounts

Manager IP Address	Connect	Status	Remove
<input type="text" value="10.10.10.7777"/>	<input type="button" value="Connect"/>	<input checked="" type="radio"/>	<input type="button" value="🗑"/>
Connect to Manager through:		<input type="text" value="MGMT eth0 10.10.10.57"/>	

```

[2018/11/20 15:39:30] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/11/20 15:35:46] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/11/14 14:50:38] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/11/14 14:41:24] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/11/14 14:38:18] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/10/31 11:39:11] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening
[2018/10/31 11:27:31] Proxy Job ID: 6ce48a60-d978-11e8-a2a4-d762a3fe78c8 Type: 'AlarmModificationRule_Del', Event: E0_Recover, State: Listening

```

After entering an IP address, press the corresponding Connect button to attempt connection to the Manager. Once connected, the indicator light will turn green. Click the Disconnect button to disconnect from the Manager. Press the trash can icon to clear the Manager IP address. Relevant log messages will appear in the grey box.

Note: For the MGMT Interface dropdown, eth0 will be the only option unless both of the following conditions are met -- 1) you are

running Bridge or Gateway mode, and 2) you have selected the MGMT checkbox on a proxied interface.

Alarm Modifications

- Alarm modifications modify the alarm generation on the system. The modifications can be initiated on the appliance or on the *WarpManager*.
 - The values are stored on the appliance and cached on the *WarpManager* display
 - In the event that they are created on the appliance, the Alarm modification is sent to the manager over the secure communications interface.
 - When the appliance first connects to the Manager, it sends all of its Alarm modifications to the Manager.
 - When an appliance is disconnected from the Manager, the Manager flushes all modifications associated with the appliance.
 - When rules are being sent to or from the appliance, a queue is kept that survives reboot. The action is removed from the queue when it is acknowledged as complete.

Type	Severity	Alarm Name	Active Time	Delay (hh:mm:ss)	Execute Action
Select Type ▾	Select Severity ▾	Select Alarm Name ▾	From: Not defined Till: Not defined	Multiple events buffering delay: Not defined	☑ Select Action ▾

Type	Alarm Name	Action	User	Source	Date Added	Active Time	Delay (hh:mm:ss)	
<input type="checkbox"/>	License	bnwTcpWeDetectedKeyLOKRemoval	Drop	admin	WarpManager+9001	1969/12/31 16:00:00	Not defined : Not defined	Not defined

- Alarm Modification:**
 - Add:** Add a new set of rules defined by what the user entered. Does nothing if the user didn't enter anything.
 - Clear:** Clear the entered values. Does nothing if user hadn't entered anything.
 - Type:** This allows the user to select one or more Alarm types with a pull-down
 - Severity:** Select the severity of the alarms to select
 - Alarm Name:** A pull-down of the alarms that meet the other filter conditions.
 - Active Time:** Time for this alarm modification to be enforced.
 - Delay (ms):** Delay reporting of multiple repeated alarms so that they can be grouped into a single alarm
 - Execute Action:** This is the modification that will be made to all of the alarms that match the filter.
- Active Alarm Modifications:**
 - The table lists all of the alarms which are currently active.
 - Each row corresponds to a single rule / modification
 - Each Column can be filtered and sorted. Sort applies to one column, but the filters are all logically ANDed.
 - Type:** the type of alarm
 - Filter: pull down multiple selection, sort (ascending / descending)
 - Alarm Name:** Name of the active alarm
 - Filter: List selection of alarm names
 - Action:** the action that will be carried out on the alarm
 - Filter: pull down for the different actions, sort ascending / descending.
 - User:** the user associated with the alarm modification
 - Source:** the source of the alarm modification (proxy vs manager)
 - Date Added:** the date of the alarm modification
 - Active Time:** the range of time the modification is active
 - Delay:** Buffer delay for repeated matching alarms

Accounts

Create and manage user accounts and their permissions.

NOTE: One of the first things that should be done when deploying the appliance is to change the administrator's password. The default password is "password"

Current User

User Name	admin
Name	admin
Phone	n/a

Change Password

User Preferences:

UI Login Timeout (mins)	30
Language:	English
Time Display:	Browser

User Permissions	Actions	New User	Clear Filters	Page Size: 100	1	
Select	User Name	Name	Phone	Role	User Permissions	
					Write	Read
<input type="checkbox"/>	admin	admin		Admin	✓	✓

