

Load Balancing
Outlook Web Access
Web Mail Using Equalizer



Copyright © 2009 Coyote Point Systems, Inc.

All Rights Reserved. Printed in the USA.

Publication Date: January 2009

Equalizer is a trademark of Coyote Point Systems Incorporated. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

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.

Table of Contents

Introduction	4
Web Mail OWA Topology	4
Required Equalizer Hardware and Software	5
Exchange/OWA Configuration Notes	5
Equalizer OWA Server Farm Configuration	6
Setup Equalizer's Network Interfaces	6
Change the Default Gateway on the Servers	8
Test Equalizer and Server Connectivity	8
Create the Virtual Cluster and Servers (Version 7)	9
Create the Virtual Cluster and Servers (Version 8)	11
Final Steps	14
Enabling Forms-Based Authentication and SSL Offloading in OWA	15
Adding a Second Equalizer for High Availability	16

Introduction

Microsoft Outlook Web Access (OWA) provides HTTP and HTTPS access to Microsoft Exchange Server resources, such as Web Mail, to Internet and Intranet clients via a web browser. OWA provides an environment that looks much like the Exchange Server Client.

To use OWA, a user logs in to an OWA server, which then fetches the user's mail, calendar and other resources from the Exchange Server running on another machine; the OWA system then displays the user's resources (such as mailboxes, calendars and folders) in the client browser, as shown above.

As the user performs various Outlook tasks in their browser, these actions are sent as requests to the OWA server, which then contacts the back-end Exchange servers to perform the tasks on behalf of the user and fulfill the request. Once the back-end server completes the requested tasks, it communicates the results to the OWA server, which sends them back to the client browser.

Web Mail OWA Topology

The OWA topology most applicable to load balancing, and the one we're using for our example configuration, is shown in the diagram below:

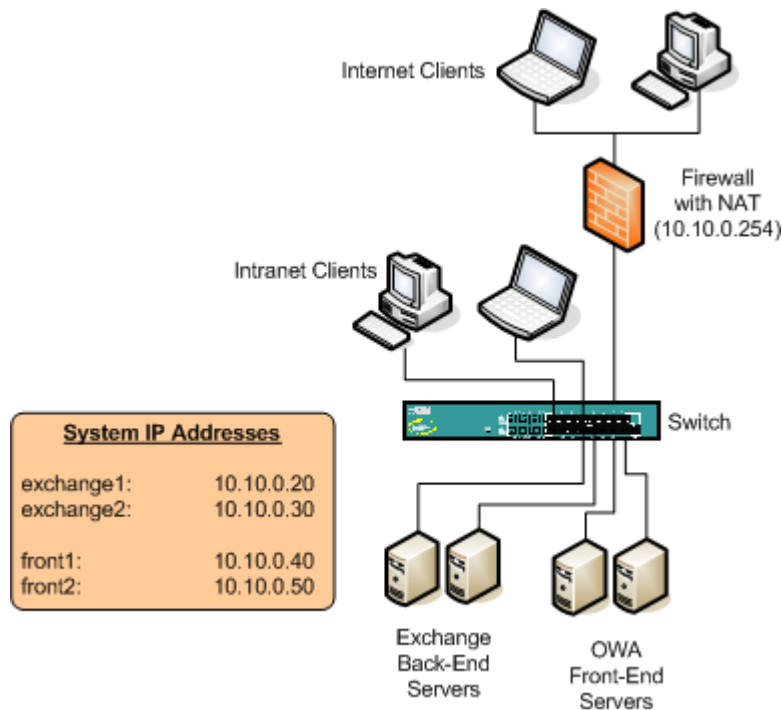


Figure 1 Web Farm with a Firewall OWA Topology

Both Intranet and Internet clients log into the OWA servers using a browser. The OWA servers connect to the Exchange servers to retrieve the user's Outlook configuration, and display the OWA client back in the browser.

Required Equalizer Hardware and Software

The implementation described in this document requires the following hardware and software in addition to your current network configuration:

- **Equalizer Hardware Model E350GX, E450GX, or E350GX**
- **Equalizer Software Version 7.2.4 or Version 8**

*We assume that Equalizer is already licensed for use. If you see a licensing error when you open the administrative interface, please see Chapter 5 of the *Installation and Administration Guide* for instructions.*

- **SSL Certificate for the cluster IP/name**

If you have an existing certificate in use in an existing OWA/Exchange configuration, you may be able to use the same certificate for the cluster, *as long as the certificate does not contain an IP address or URI that conflicts with the cluster IP/URI. In other words, if a specific, non-wildcard URI or IP address is contained in the certificate, it MUST match the URI or IP address of the Equalizer cluster, or it will not be accepted by the client browser.* For more information on using client certificates with Equalizer, log into the Support Portal (support.coyotepoint.com) and download the document “Using Certificates for HTTPS Clusters” from the Device Manuals section.

