AVANU®

Load Balancing for Microsoft® Office Live Communications Server 2005 WebMux Delivers Improved Reliability, Availability and Scalability

Overview of WebMux Load Balancer and Live Communications Server 2005

- Introduction
- Why WebMux Load Balancer
- Live Communications Server and WebMux Network Topology

Configuring WebMux for Live Communications Server 2005 Deployment

- Pre-configuration Check List
- Configure WebMux in NAT Mode and Enable Web Administration
- Configure Live Communications Server Enterprise Edition Pool to use the Load Balancer

Managing WebMux in Live Communications Server 2005 Deployment

- Overview
- Remote Management
- Change Default Password
- Restricted Access
- Email Notification
- WebMux Settings Backup

WebMux Product Specifications and Technical Support Information

Overview of WebMux Load Balancer and Live Communications Server 2005

Introduction

Microsoft®, AVANU® and CAI Networks joined forces to incorporate load balancing using WebMux to assure maximum availability of service in directing traffic in Microsoft's Office Live Communications Server 2005.

The Live Communications Server network topology incorporates a pool of servers to service client sessions. With a WebMux load balancer, incoming client traffic is managed and directed to this pool so that no one server is ever overloaded. WebMux supports both Microsoft® Office Live Communications Server 2005 Enterprise Edition and Microsoft® Office Live Communications Server 2005 Standard Edition.

Reliable traffic management, security, and ease of implementation are just a few of the WebMux load balancer benefits validated by interoperability tests completed by Microsoft® and CAI Networks in the Live Communications Server environment.

Why WebMux Load Balancer

The approach used to achieve load balancing impacts the reliability and high availability of a service. WebMux uses a dedicated hardware platform with an optimized load balancing algorithm. This approach uses minimal overhead and requires no software interaction or other resource contention. CAI Networks chose a solid-state design approach for WebMux to eliminate hard drive failure worries for enhancing reliability and high availability of service.

WebMux performs automatic health checks to evaluate the functioning of the servers in the pool. If a problem server is identified or is taken off line for service, WebMux will direct Live Communications Server traffic to other available servers. WebMux can bring a standby or backup server online, and can notify an administrator of these network activities. WebMux also allows servers to be added to the pool in real time to increase a network's capacities. Resistances to hacker intrusions are assured with the built-in firewall functions.

For maximum availability, a Live Communications Server network may have a primary and secondary WebMux in a failover configuration to assure uninterrupted network.

WebMux is a stand alone, self-contained and ready to install network device. WebMux's front panel menu-driven display and keypad allow for easy configuration and expedient deployment. WebMux is 14" deep x 1-3/4" high, 1U in a standard 19" rack.

The WebMux load balancer delivers unmatched reliability with the industry's lowest total cost of ownership. The $3,999 list price includes a full three (3) year warranty and three (3) years of free technical support.

♦ NOTE

This document assumes you are familiar Microsoft® Office Live Communications Server 2005 Enterprise Edition or Microsoft® Office Live Communications Server 2005 Standard Edition and WebMux Load Balancer. Consult appropriate documents for additional information.

Additional information on Live Communications Server can be found at http://www.microsoft.com/livecomm. For additional information on WebMux Load Balancer, go to http://cainetworks.com or http://www.avanu.com.

Live Communications Server and WebMux Network Topology

The example in Figure 1.1 shows a network topology using a pair of WebMux Load Balancers to direct and manage traffic between client and a Live Communications Server pool

♦ NOTE

A redundant WebMux configuration is recommended to assure high availability and uninterrupted service. The secondary WebMux is passive on the network and becomes active, should the primary WebMux fail or be taken off line for service.

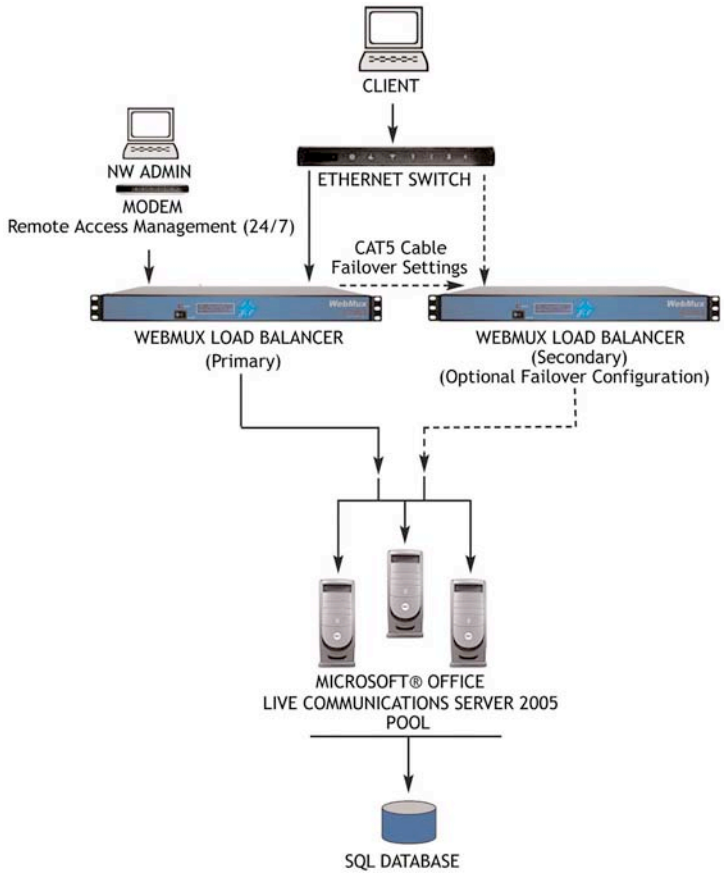


Figure 1.1 Microsoft® Office Live Communications Server 2005 Network Topology Example Using Redundant WebMux Load Balancers

Configuring WebMux for Live Communications Server 2005 Deployment

This paper describes how to install, configure and manage WebMux in the Live Communications Server environment. First is a section on what to do before starting the configuration. Then there is a step-by-step description of how to configure WebMux using its front panel keypad and LCD display. WebMux can be managed via web UI, which is addressed later. Once WebMux is configured and ready for operation, a web UI is used to configure the pool. Key screens are displayed to assist the user in identifying the appropriate fields. Finally a discussion on several key management functions is presented.

