OPTIMIZERCREW

# Installation Notes

## Installation

The blue Ethernet connector on the back of the unit should be connected to your broadband satellite device.  The broadband satellite unit should be configured as a DHCP server, which is the default for most terminals.

The 4 yellow Ethernet connectors are LAN adapters and are bridged to WiFi. There are 2 WiFi transmitters with frequencies at 2.54 and 5.2 Ghz.  The WiFI SSID is of the form “wxa-115-XXXX-frequency” where XXXX is the last 4 digits of the unit’s WiFi interface MAC address and “frequency” is the transmission frequency of the transmitter.  The WiFi is unsecured so no password is required to connect to this device.

## Connecting to the Device

Connect a PC to either the LAN or WiFi on the router.  Alternately, administrators can access the unit through the WAN port.   The router is configured as a DHCP server so PCs should be able to access the router and the Internet once they are connected.

## Router Interface Addresses

LAN/WiFi bridge:  192.168.10.1
Captive Portal: 10.1.5.1
WAN: DHCP

***New Feature:***

## Multi-Level Access To Optimizer Crew User Interface

There are two levels of administrative access for Optimizer Crew:

## Admin

- Create PIN-codes for controlled Internet access
- Manage users
- Create email subaccounts for guests and crew
- View CDRs (Usage Records)

“Admin” access is designed for the on-site administrator who may not have the technical knowledge required to configure the router. Basic functions (like creating PIN-codes) can be accessed, but more advanced features like router and network configuration require “Superadmin” access.

## Superadmin

“Superadmin” access is designed for the installer/technician/network administrator. It allows full access to the user interface for setup, configuration, and maintenance of the router.

# Router Admin Login

**Superadmin**
Username: superadmin
Password: webxaccess

**Admin**
Username: admin
Password: webxaccess

# Default Router Configuration

Optimizer Crew is shipped with the following configuration:

1. Captive portal enabled, allowing for crew Internet access with pincodes or administrator assigned username and password.
2. Transparent proxy for http URL and content filtering.
3. Open firewall allowing full access to the Internet once the crew member logs into the captive portal.
4. Open DNS allowing the resolution of IP addresses for all machines on the LAN/WiFi whether logged in or not through the captive portal.

5. RedPort email, web compression, and VOIP servers white listed through the captive portal. The captive portal in this configuration does not account for use of XGate/XWeb software or RedPort VOIP.

Note that browsers needing to access the Internet require DNS. DNS will generate traffic that is not accounted for by the captive portal. On networks with multiple PCs this traffic can be considerable.

# First Use with XGate, XWeb, and/or RedPort VOIP

No router changes or configuration is required when using XGate, XWeb or RedPort VOIP services. The router is configured to allow this traffic through. The Optimizer Crew blocks all other traffic except for DNS.

XGate/XWeb users should refer to the Optimizer Quick Start Guide when using Optimizer Crew in this mode.

# First Use

Users must log in through the captive portal before they can access the Internet. To log in, open a browser and enter a URL such as http://www.amazon.com. The captive portal will intercept the request and redirect the user to a login page. A valid username/password or pincode must be entered before access to the Internet is granted.

Once logged in, any application (web based or otherwise) should have access to the Internet.

# Captive Portal Usage

As stated above, entering an http:// URL into a browser redirects the user to the captive portal login page. Alternately, users can access the captive portal directly using one of the following URLs.

- Login – http://10.1.5.1:4990/www/login.chi
- Status – http://10.1.5.1:4990/www/status.chi
- Logout – http://logout

The captive portal status page provides status information for the current active session such as:

- Max Session Time: maximum allowed time before user is forcibly logged off.
- Max Idle Time:  user is logged off automatically if no traffic is observed within this period.
- Start Time: session start time.
- Idle time: time of idle activity.
- Downloaded: amount of data transferred to the user.
- Uploaded: amount of data requested by the user.
- Original URL:  URL that initiated the login request.

Users can end a captive portal session by either clicking the logout link on the status screen or by entering http://logout in their browser.

The captive portal ships configured with two accounts. They are:

- admin/webxaccess
- test/1234

The admin account is open and has no restrictions.  The test account is restricted to 10Mbytes of total usage at a speed of 128kbps.

# Router Administration

When the captive portal is enabled, the router admin page is accessed via http://10.1.5.1.  However, this URL will not work when the captive portal is disabled and not in use.

When the captive portal is disabled, the router admin page is accessed via http://192.168.10.1.

# Web Compression

You must have a valid web compression account before using this feature.  Please contact your RedPort dealer and request a username and password for the compression service.

Once you have your account information, log in to the router and browse to Services > Web Compression and Filtering > select the Compression tab.  Check the Enable Compression option and enter your assigned credentials. Click <Save & Apply>.

You should now be able to browse the Internet with compression enabled.

# Optimum Setup

The default configuration works well offering reasonable bandwidth over-utilization protection. With the default, users must log in through the captive portal before they can access Internet resources. However, once logged in, their computers can generate unwanted usage that causes their pincodes to be consumed quickly. Users can also use Skype and other P2P applications that require a lot of bandwidth.

Also note that DNS access must be enabled to use the default configuration. Without DNS, web browsers timeout when trying to resolve host names which prevents them from being redirected to the captive portal login page. DNS can drive unexpected large bandwidth usage because it is accessible to all computers and programs running on the local network. 30-50Mbytes per month in DNS traffic usage is not unusual for vessels with 10 or more computers connected to the LAN and powered on all the time.

The following configuration blocks all traffic to the Internet. Users must log in though the captive portal to have access to HTTP and HTTPS traffic. All other traffic is blocked, preventing Skype and other P2P applications from working. This setup also has the advantage of passing HTTPS traffic through the filtering proxy server that allows the administrator to block sites. Users, when using this alternate setup, will need to change the default settings in their browsers and use the direct captive portal login link to login.

The following procedure will enable the alternate optimum setup:

1. Log in to the Optimizer Crew admin portal.
2. Navigate to Network > Firewall > Traffic Rules
3. Uncheck the first 6 rules at the top of the list labeled "XX – DO NOT MODIFY" where XX is ALL, PASS DNS, DNS, HTTP, HTTPS, and FTP.
4. Select "Save and Apply" at the bottom of the page. This will modify the firewall to block access to all traffic including DNS.
5. Instruct the end user to modify their browser configuration to enable "Automatic Proxy Detection". For Firefox this is done under Preferences > Advanced > Network > Settings by selecting "Auto-detect proxy settings for this network". Other browsers can be configured similarly.
6. Instruct the user to use the captive portal URL to access the login page. This is done by entering http://10.1.5.1:4990/www/login.chi in the browser.
7. Once logged in, the user will have access to all http and https websites.
8. Entering http://logout will log the user out of the captive portal and end his session. Alternately, the user could use the status page at http://10.1.5.1:4990/www/status.chi and log out from there.

# Factory Default

Optimizer Crew can be reset to factory default by pressing the reset button on the back of the router for 15 seconds and then releasing it.  The router will then reboot and start backup with its default settings.

# Optimizer Crew Guides

Usage and administration guides can be found at http://www.redportglobal.com