Exchange/OWA Configuration Notes

If not already installed, **install and configure Exchange Server 2003** on the Exchange Back-End Servers and OWA Front-End Servers, and configure them according to the Microsoft Exchange 2003 documentation, using the configuration diagram in as a guide. Also note the following:

- **This configuration uses 2 Back-End Servers running Exchange Server 2003 R2 and 2 Front-End Servers running Exchange Server 2003 R2 with OWA enabled.** If your configuration has more than 2 OWA servers, simply plug them into Equalizer’s internal ports and add them as servers in the virtual cluster on Equalizer.
- **All Exchange/OWA user accounts should be enabled to log in to all front-end servers.** This is important because, once we add Equalizer to the configuration, Equalizer can then decide which front-end server is the best choice for the client session.
- **Do not enable SSL on either the front-end or back-end servers.** Exchange can be configured to use SSL between clients and the OWA front-end servers, and the back-end servers can be configured to require SSL connections. One of the major advantages of using a hardware load balancer like Equalizer is that you can offload all SSL traffic and processing to the Equalizer, which will then communicate to the front-end servers using HTTP. (Equalizer must be running version 7.2.4 or later to offload SSL from OWA).
- In this procedure, we will configure Equalizer to accept SSL connections, and insert a special header into requests that tells OWA/Exchange that the SSL connection was terminated at Equalizer. When OWA/Exchange receives a request containing the special header, it knows that its response to the request must be in HTTPS.
- **Forms-Based Authentication can be used with Equalizer.** Forms-Based Authentication is an Exchange option that provides persistent connections through the use of cookies. It’s purpose is to allow session data to persist across connections, as well as to allow the Exchange servers to terminate idle client sessions and free server resources for other connections. Equalizer also provides connection persistence using cookies, and we recommend that you enable *both* Forms-Based Authentication on Exchange and cluster persistence on Equalizer. At a minimum, you *must* enable persistence when you setup the cluster on Equalizer in Step . Forms-Based Authentication can then be set up after your cluster is working without it. See the section “Enabling Forms-Based Authentication and SSL Offloading in OWA” on page 15 for more information.

See the Exchange Server documentation for complete instructions on performing the above tasks.

Equalizer OWA Server Farm Configuration

The following diagram illustrates how Equalizer can be dropped into an existing OWA Server Farm configuration:

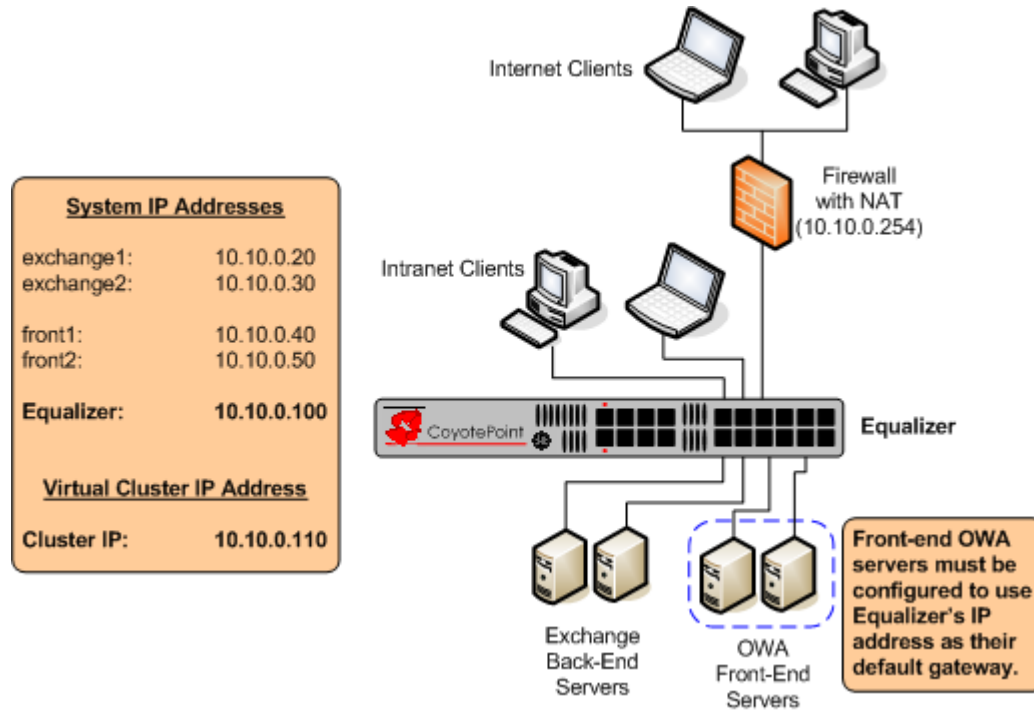


Figure 2 Equalizer OWA Server Farm Configuration

In the above configuration, we define a virtual cluster on Equalizer, and tell all of our clients to use Equalizer's cluster IP to get their mail. Equalizer basically acts like a proxy server between the clients and the OWA Front-End Servers for the purpose of balancing the load between the Front-Ends. Each of the front-end servers in the cluster are configured to use Equalizer as their default gateway, so that all responses are routed through Equalizer.

As you can see, the introduction of Equalizer into the network requires only two private IP addresses and a single configuration change on the servers. No other changes to the network infrastructure are necessary.

We recommend that you setup your Equalizer/OWA server farm in a staged manner, as shown in this procedure. By testing each stage as we go along, we can eliminate basic configuration errors as they occur, rather than debugging a potential mix of problems after the configuration is complete. A staged implementation also allows existing installations to continue to provide normal Exchange services to current OWA users while Equalizer is configured.

Setup Equalizer's Network Interfaces

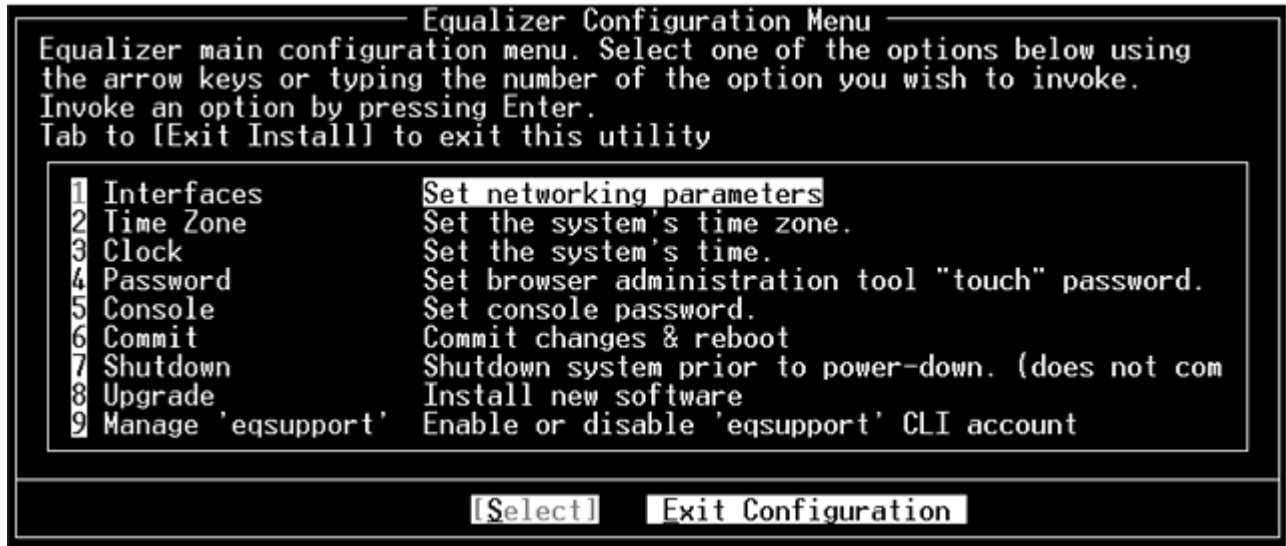
Connect Equalizer using the supplied serial cable to another system running terminal emulation software. On Windows systems, use a terminal emulator such as HyperTerminal or Tera Term Pro. TeraTerm Pro is freely available at:

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

The emulator you use must be set for **9600 baud, 8 data bits, no parity, one stop bit, and VT100 terminal emulation.**