Pre-Configuration Checklist

A typical network topology is show in Figure 1.2. It is important to assimilate all the network information and product documentation. The table in the following section can be used. It is recommended that you familiarize yourself with the User Guide which ships with WebMux or can be downloaded at http://www.cainetworks.com or http://www.avanu.com (Support & Downloads)

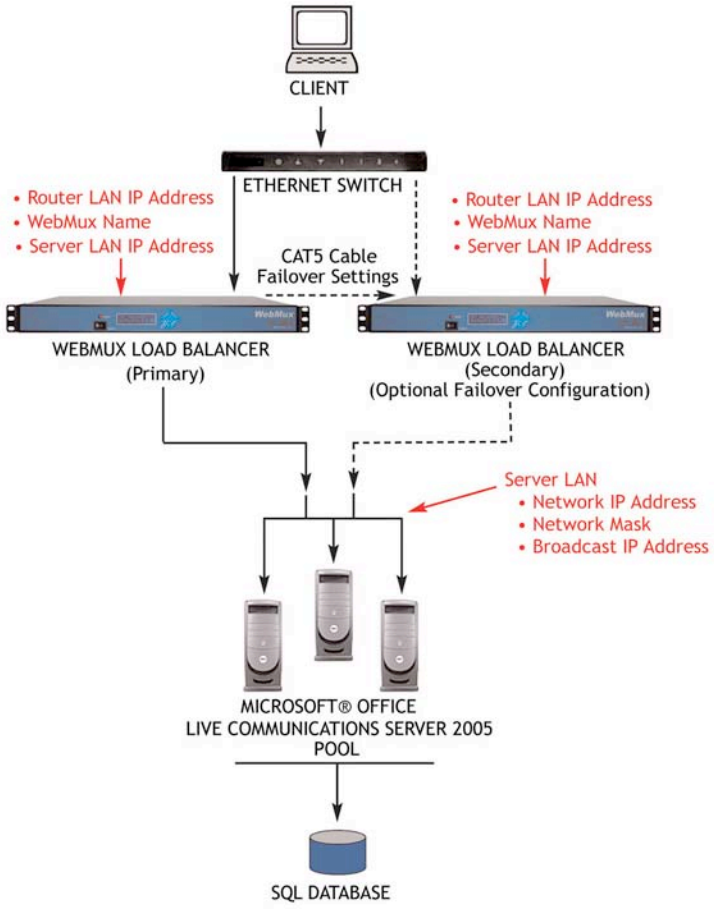


Figure 1.2 Network for Live Communications Server Implementation

Network Information

1. Make a drawing of the existing network and note all the configuration settings. This provides a fall back to the existing configurations if needed.
2. Make a new drawing for the new setup with the WebMux and the Live Communications Server in place. This is used as a guide for setup and preparation of all the necessary material and equipment. Use figure 1.2 as a guide.
3. Collect all the IP addresses, their network masks, network addresses, and broadcast addresses for the Server LAN and Router LAN WebMux interfaces. The IP address of the network is also needed. The table below can be used to document all the collected IP information.
4. Label all the cables. Prepare additional cables if needed.
5. Make sure there are enough electrical or UPS outlets for all the new equipment.

Sample Network Information (Before WebMux Installation)

Equipment	IP Address
Internet Router (or Firewall) Address	205.133.156.1
Webserver(s) Default Gateway	205.133.156.1
Web Site IP Address	205.133.156.200

Sample Network Information (After WebMux Installation)

Question	Entry	
	Primary	Secondary
Host Name	webmux1	webmux2
Domain Name	Cainetworks.com	Cainetworks.com
NAT or Out-of-Path	NAT	NAT
Router LAN Information		
Router LAN WebMux Proxy IP Address	205.133.156.200	205.133.156.200
Router LAN Network IP Address Mask	255.255.255.0	255.255.255.0
Router LAN Network IP Address	205.133.156.0	205.133.156.0
Router LAN Broadcast IP Address	205.133.156.255	205.133.156.255
Server LAN Information		
Server LAN WebMux IP Address	10.1.1.10	10.1.1.20
Server LAN Gateway IP Address	10.1.1.1.1	
Server LAN Network IP Address Mask	255.0.0.0	255.0.0.0
Server LAN Network IP Address	10.0.0.0	10.0.0.0
Server LAN Network Broadcast Address	10.255.255.255	10.255.255.255
Administration Setup Information		
External gateway IP address	205.133.156.1	205.133.156.1
Remake /home/webmux/conf/passwd	Y	Y
Administration HTTP Port Number	24	24
Secure Administration HTTPS Port	35	35
Is this WebMux primary	Y	N
WebMux running solo without backup	N	
Reboot?	Y	Y

Network Information Worksheet (Before installing WebMux)