- **Current User:** Displays information about the current user
 - **Change Password:** Allows user to change their password
- **User Preferences:** Change basic preferences for current user.
 - **UI Login Timeout (mins):** How long before the *WarpAdmin* interface logs out due to inactivity
 - **Language:** Which language to display *WarpAdmin* text? (English, Korean, Chinese)
 - **Time Display:** Which time to display to user? (Browser, UTC, System Time)
- **User Permissions:** This table displays all users and their information
 - **Select:** Checkboxes allow editing multiple users at once
 - **New User:** Create a new user
 - **Actions:** Perform actions on selected users
 - **Delete User:** Delete selected users
 - **Change Username:** Change username for selected users
 - **Change Name:** Change name for selected users
 - **Change Phone:** Change phone number for selected users
 - **Reset Password:** Reset password for selected users
 - **Change Role:** Change role for selected users (Admin, Member)

Diagnostics Page

****NOTE** WarpAdmin only supports Chrome and Firefox browsers.**

Diagnostic and troubleshooting data can be collected by capturing data passing through the appliance. Additional network diagnostic tools are available.

Network Diagnostics

Tools

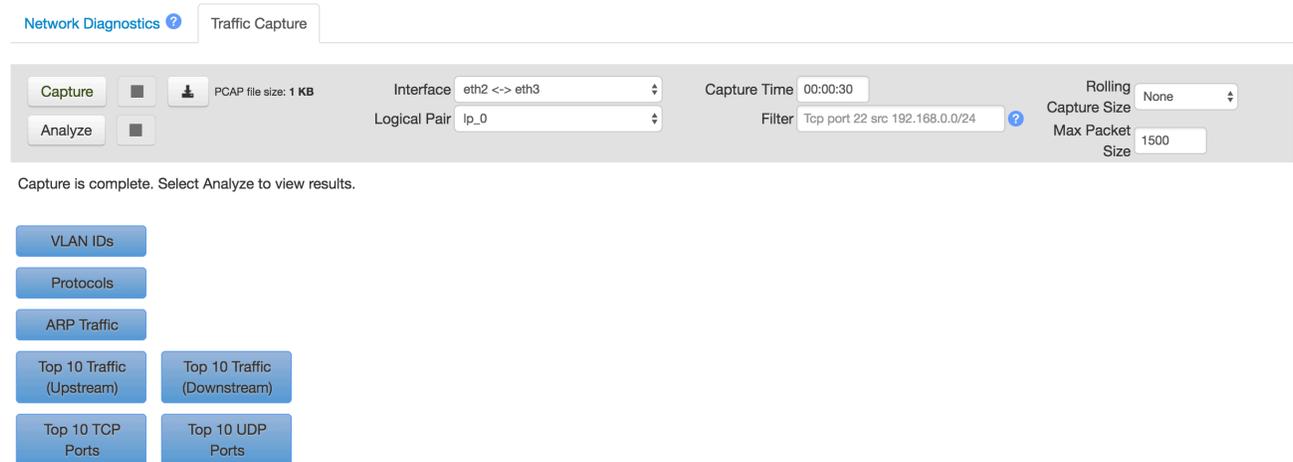
- **Ping:** Ping the provided IP address on the specified interface. This is useful to verify that other machines are up and reachable on the network. Supports both IPv4 and IPv6. *Note: Ping tool is not available for interfaces configured in Transparent mode*
- **ARP Probe:** ARP the provided IP address on the specified interface, and return the MAC address for selected IP address. This is particularly useful when configuring MAC spoofing for bridge gateway mode.
- **NSLookup:** Look up IP address for a given hostname (only works if DNS is properly configured on the Management Interface)
- **Show ARP Cache:** Show the current contents of the appliance ARP cache
- **Clear ARP Cache:** Clear the appliance ARP cache
- **Verify Interfaces:** Verify that the configured gateways exist on the network

The screenshot shows the 'Network Diagnostics' section with a sub-tab for 'Traffic Capture'. On the left, there are several tool buttons: 'Ping', 'ARP Probe', 'NSLookup', 'Show ARP Cache', 'Clear ARP Cache', and 'Verify Interfaces'. Each tool has associated input fields: 'Ping' and 'ARP Probe' require an 'IP Address' and an interface (currently 'eth0'); 'NSLookup' requires a 'Hostname'. On the right, there is a large 'Results' box which is currently empty. At the bottom right of the results box, there are two icons: a download icon and a trash can icon.

The download icon can be used to dump the output to a text file. The trash can icon will clear any text from the Results box.

Traffic Capture

The traffic analysis function allows the user to take a packet capture on both of the physical ports and do a basic analysis of the results. This can be particularly useful for debugging configuration issues. Note that the Analysis of large capture files can be quite CPU intensive, and may disrupt the collection and display of graph data.