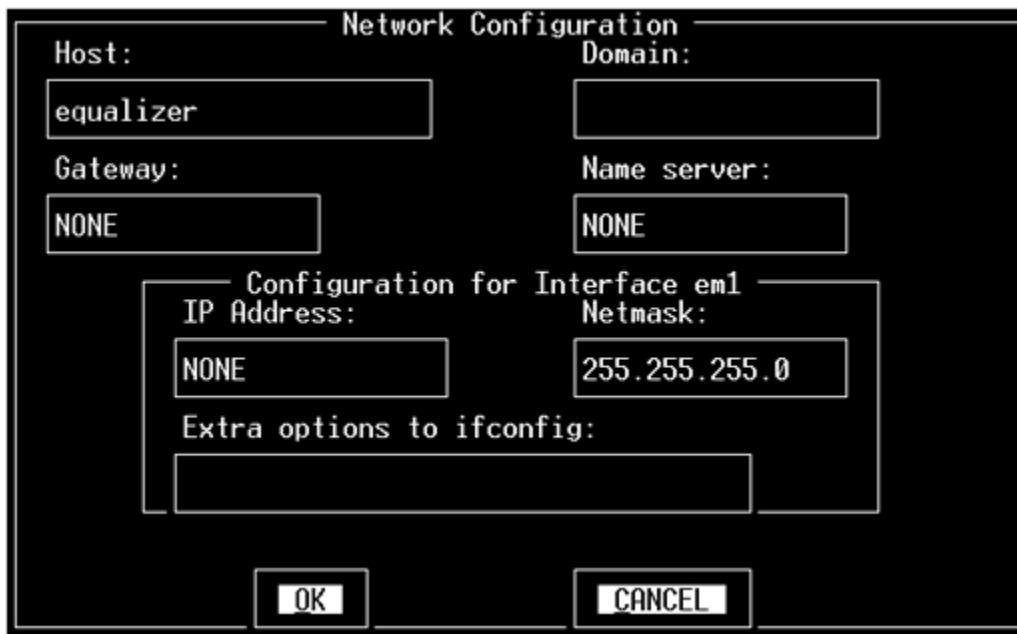
1. Power Equalizer on and when the boot process is complete, press **Enter** on the terminal keyboard to display the login prompt. Type **eqadmin** and press **Enter**. When the password prompt appears, enter the **eqadmin** password

(default **equalizer**) and press **Enter**. Equalizer automatically launches the **Equalizer Configuration Utility**, a character-based interface for setting and changing Equalizer configuration parameters.



Note: In Version 8.5 and later releases, an additional option (not used in this procedure) is listed at the bottom of the above menu.

2. In the Equalizer Configuration Menu window, select option 1, **Interfaces**, and press **Enter**. Equalizer displays the **Configure network interfaces** window.
3. Select the **external ethernet interface** and press **Enter**. The Network Configuration window is displayed.

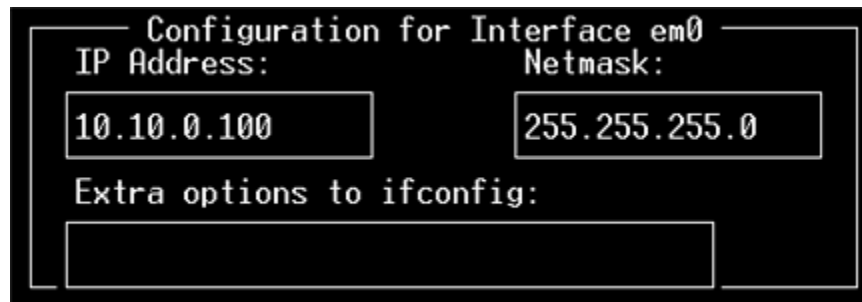


- In the **Host** field (required), enter the name for the Equalizer on your network. This can be the system node name (such as “eq-ext”), or the fully qualified domain name (FQDN, such as “eq-ext.customer.com”). If you supply the FQDN in the **Host** field, the **Domain** field will automatically be filled in using the domain of the FQDN.

- In the **Domain** field, enter the domain name for the Equalizer. (For example, for the fully qualified domain name, `eq-ext.customer.com`, you would enter “customer.com” in the **Domain** field.
- In the **Gateway** field, enter the IP address of the router on the external network; in our example configuration, this is the address of the firewall (**10.10.0.254**).
- In the **Name Server** field, enter the IP address of the domain name server that Equalizer will use; in our example configuration, this is the address of the firewall (**10.10.0.254**). To indicate that no name server is available, enter **0.0.0.0**.
- Leave the **IP address** field for the external interface set to **NONE**.

Tab to **OK** and press **Enter** to go back to the **Configure Network Interfaces** screen.

4. Select **internal ethernet interface** and press **Enter**:



- In the **IP Address** field enter **10.10.0.100**.
- In the **Netmask** field enter **255.255.255.0**.

Select **OK** and press **Enter** to go back to the **Configure Network Interfaces** screen.