Equipment	IP Address
Internet Router (or Firewall) Address	
Webserver(s) Default Gateway	
Web Site IP Addresses	

Network Information Worksheet (After WebMux installation)

Question	Entry	
	Primary	Secondary
Host Name		
Domain Name		
NAT or Direct Routing		
Router LAN Information (NAT ONLY)		
Router LAN WebMux Proxy IP Address		
Router LAN Network IP Address Mask		
Router LAN Network IP Address		
Router LAN Broadcast IP Address		
Server LAN Information		
Server LAN WebMux IP Address		
Server LAN Gateway IP Address		
Server LAN Network IP Address Mask		
Server LAN Network IP Address		
Server LAN Network Broadcast Address		
Administration Setup Information		
External Gateway Address		
Remake /home/webmux/conf/passwd	Y/N	Y/N
Administration HTTP Port Number		
Secure Administration HTTP Port #		
Is this WebMux primary	Y	N
WebMux running solo without backup	Y/N	
Reboot?		**Y/N**

Network Setup

1. Power down all the devices on the network
2. Connect the Secondary WebMux with a crossover Ethernet (Standard CAT5) cable.
3. Connect the Servers in the pool to the LAN.
4. Connect the WebMux unit(s) to the Server LAN (pool side)
5. Connect the WebMux unit(s) to the Router LAN (client side)

Configure WebMux in NAT Mode and Enable Web Administration

Initial configuration of a WebMux Load Balancer to work with a Live Communications Server pool is accomplished using the WebMux front panel keypad and display.

♦ NOTE

For more information about WebMux, go to http://www.cainetworks.com or http://www.avanu.com.

1. **WebMux firmware** must be version 5.8.08 or later.
   This will display on front panel LCD as the system is turned on.

2. After WebMux runs a self-test and is fully booted, hold down the **Check-Mark** button. Enter **WebMux host name**

3. All information can be changed later using the configuration URI /cgi-bin/rec

4. Enter WebMux's **host name** using right, up and down arrows.
   Used for identification purposes only.

5. Enter the WebMux **domain name**.
   Used for identification purposes only, has no effect on the network operation

6. Choose **NAT** mode.

7. Enter WebMux **Router LAN Proxy IP** address.
   This is the IP address of the WebMux interface that connects to the enterprise LAN and must be unique for each WebMux.

8. Enter **network mask** of the Router LAN network.
   Commonly 255.255.255.0 for class C networks.

9. Enter WebMux **Server LAN IP** address.
   This is the IP address of the WebMux interface that connects to the Server LAN and must be unique for each WebMux. This address must also be different from the server LAN gateway address.

10. Enter **Server LAN Network IP address mask**.
    This is the network mask of the Server LAN. For a class A network it may be 255.0.0.0. For a class C network, it may be 255.255.255.0.

11. Enter **server LAN Gateway IP** address.
    This IP address will be the Default Gateway entry for all the servers on the Server LAN. In a single WebMux set up, this address cannot be the same as the WebMux IP interface address on the Server LAN. In a dual WebMux set up, if a gateway of 10.1.1.1 is used, this address will "float" between the primary and secondary WebMux.

12. Enter **External Gateway**. The default gateway for WebMux.

13. Finish configuration with regard to Primary or Secondary WebMux. (For more information about setup and configuration of dual WebMux units, see the OEM documentation.)

14. Answer **[Yes or No]** to "Clear allowed hosts?"
    Clearing the host file will allow any computer to access the management console. By default all hosts are allowed to connect. This is only necessary when you may have locked yourself out of the management interface.

15. Answer **[Yes or No]** to "remake passwords?"
    The factory default password is the same as the logon ID. Answering, "Yes" will reset the password back to factory default. Default users are webmux and superuser. The passwords are webmux and superuser respectively.

16. Enter **Admin http Port number**.
    This is the port number for accessing the Management Console in non-secure mode. Any unused port number can be used. The factory default is port 24.

17. Enter **Admin https Port Number**.
    This is the https port number for accessing the Management Console in secure mode. The factory default is port 35.

18. Save changes by answering "No" to 'Discard Changes' and reboot WebMux.

♦ NOTE

Ensure Connectivity between the Client and Live Communications Server pool. Ideally, DNS is used for automatic discovery. For manual configuration, you must modify host files on each client as: <IP_address_of_the_TLS_Farm_or_TCP_Farm> <FQDN_of_the_Pool>

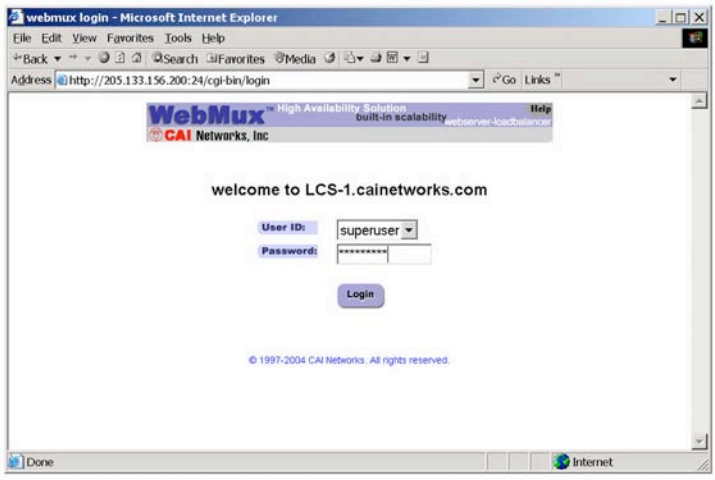
Configure Live Communications Server Enterprise Edition Pool to Use the Load Balancer

Use the following procedure to configure Live Communications Server Enterprise Edition pool and its servers to use the load balancer.