Inputs:

- **Capture:** Start the packet capture. The user can browse away or even log off the proxy during the capture
- **Stop:** Stop the packet capture (active when the capture is in progress). The capture will be analyzed and displayed after the capture is complete.
- **Download:** Download the raw capture files in Zip format. The captured files persist on the Proxy until another packet capture is run, or the box is rebooted.
- **Interface:** The physical interface pair on which the capture will be taken.
- **Capture time (HH:MM:SS):** The amount of time that the packet capture will run.
- **Rolling Capture Size:** Rolling Capture is a continuously updating capture file that will overwrite itself if the specified rolling capture size is reached (i.e., it 'rolls over'). It will keep overwriting the captured data until it is stopped by the user. The selected rolling capture size may never be reached, as many of the packets captured may be less than the maximum MTU size (so the buffer may never be entirely full). The default selection is 'None' as Rolling Capture is off by default. The file may be downloaded after the capture is stopped.
- **Logical Pair:** The logical pair on which to capture traffic.
- **Filter:** Specify tcpdump filters to limit capture data. Click the blue question mark icon for sample filters.
- **Max Packet Size:** The maximum number of bytes to capture per packet
- **Analyze:** Once the capture has been taken it can either be analyzed, or downloaded.
- **Stop Analysis:** This allows the user to stop the analysis while it is processing. For large captures the analysis may take a good deal of time.

Display:

Pressing each of the display buttons shows the corresponding analysis to the right of the buttons.

- **VLAN IDs:** These are the VLAN IDs seen in the capture files
- **Protocols:** The different protocols seen on those interfaces
- **ARP Traffic:** The ARP messages seen on each of the interfaces.
- **Top 10 Traffic (Upstream):** Statistics for the traffic seen on the upstream interface, sorted by the number of packets.
- **Top 10 Traffic (Downstream):** Statistics for the traffic seen on the downstream interface, sorted by the number of packets.
- **Top 10 TCP Ports:** Display statistics on the ports being used by the TCP traffic
- **Top 10 UDP Ports:** Display statistics for the top UDP ports used in the capture

Limited Shell Commands

Using the key you generated from the System page, you can log into the appliance over SSH. This will give you a limited shell.

```
$ ssh -i badu_hostname_ssh_key_mm_dd_yyyy_HH_MM_SS.key customer@10.10.10.10
Last login: Thu Aug 17 14:05:20 2017 from 10.10.10.15
You are in a limited shell.
Type '?' or 'help' to get the list of allowed commands
customer:~$
```

As you can see above, typing '?' or 'help' will list the allowed commands. They are also listed below, with descriptions:

- **arp** - Address resolution display and control
- **arping** - Send ARP REQUEST to a neighbor host
- **bpctl_util** - Silicom Linux Bypass-SD control utility
- **clear** - Clear the terminal screen
- **ethtool** - Query or control network driver and hardware settings
- **exit** - Exit the SSH session
- **help** - Print the list of allowed commands
- **history** - Print command line history
- **ifconfig** - Configure network interface
- **ip** - Show / manipulate routing, devices, policy routing, and tunnels
- **lsblk** - List block devices
- **netstat** - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
- **ping** - Send ICMP ECHO_REQUEST to network hosts
- **reset_to_default** - Resets the appliance to default configuration
- **restart** - Reboot the machine
- **revert_to_factory_firmware** - Revert the appliance to manufacturer firmware version
- **route** - Show / manipulate the IP routing table
- **sensors** - Print sensors information
- **smartctl** - Control and Monitor Utility for SMART Disks
- **traceroute** - Print the route packets trace to network host

These can be useful tools for debugging and diagnosing any issues, should they arise. If there is some desired functionality that is not available, please contact Badu for remote support.

Console Options

If for some reason you want to boot to another partition (to run an older version of software, for example), you can do so via the Grub menu when you have console access. Generally, this should only be done when directed by Badu support.

During boot, you will have 10 seconds to press a key to enter the Grub menu.



When you press a key, you will see the menu with each of the available software versions.



You will not be able to edit these entries. Select the desired option and press Enter to boot. Note that this is a **one time** boot, and any subsequent reboots will revert back to the default partition.

Manufacturing Reset

For boxes manufactured with 4.2-b14.2 or later, there will be a "Manufacturing Reset" option. This will perform the factory reset functionality and reset the active and inactive partitions to match the manufacturing partition. Note that this will cause loss of data and configuration settings.

Known Issues

- If your browser is having issues communicating with the *WarpAdmin* GUI, please make sure the appliance IP address is a trusted site in your browser settings.
- Firefox and Chrome are the only officially supported browsers for *WarpAdmin*. If you experience issues with Internet Explorer or some other browser, please try again with Chrome or Firefox before contacting Badu.
- Occasionally a page refresh may be required if a page appears to hang, or if *WarpAdmin* fails to reconnect after a reboot.