5. Select **Back** and press **Enter** to return to the **Equalizer Configuration Menu**.
6. Select option 6, **Commit**; then press **Enter**. Equalizer commits your changes and automatically reboots.

Change the Default Gateway on the Servers

Log into *each* front-end OWA server, and change the default gateway for the server to Equalizer’s IP address.

To do this, open **Start > Network Connections**, right-click the appropriate network interface and select **Properties**. Select **Internet Protocol (TCP/IP)** from the list and click **Properties**. Change the default gateway to **10.10.0.100**, and click **OK**; or, if DHCP is enabled, click **Advanced**, add a new gateway entry, and click **OK** twice to close.

Test Equalizer and Server Connectivity

1. Log into a client on the internal network and each server in the cluster, and use the **ping** command with Equalizer’s internal address to see if Equalizer responds:

```
ping 10.10.0.100
```
2. Log into Equalizer over the serial interface and ping each server in the cluster.
3. If DNS is configured, log into Equalizer over the serial interface as *root* and **ping** a host on the Internet (e.g., `www.coyotepoint.com`) from the Equalizer command line to ensure that DNS and the defined gateway are functioning properly.

If any of these tests fail, go back to Step 3 on page 7 and check your network configuration. [Note that more complex configurations than our example may require static routes on the servers, clients, or Equalizer.]

Create the Virtual Cluster and Servers (Version 7)

Follow the procedures in this section if your Equalizer is running any release of Version 7 of the Equalizer software.

Create the Virtual Cluster (Version 7)

- Using your browser, open either of Equalizer's administrative URIs:

```
http://10.10.0.100
https://10.10.0.100
```

You should see Equalizer's login screen in your browser.

- Log in to the Administrative Interface as user *touch* or another user with the **add/del** permission on global parameters.
- Select **Add > Virtual Cluster** from the main menu at the top of the right frame of the Administrative Interface. The **add cluster** screen is displayed:

The screenshot shows the 'add cluster' configuration window. The fields and their values are as follows:

- cluster name:
- protocol:
- ip:
- port:
- policy:
- responsiveness:
- cookie age:
- cookie domain:
- cookie path:
- ACV probe:
- ACV response:
- server agent port:

The 'flags' section contains the following checkboxes:

- advanced:
- disable:
- ignore case:
- server_agent:
- spoop:
- persist:
- once only:

The 'cookie_flags' section contains the following dropdown menu:

- cookie_flags:

At the bottom of the window are two buttons: **commit** and **cancel**.

- Set the following cluster parameters to the values shown below:

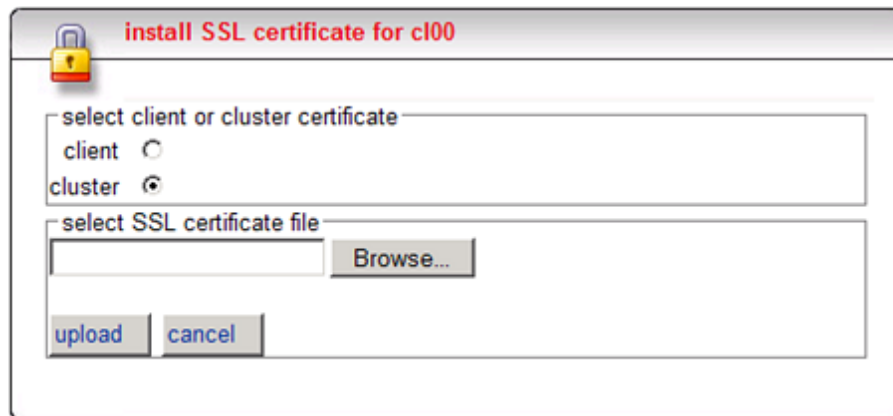
```
cluster name: OWA
protocol: HTTPS [or, if you are not enabling SSL Offloading, use HTTP]
ip: 10.10.0.110
policy: adaptive
```

5. Disable the **spoof** flag, which tells Equalizer to use its own IP address as the source IP in all packets it forwards to the servers in the cluster.
6. To enable SSL offloading, click on the **advanced** flag. Find the text box labelled **custom header** and enter the following value into the text box:

Front-End-Https: On

Doing this tells Equalizer to not only terminate the SSL connection, but to also insert the above text as an HTTP header into the client request. Equalizer will use HTTP to communicate with the OWA front-end servers, which will forward the requests to the Exchange Back-End Servers. This special header tells the back-end servers to reply using HTTPS.