19. Open Web UI for the WebMux Load Balancer http://ip:24/cgi-bin/login

♦ NOTE

Browser must be set to accept all cookies.

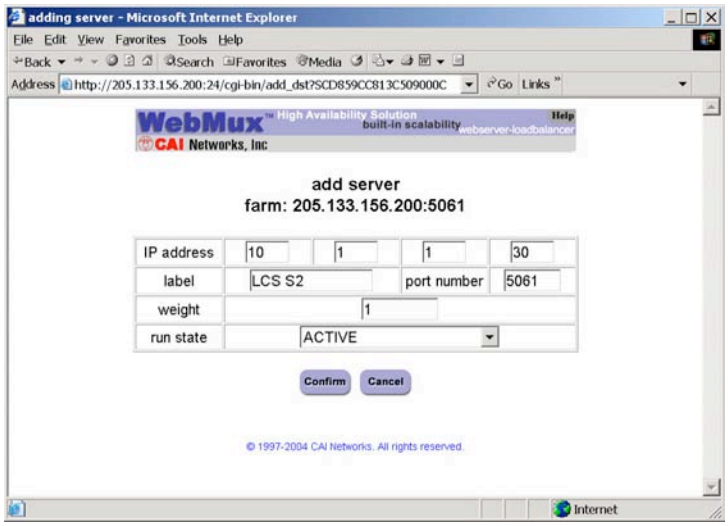


a. Pull down account name superuser and type superuser for the password.
b. Click **Login**.

20. Add a TLS Farm:
    a. At the bottom of the page, click **Add Farm**.

b. In **IP address**, type the assigned Virtual IP address for your pool.
c. In **Label**, type in a friendly name for your pool.
d. In **Port number**, type 5061.
e. In **Service**, click **generic (TCP)**.
f. In **Scheduling method**, click **Least connections**.
g. Click **Confirm**.

21. Add internal Live Communications Servers to the TLS Farm:
    a. Click the IP Address link for the TLS Farm.
    b. Click **Add Server**.



    c. In **IP address**, type static IP address of the internal Live Communications Server you want to add to the farm.
    d. In **Label**, type in the server name for the Live Communications Server.
    e. Click **Confirm** and repeat these steps for each additional server in the pool.

♦ NOTE

If you must delete a farm, you do not have to delete all servers within this pool before you delete the farm. When deleting the farm, all virtual servers contained in that farm are also deleted.

22. Optionally, add a TCP Farm (if clients are to connect to the pool through TCP):
    a. At the bottom of the page, click **Add Farm**.
    b. In **IP address**, type assigned Virtual IP address for your pool.
    c. In **Label**, type in a friendly name for your pool.
    d. In **Port number**, type 5060.
    e. In **Service**, click **generic (TCP)**.
    f. In **Scheduling method**, click **Least connections**.
    g. Click **Confirm**.

23. Add internal Live Communications Servers to the TCP Farm (only if a TCP Farm is added in Step 22):
    a. Click the IP Address link for TCP LC Farm.
    b. Click **Add Server**.
    c. In **IP address**, type the static IP address for Live Communications Server that you want to add.
    d. In **Label**, type the server name for the Live Communications Server.
    e. Click **Confirm** and repeat this process for each server in the pool.

24. Add Management Farm:
    a. At the bottom of the page, click **Add Farm**.
    b. In **IP address**, type the assigned VIP address for your pool.
    c. In **Label**, type a friendly name for your pool.
    d. In **Port number**, type 135.
    e. In **Service**, if a TLS farm was configured then **select management of Microsoft TLS Live Communications Server (TCP)**, or else if only a TCP farm was configured then select **management of Microsoft TCP Live Communications Server (TCP).**

♦ NOTE

If menus above do not come up, contact support@cainetworks.com or support@avanu.com for configuration instructions.

    f. In **Scheduling method**, click **Least connections**.
    g. Click **Confirm**.

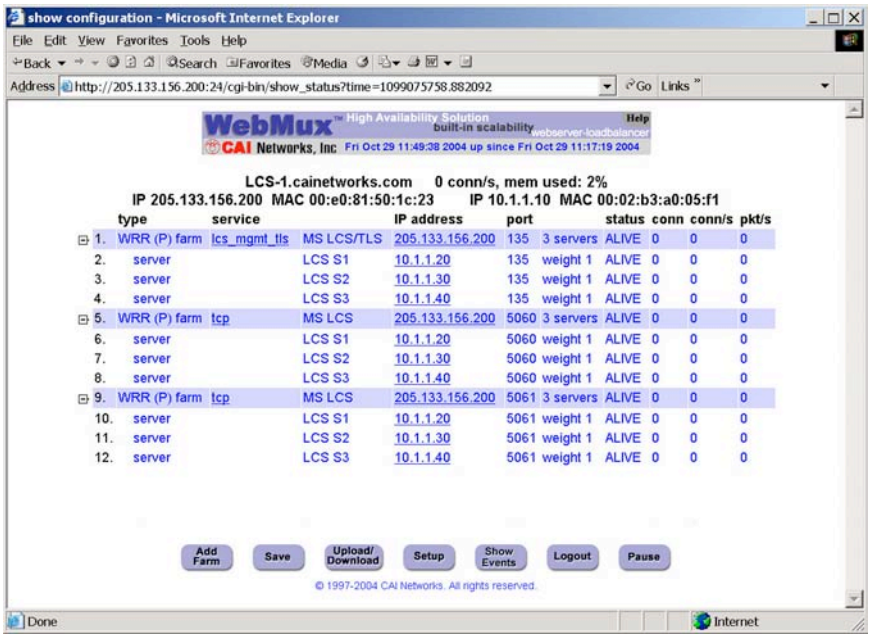
25. Add internal Live Communications Servers to the Management Farm:
    a. Click the IP Address link for Management Farm.
    b. Click **Add Server**.
    c. In **IP address**, type the static IP address for Live Communications Server that you want to add.
    d. In **Label**, type the server name for the Live Communications Server.
    e. Click **Confirm** and repeat this process for each server in the pool.