Full release notes can be obtained on the Badu Networks Licensing web site at license.badunetworks.com.

Contacting Badu Networks

Support Checklist

In order to efficiently address issues with *Warp* products the following items are required to provide support:

- A network diagram that includes the following components
 - Server and Client with their IP addresses
 - Private equipment between the server and client (network emulation, VPN, etc.)
- A description of the problem, including expected behavior
- A traffic capture on the *Warp* product while the issue is occurring (capture should include the start of the TCP connection)
- The SOS file from the proxy taken after the issue has occurred (before reboot)
- A description of what debugging steps have been carried out, and their results.

Send this information or a link to the information to: support@badunetworks.com

If this issue relates to an ongoing POC, please send to: poc-support@badunetworks.com

General Contact Information

Email: support@badunetworks.com

Phone: (949) 310-5390

Fax: (888) 958-7697

Address: 2640 Main Street, Irvine, CA 92614, USA

Warranty Information

Limited Software Warranty

Badu warrants that the encoding of the software program on the media on which the Product is furnished will be free from defects in material and workmanship, and that the Product shall substantially conform to its user manual, as it exists at the date of delivery, for a period of ninety (90) days. Badu's entire liability and Your exclusive remedy under this warranty shall be, at Badu's option, either: (i) return of the price paid to Badu for the Product, resulting in the termination of this Agreement, or (ii) repair or replacement of the Product or media that does not meet this limited warranty. EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN THIS SECTION, THE PRODUCT AND ANY SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. BADU DOES NOT WARRANT THAT THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. BADU DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to You. This warranty gives You specific legal rights. You may have other rights that vary from state to state.

Limited Hardware Warranty

Badu Networks, Inc. ("Badu") systems use 100% compliant hardware components in accordance with industry-standard practices. Badu warrants that its hardware systems will be free from defects in materials and workmanship. The limited warranty term is one year beginning on the date of invoice, as further described below.

Damage due to shipping the products to you is covered under this limited warranty. Otherwise, this limited warranty does not cover damage due to external causes, including accident, abuse, misuse, problems with electrical power, servicing not authorized by Badu, usage not in accordance with product instructions, failure to perform required preventive maintenance, and problems caused by use of parts and components not supplied by Badu.

This limited warranty does not cover any items that are in one or more of the following categories: software; external devices; accessories or parts added to a Badu system after the system is shipped from Badu; or accessories and parts that are not installed in a Badu approved facility. Ethernet cables and power cables are not covered under this limited warranty.

During the one-year period beginning on the invoice date, Badu will repair or replace products returned to Badu's facility or to a designated reseller. To request limited warranty service, you must contact Badu's Customer Technical Support within the limited warranty period. Refer to the following section titled "Contacting Badu" to find the appropriate telephone number for obtaining customer assistance. If limited warranty service is required, Badu will issue a Return Material Authorization Number. You must ship the products back to Badu in their original or equivalent packaging, prepay shipping charges, and insure the shipment (or accept the risk of loss or damage during shipment). Badu will ship the repaired or replacement products to you freight prepaid if you use an address in the continental United States, where applicable. Shipments to other locations will be made freight collect.

NOTE: Before you ship the product(s) to Badu, make sure to back up your configuration files. Badu does not accept liability for lost configuration or other modifications made to a Badu system. Do not ship any cables or power cords with your product.

Badu owns all parts removed from repaired products. Badu uses new and reconditioned parts made by various manufacturers in performing limited warranty repairs and building replacement products. If Badu repairs or replaces a product, its limited warranty term is not extended.

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE (OR JURISDICTION TO JURISDICTION). BADU'S RESPONSIBILITY FOR MALFUNCTIONS AND DEFECTS IN HARDWARE IS LIMITED TO REPAIR AND REPLACEMENT AS SET FORTH IN THIS LIMITED WARRANTY STATEMENT. ALL EXPRESS AND IMPLIED WARRANTIES FOR THE PRODUCT, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD SET FORTH ABOVE AND NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WILL APPLY AFTER SUCH PERIOD. SOME STATES (OR JURISDICTIONS) DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

BADU DOES NOT ACCEPT LIABILITY BEYOND THE REMEDIES SET FORTH IN THIS LIMITED WARRANTY STATEMENT OR LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION ANY LIABILITY FOR PRODUCTS NOT BEING AVAILABLE FOR USE OR FOR LOST DATA OR SOFTWARE. SOME STATES (OR JURISDICTIONS) DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

These provisions apply to Badu's one-year limited warranty only. For provisions of any on-site service contract covering your system, refer to the separate on-site service contract.