7. Scroll to the bottom of the screen and select the **commit** button to create the cluster.
8. **Load the SSL server certificate for the cluster.** [If you are *not* enabling SSL Offloading (i.e., your cluster protocol is HTTP), skip this step and go to Step]
 - a. From the cluster screen, select **menu > Manage SSL Certificates**. The **install SSL certificate** screen is displayed.



- b. Make sure the **cluster** radio button is enabled, and then select **Browse** to find the file containing the cluster certificate on your local system.
- c. Select the **upload** button to upload the certificate to Equalizer. When prompted, enter the certificate's password and click **submit**. If successful, you are returned to the **install SSL certificate** screen, which should now display the certificate details.

Create the Cluster Servers (Version 7)

1. In the left frame, click on the name of the cluster you just created. When the **cluster** screen is displayed, select **menu > add server** to display the **add server** screen.

2. Set the following server parameters to the values shown below:


```
server name: front1
ip: 10.10.0.40
```
3. Click **commit** to create the server and return to the **cluster** screen. The server (**front1**) should now be displayed under the cluster name in the left frame.
4. Select **menu > add server** to display the **add server** screen again.
5. Set the following server parameters to the values shown below:


```
server name: front2
ip: 10.10.0.50
```
6. Click **commit** to create the server and return to the **cluster** screen. The server (**front2**) should now be displayed under the cluster name in the left frame.

Create the Virtual Cluster and Servers (Version 8)

Follow the procedures in this section if your Equalizer is running any release of Version 8 of the Equalizer software.

Create the Virtual Cluster (Version 8)

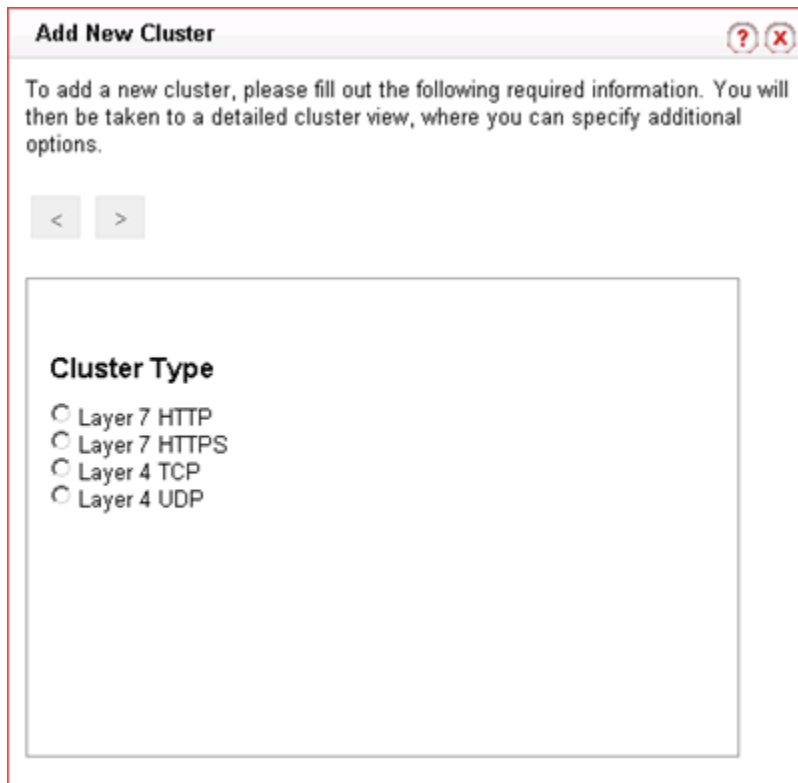
1. Using your browser, open either of Equalizer's administrative URIs:

```
http://10.10.0.100
https://10.10.0.100
```

You should see Equalizer's login screen in your browser.

2. Log in to the Administrative Interface as user *touch* or another user login with the **add/del** permission on global parameters.

3. In the left frame, right-click on Equalizer and select **Add Cluster** from the popup menu. The **Add New Cluster** dialog is displayed:



4. If you are enabling SSL offloading, select Layer 7 HTTPS; otherwise, select layer 7 HTTP. Click next (>) at the top of the dialog.
5. Type in the following cluster parameters:
Cluster Name: OWA
Cluster IP Address: 10.10.0.110
Click next (>) and then **commit**. The cluster is created and appears in the left frame. The **Configuration** tabs for the cluster open in the right frame.
6. Disable the **spoof** flag (this tells Equalizer to use its own IP address as the source IP in all packets it forwards to the servers in the cluster). Click **commit**.
7. Open the **LB Algorithm** tab, and select **adaptive** in the **policy** drop down box. Click **commit**.
8. To enable SSL offloading, open the **Networking** tab and enter the following value into the **custom header** text box:

Front-End-Https: On

Doing this tells Equalizer to not only terminate the SSL connection, but to also insert the above text as an HTTP header into the client request. Equalizer will use HTTP to communicate with the OWA front-end servers, which will forward the requests to the Exchange Back-End Servers. This special header tells the back-end servers to reply using HTTPS.