26. Enable IP forwarding
    a. Open web admin interface http://[ip address]/cgi-bin/login
    b. Log in as superuser
    c. Click **Setup** button at the bottom of the page
    d. In forwarding policy field, choose accept
    e. Click **Confirm** button
    f. Click **Logout** button
    g. Click **Confirm** button

♦ NOTE

The enterprise router must be configured to route traffic to the server LAN IP subnet via the router LAN IP address on the WebMux

The following picture shows an example of what the main screen might look like after all the configuration changes are made.



27. Log off the WebMux load balancer Web UI:
    a. At the bottom of the page, click **Logout**.
    b. Click **Confirm**.

Overview

WebMux offers a variety of administrative, management, security, and monitoring functions that can be managed and accessed through a web browser. A complete description of these is in the WebMux User Guide. Following is a brief overview of steps for implementing these basic functions:

- Remote management
- Change default passwords
- Restricted access
- Email notification
- Farm configurations and WebMux settings backup

♦ NOTE

WebMux User Guide comes with WebMux Load Balancer and is available at www.cainetworks.com/manuals/manuals.htm or www.avanu.com (Support & Downloads)

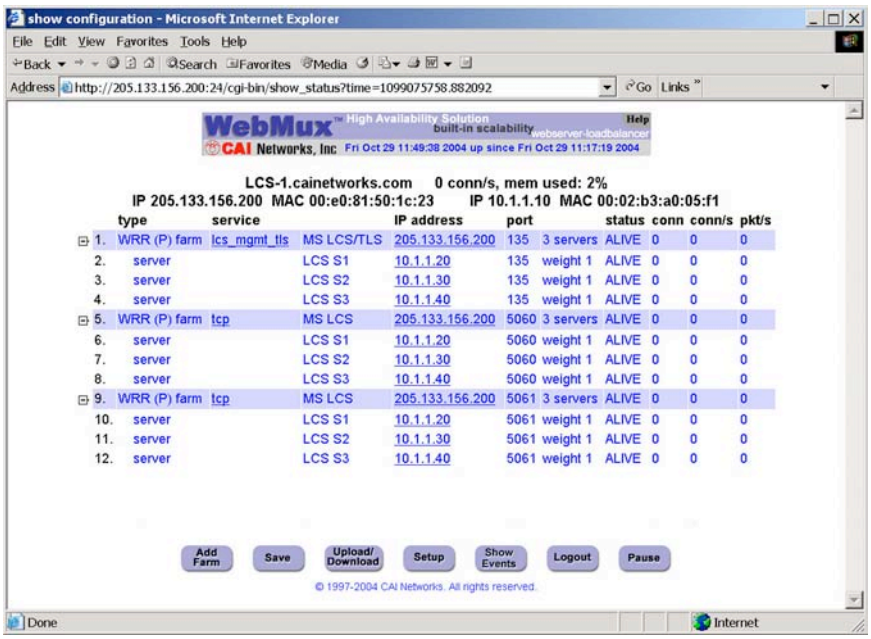
Remote Management

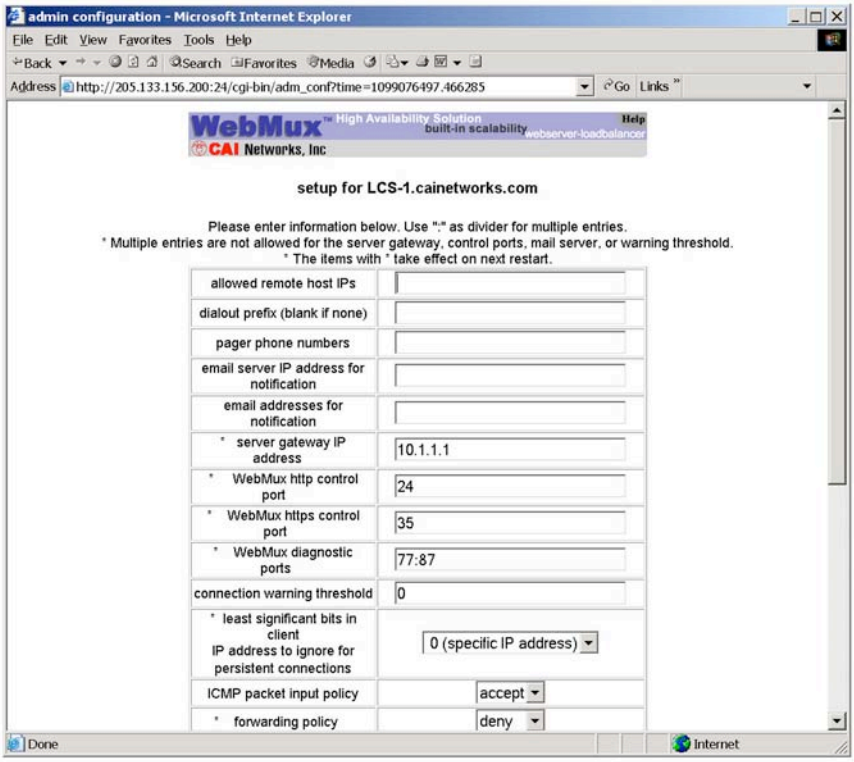
Since the configuration of the Live Communications Server Enterprise pool requires that IP forwarding be enabled between the router LAN and the server LAN networks, the servers in the farm are directly accessible from the router LAN network.