Click **commit**.

9. If you are *not* enabling SSL Offloading (i.e., you selected **Layer 7 HTTP** in Step 4 on page 12), skip this step and continue with the next section, “Create the Cluster Servers (Version 8)” on page 14. If you selected **Layer 7 HTTPS** in Step 4 on page 12, do the following to load a certificate for the cluster:

- a. Open the **Security** tab.

select client or cluster certificate

For client verification, upload a single client certificate to authenticate all clients. For server verification, upload a single server certificate for the cluster.

client

cluster

select SSL certificate file

The certificate file must be in PEM (.pem) or PKCS12 (.pfx) format, and must contain the private key and the entire certificate chain.

- b. Make sure the **cluster** radio button is enabled, and then select **Browse** to find the file containing the cluster certificate on your local system.
- c. Select the **upload** button to upload the certificate to Equalizer. When prompted, enter the certificate’s password and click **submit**. The tab should now display the certificate details in a separate field at the bottom of the right frame.

cluster SSL certificate details for cl01

certificate 1

serial number	8B8028F2029CF778
keylength	1024
issuer	/C=US/ST=New York/L=Millertc
subject	/C=US/ST=New York/L=Millertc
valid from	May 2 20:21:17 2007 GMT
valid till	May 1 20:21:17 2010 GMT

If there is more than one certificate in the certificate chain contained in the uploaded file, then the interface will display all the certificates in the chain.

Create the Cluster Servers (Version 8)

1. In the left frame, right-click on the name of the cluster you created above and select **Add Server** from the popup menu.



Add New Server ? X

In order to add a new server, please fill out the following required information.

< >

Server Parameters

Server Name: sv02

Server IP Address:

Server Port: 80

Associate with Virtual Machine:

2. Set the following server parameters to the values shown below:

Server Name: front1
Server IP Address: 10.10.0.40

Click next (>) and then **commit**. The server is created and appears in the left frame. The **Configuration** tabs for the server open in the right frame.

3. In the left frame, right-click on the name of the cluster again and select **Add Server** from the popup menu
4. Set the following server parameters to the values shown below:

Server Name: front2
Server IP Address: 10.10.0.50

Click next (>) and then **commit**. The server is created and appears in the left frame. The **Configuration** tabs for the server open in the right frame.

Final Steps

1. **Test the cluster.** Try accessing the Equalizer cluster IP (**10.10.0.110**); you should be asked to accept the cluster certificate, and then the OWA login prompt should be displayed. You should now be able to log into OWA and display the OWA desktop (see on page).
2. **Update DNS so that the mail URL used by your user community points to the virtual cluster IP 10.10.0.110.** Then, test accessing the cluster IP from an external client.

Enabling Forms-Based Authentication and SSL Offloading in OWA

There are two pieces to enabling Forms-Based Authentication (FBA) when OWA is behind an Equalizer HTTPS cluster (that is, when Equalizer is offloading SSL processing). See “*Enabling Forms Based Authentication*” and “*How to Enable Forms-Based Authentication When Using SSL Offloading*” in the Exchange Server 2003 documentation at the links below:

<http://support.microsoft.com/kb/830827/>

<http://technet.microsoft.com/en-us/library/d7a6c54d-bb5d-443d-9759-d552695c5176.aspx>

The basic procedure is included here for your convenience:

1. Follow these steps on *both* of the *front-end* OWA servers *only*:
 - 1a. Start the **Exchange System Manager**.
 - 1a. If administrative groups are enabled, expand **Administrative Groups**.
 - 1b. Expand **Servers**, and then expand one of the front-end servers.
 - 1c. Expand **Protocols**, expand **HTTP**, right-click **Exchange Virtual Server**, and then click **Properties**.
 - 1d. Click the **Settings** tab, and then click to enable the **Enable Forms Based Authentication** check box.
 - 1e. In the **Compression** list, click the level of compression that you want.
 - 1f. Click **OK**.
2. Edit the registry on *both* of the OWA *front-end* servers *only*, and add the **SSLOffloaded** keyword. Select **Start > Run** and enter the following command:

```
regedit
```

Click **OK**.