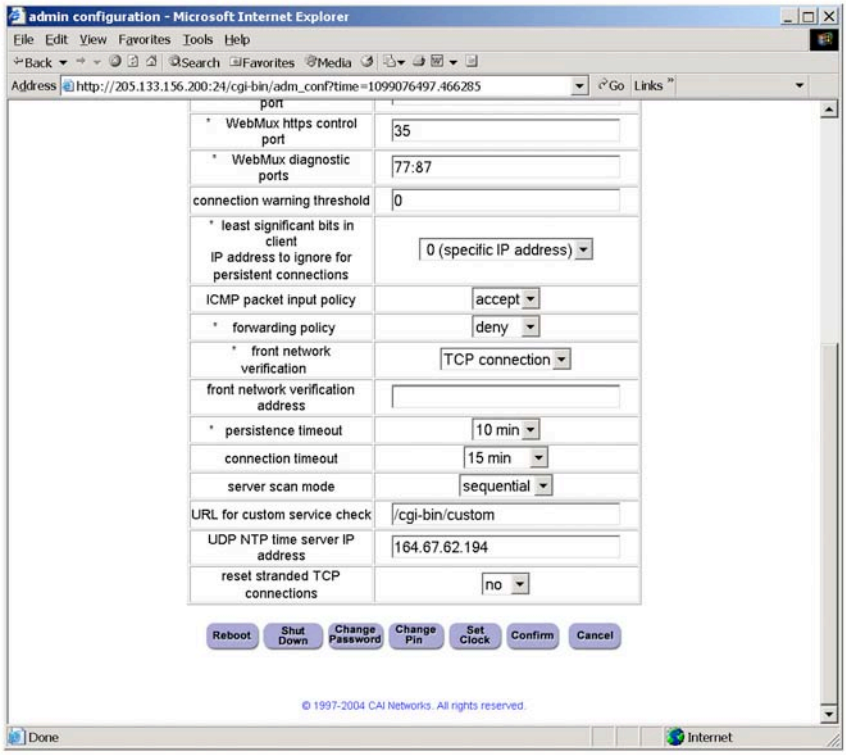
Change Default Passwords

WebMux ships with two default passwords; webmux and superuser. It is recommended these be changed to user specific passwords.

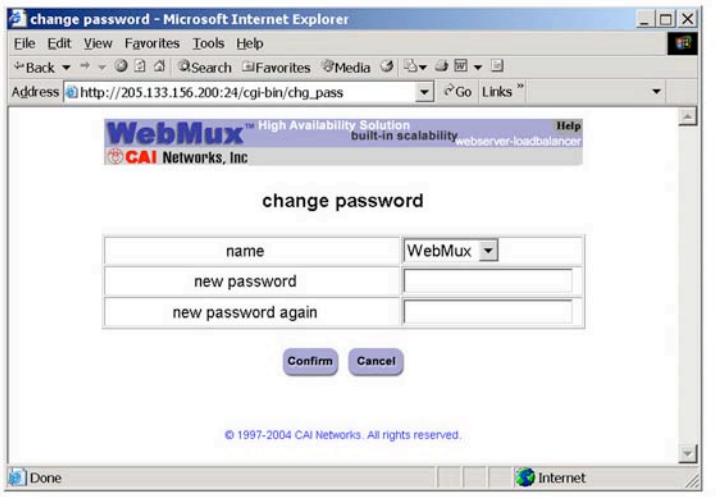
1. Log on as superuser (you must change password from this configuration)
2. From main menu screen select: **Setup**







3. Change password
4. Select user ID for password change



5. Type new password twice (2 times)
6. Click **confirm**
7. Repeat steps for second login and save the configuration once. Both passwords are changed.

Restricted Access

Access to the administrative console can and should be restricted by the WebMux in addition to any firewall or packet filtering device. To restrict access to the WebMux interface:

1. Login to the WebMux as superuser
2. Click **setup** – multiple fields will display. (more detailed explanation in manual
3. Select the box allowing remote host IPs with your management network and/or hosts that will be accessing the WebMux
4. Multiple hosts and networks can be entered using a colon (:) to separate
5. Click **confirm** and **save** the configuration