- 2a. Locate the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
```

- 2b. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
 - 2c. In the details pane, name the new value **SSLOffloaded**.
 - 2d. Right-click the **SSLOffloaded** DWORD value, and then click **Modify**.
 - 2e. In **Edit DWORD Value**, under **Base**, click **Decimal**.
 - 2f. In the **Value Data** box, enter the value **1**.
 - 2g. Click **OK**.
3. Restart the IIS server on the *front-end* servers, by opening a **Command Prompt** window and entering the following command:

```
iisreset
```

4. Do the following on *both* of your *back-end* Exchange servers *only*:
 - 4a. Start the **Exchange System Manager**.
 - 4b. If administrative groups are enabled, expand **Administrative Groups**.
 - 4c. Expand **Servers**, and then expand one of the back-end servers.
 - 4d. Expand **Protocols**, expand **HTTP**, and then expand **Exchange Virtual Server**.
 - 4e. Right-click the **Exchange** virtual directory that appears under the **Exchange Virtual Server** container, and then click **Properties**.
 - 4f. Click the **Access** tab, and then click **Authentication**.
 - 4g. If it is not already selected, click to enable the **Basic authentication** check box.

- 4h. Remove any existing text from the **Default Domain** text box, and enter a backslash (\) for the **Default Domain**. Only the backslash should appear in the text box.
- 4i. Click **OK** two times to close the property windows.

Once you complete the above steps, you should be able to access OWA from your clients with Forms-Based Authentication and SSL Offloading enabled.

See the Microsoft Exchange Server documentation for more information on configuring and using Forms-Based Authentication and SSL Offloading in a front-end/back-end server configuration.

Adding a Second Equalizer for High Availability

Adding a second backup Equalizer provides high availability in the event that your primary Equalizer becomes unresponsive. The backup Equalizer continually monitors the health of the primary Equalizer, and if the primary Equalizer does not respond to health checks, the backup Equalizer takes over the Cluster IP and begins processing client requests.

The diagram below shows how simple it is to insert a backup Equalizer into the configuration shown in Figure 2.

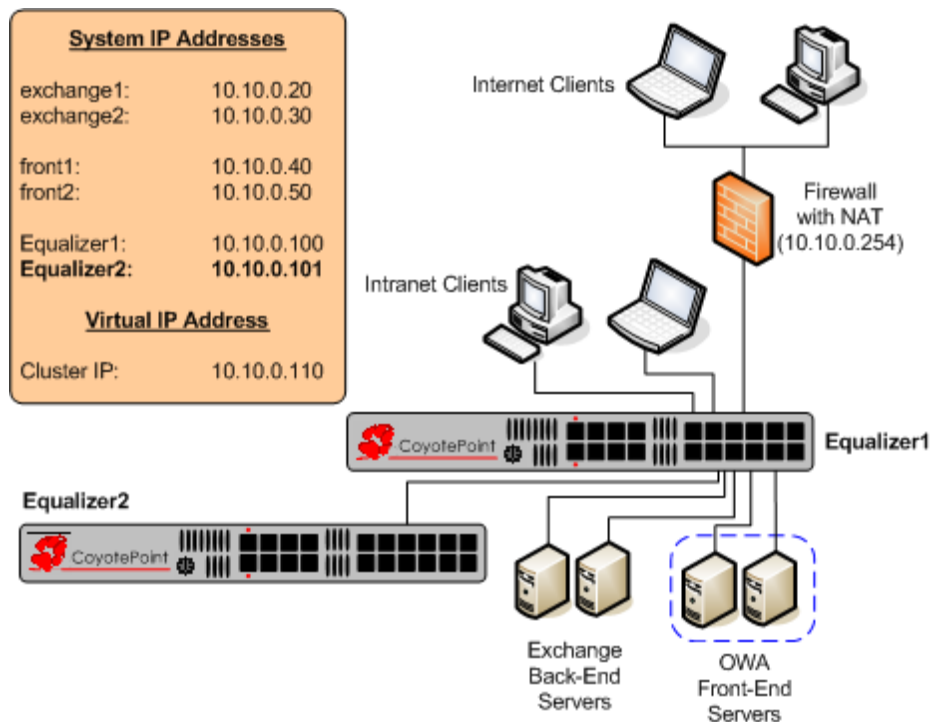


Figure 3 OWA Failover Configuration

Chapter 5 of the *Installation and Administration Guide* (included with your Equalizer, and also available from the Administrative Interface's **Help** menu in the latest versions) contains complete instructions for failover configuration. You can also pick up a copy from the Device Manuals section of the Support Portal.