Email Notification

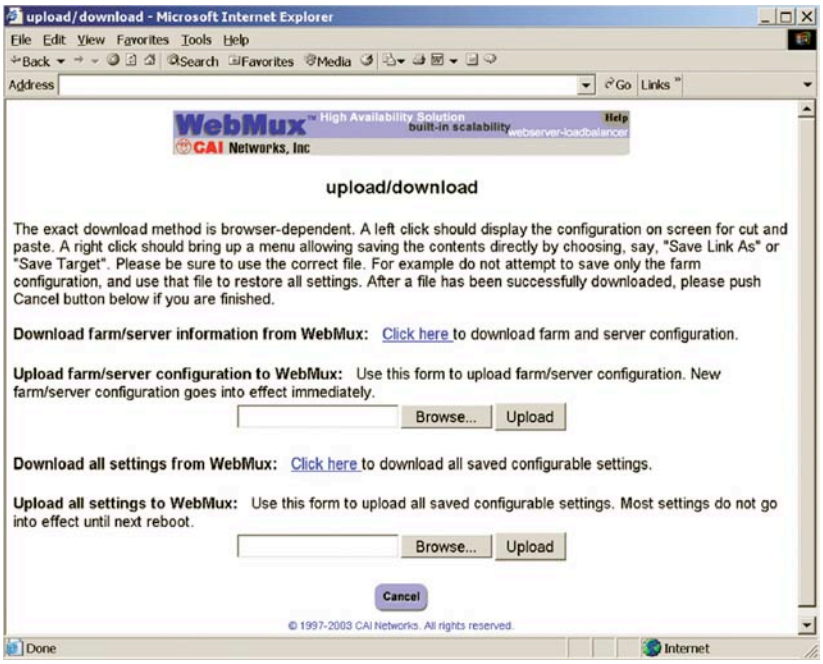
WebMux can be configured to provide email notification of WebMux events

1. Log on as superuser or new password.
2. Select: **setup**
3. Configure the email server IP address for notifications.
4. Configure the email addresses for notifications
5. Multiple email addresses can be entered using colons (:) to separate addresses
6. Click **confirm** and **save** the configuration.

Farm Configurations and WebMux Settings Backup

When changes are implemented, it is recommended that backups of the Web Farm configurations and WebMux configurations are made. The configuration files are small text files that can easily be archived. Be sure to save the configuration before backing up. To back up:

1. From the main menu click **Upload/Download**.



2. Select either:
   a. **backup the settings** or
   b. **backup the farm configurations**

♦ NOTE

When saving the system displays the configuration which can either be cut and pasted into a new file or use the 'save as' feature of the web browser (right click on mouse)

After the Initial Configuration using the keypad and display, a network administrator can now manage WebMux and the network pool through a web browser.

WebMux Product Specifications and Technical Support Information

WebMux product specifications are detailed in the attached data sheet (Appendix A). Additional information is available from www.cainetworks.com, www.avanu.com and the WebMux User Guide.

Technical support is available from CAI Networks at 1.714.550.091, Monday-Friday, 6:30am to 5:00pm PST (Santa Ana CA, USA) and AVANU® can be reached at 1.888.248.4900 (US & Canada toll free), 1.408.248.8961 (Direct), Monday-Friday, 8:00am to 5:00 pm PST (San Jose CA, USA).

AVANU®

1.888.248.4900
US & Canada Toll Free

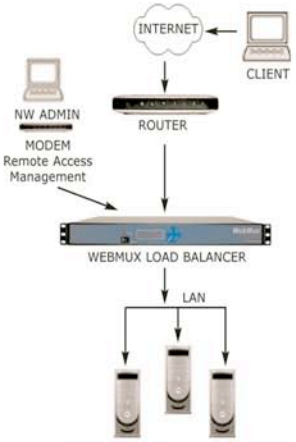
CAI Networks

WebMux Load Balancers

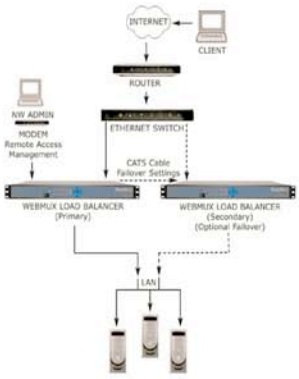
Three (3) Years Product Warranty with Free Technical Support

WebMux load balancers maximize Internet or Intranet service reliability assuring steady network traffic flow, server up time, and resistance to hacker intrusion. They are stand-alone, self-contained and ready-to-install network appliances providing reliable management of IP traffic on 10/100 and Gigabit Ethernet networks. WebMux delivers maximum server performance, flexibility, and user connection with proprietary routing algorithm and supports Network Address Translation (NAT) and direct (Out-of-Path) routing methods. They feature solid-state storage, key pad interface withmenu-driven LCD display for easy setup and deployment. The WebMux products comes with three (3) year warranty and three (3) years technical support

Features	Benefits
Service Reliability	Site or domain traffic is distributed among multiple servers. No one server is bogged down trying to service a particular site. If a server unexpectedly goes down, WebMux will direct the traffic to other servers, or will bring a standby or backup server online to service the traffic.
Health Check	WebMux does application level health check to many service protocols on servers by tracking which servers are functioning properly and which servers are out of service.
Built-in Firewall Protection	Stops possible hacker intrusion into network from farm IP address. Built-in functions will detect any possible denial of service attack and make services always available. (Note: this function only works in NAT mode).
Hardware Based (System Operative Independent)	Reliability of solid-state design and no software or agent to load on the servers. Non-intrusive independent load/failure detection and management.
Burst Activity Management (BAM™)	Eliminates possibility of traffic overloads during bursts of UDP DNS client request.
Fault Tolerance	Two WebMux units, a primary and a secondary will automatically sync the configuration datum. If one experiences a failure, the other will handle traffic.
Proxy Function	When communication is initiated from behind the WebMux, the WebMux will substitute its own address for the internal address. This allows the web servers to initiate communication for services such as credit card validation and mapping services. (Note: this function only works in NAT mode).
Persistent Connections	User browser and server sessions are memorized - sends and keeps the user session with the same server. This is important for sites using shopping cart and dynamically generated pages, like BroadVision, ASP and JSP sites.
In-Path Load Balancing	In normal setup, the WebMux is configured In-Path, to act as firewall in addition to the load balancer and health checker.
Out-of-Path Load Balancing (Direct Routing)	Configuration option when outbound traffic is much larger than inbound traffic and there is already a firewall in place, or change of IP address causes problem.
Services Supported	DNS, FTP, HTTP, HTTPS, NTP, POP3, SMTP, TCP, VOP, UDP, Alkaline Search Engine.
Remote Mangement	Can be managed via a secured web browser session from anywhere in the world using HTTPS 128 bit encryption.
24 x 7 Monitoring	Provides phone pager and email notification to network administrator whenever a server or WebMux goes down, and when it returns online (External modem required)

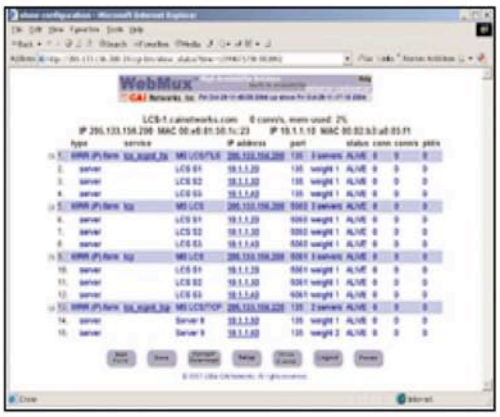


Single WebMux Configuration



Dual WebMux Configuration

Remote Management Browser Window



WebMux Front

Reset Switch
Press & release May take several minutes to reset.

Toggle On/Off
Power Switch Press & hold for 5 seconds.

LCD Display
Menu driven (2 lines), illuminated green lite background.

Cross Button
Cancels a selection. Holding down the button will invoke the configuration menu, allowing IP address changes.

Check Mark Button
Confirms selection.

Left/Right Arrow Button
Moves cursor to left and right of display.

Up/Down Arrow Buttons
Changes value of the cursor location (increase/decrease - lower/upper case letters, numbers and symbols)

When cursor is placed at left most position of LCD, allows different item selection setup.

WebMux Back

Power Supply Connection
Power cord included with WebMux - 115V/230V AC universal power supply

On/Off Power Switch
In "off" position, front panel on/off power

Router LAN Port
Connect to Router LAN switch or hub. Note: Router LAN and Server LAN ports are not intechangeable.

Server LAN Port
Connect to Server LAN switch or hub of servers and local computers.

'Unused' Port

Fail-over Port
Connect a second WebMux for fault tolerant redundancy function (Standard CAT5)

Modem Port
External modem (standard modem cable) for paging, email notification, remote dial-in diagnostic port over Internet (Manufacturer configuration assistance, troubleshooting)

Modems Tested:
USRobotics V.Everything modem, US Robotics part number 3CP3453. Modem dip switches 3/8/10 in down position, all others in up position.

	WebMux #WM108E	WebMux Pro #WM585P
Topologies		
Ethernet/Fast Ethernet (10/100)	Yes	N/A
Gigabit Ethernet (1000Base-TX)	N/A	Yes
Balancing Method		
Round-Robin	Yes	Yes
Persistent Round-Robin	Yes	Yes
Weighted Round-robin	Yes	Yes
Persistent Weighted Round-robin	Yes	Yes
Least Connections	Yes	Yes
Persistent Least Connections	Yes	Yes
Weighted Least Connections	Yes	Yes
Persistent Weighted Least Connections	Yes	Yes
Fastest Response	Yes	Yes
Fault Tolerance		
Solid State Design (no disk drive)	Yes	Yes
Port aggregation	Yes	Yes
Failover via Ethernet (Std CAT5)	Yes	Yes
Service aware	Yes	Yes
Server aware	Yes	Yes
Backup server	Yes	Yes
Performance		
Maximum concurrent connections	*1,440,000	5,760,000
Maximum new connections/second	*7,000	40,000
Maximum throughput/second	200 Mbits/s	1 Gbit/s
Maximum Internet Link Speed	2 x T3	1.5 x OC-12
* Default NAT Mode, Out-of-Path or Direct Routing Mode provides higher performance connections (10 to 100X)		
Management		
Secure web browser access	Yes	Yes
In service/Not in service	Yes	Yes
Page alarms (Modem Req'd)	Yes	Yes
Email notification (Modem Req'd)	Yes	Yes
Configuration access	Yes	Yes
Remote telnet access	Yes	Yes
Persistent connections	Yes	Yes
Port mapping	Yes	Yes
Port-specific services	Yes	Yes
Security Features		
Network Address Translation	Yes	Yes
TCP SYN protection	Yes	Yes
TCP DoS protection	Yes	Yes
SSL support	Yes	Yes
Device Support		
Maximum virtual servers	Unlimited	Unlimited
Maximum real servers	65,532	65,532
Device's role in the network	IP Router	IP Router
UDP-based service support	Yes	Yes
Other		
Product Warranty & Tech Support	3 years	3 years
Overnight Exchange Unit	24/7 Service Contract	
Email Support	Yes	Yes
Phone Support	Yes	Yes
Rack mount chassis (19"x 14"x1.75")	1U	1U
Weight	19 lbs	20 lbs
Power requirement	90-130VAC, 2.5 A or 190-235 VAC, 1.5 A, 50-60 Hz	
Operating temperature	0-40 C	0-40 C
Compliance	Part 15, FCC (US), Class B (Canada), CE Mark (Europe)	

AVANU®
1600 Saratoga Ave #403-107
San Jose CA 95129-5108
USA

Rev 1104a