



**Alteon Application Switch  
And  
Microsoft Exchange 2010  
Integration Guide**

**Version - 1.05**

**Products:**

**Alteon Application Switch**

**Software:** Alteon v.27.0

# Microsoft Exchange 2010

## Contents

Microsoft Exchange 2010 High Availability and Acceleration with Radware Application Delivery Solution .....	3
Microsoft Exchange 2010 Overview.....	3
Radware Alteon Overview.....	3
Exchange 2010 Definitions.....	4
Understanding Load Balancing in Exchange 2010.....	5
Alteon and Microsoft Exchange 2010 Server Architecture .....	6
Diagram 1.0 - Alteon and Microsoft Exchange 2010 Reference Architecture .....	6
Primary Front-End Alteon Configuration .....	7
Network configuration .....	7
addr 192.168.1.254 .....	7
VRRP Configuration .....	8
Compression Configuration .....	8
Caching Configuration.....	8
SSL Configuration .....	8
Sync Configuration .....	9
SLB Configuration .....	9
Nat Configuration .....	9
Real Servers Configuration .....	9
Group Configuration .....	10
Virt Configuration.....	10
Network configuration .....	11
VRRP Configuration .....	12
Appendices .....	13
Appendix 1 – SSL Configuration for CAS servers .....	13
Appendix 2 – Exchange CAS Array Configuration .....	14
Appendix 3 – RFC Client Access.....	15
Appendix 4 – POP3 and IMAP4.....	17
Appendix 4 – Alteon VA deployment.....	20

## **Microsoft Exchange 2010 High Availability and Acceleration with Radware Application Delivery Solution**

Radware's Alteon application Switches and Microsoft Exchange 2010 joint solution is designed to provide a highly scalable and highly available unified messaging and communication infrastructure, with fastest response time.. By deploying these two best of breed subsystems, end users can benefit from a significantly improved Quality of Experience.

Using advanced health monitoring of each of the client access servers, Radware's Alteon application switches can validate the availability and response time of those resources, as well as deliver seamless load balancing, redundancy and persistency features. Furthermore, Radware's Alteon provides service acceleration through compression, caching and SSL termination to the Exchange users, offloading critical resources from the CAS servers, enabling smaller CAS arrays and thus lower CAPEX and OPEX to the organization.

## **Microsoft Exchange 2010 Overview**

Now, more than ever, your organization requires cost-effective and flexible communication tools. With Microsoft Exchange Server 2010 you can achieve new levels of reliability and performance with features that simplify your administration, help protect your communications, and delight your users by meeting their demands for greater mobility.

Microsoft Exchange Server, the cornerstone of Microsoft's Unified Communications solution, is a flexible and reliable messaging platform that can help you lower your messaging costs by 50-80%, increase productivity with anywhere access to business communications, and safeguard your business with protection and compliance capabilities that help you manage risk.

For more information visit Microsoft Exchange 2010 web page:  
<http://www.microsoft.com/exchange/en-us/overview.aspx>

## **Radware Alteon Overview**

Alteon Application Switch provides breakthrough performance, advanced application acceleration capabilities and on demand scalability needed to effectively meet contemporary network and business needs. Specifically designed for the majority of enterprises and carriers that operate in dynamic, ever-changing environments and face diverse requirements, the Alteon Application Switch provides the extendable throughput they need from 0 to 80Gbps for unparalleled scalability, business availability and performance.

For more information visit Radware Alteon web page:  
<http://www.radware.com/Products/ApplicationDelivery/Alteon/default.aspx>

## **Exchange 2010 Definitions**

### ***Microsoft Outlook***

Microsoft Outlook is a personal information manager from Microsoft. It can be used as a stand-alone application, or can work with Microsoft Exchange Server and Microsoft Office SharePoint Server for multiple users in an organization, such as shared mailboxes and calendars, Exchange public folders, SharePoint lists and meeting schedules. There are third-party add-on applications that integrate Outlook with devices such as BlackBerry mobile phones and with other software like Office & Skype internet communication. Developers can also create their own custom software that works with Outlook and Office components using Microsoft Visual Studio. In addition, Windows Mobile devices can synchronize almost all Outlook data to Outlook Mobile.

### ***Outlook Anywhere***

Outlook Anywhere utilizes the RPC Proxy component in Windows to proxy RPC calls to the RPC Client Access Service and Exchange Address Book Service.

### ***Outlook Web App (OWA)***

Outlook Web App is a webmail service of Microsoft Exchange Server 5.0 and later. The web interface of Outlook Web App resembles the interface in Microsoft Outlook. Outlook Web App comes as a part of Microsoft Exchange Server.

Outlook Web App lets you access your e-mail from any Web browser. Outlook Web App (known as Outlook Web Access in earlier versions of Microsoft Exchange) has been redesigned in Exchange 2010. Features such as Chat, Text Messaging, mobile phone integration, and Conversation View provide an enhanced user experience from any computer that has a Web browser. In Exchange Server 2010, these features can be accessed from an expanded set of Web browsers including versions of Internet Explorer later than 6.0, Firefox, Safari, and Google's Chrome.

### ***Exchange ActiveSync (EAS)***

Exchange ActiveSync is used by mobile devices to synchronize mailbox content with an Exchange server 2010. You can synchronize e-mail, contacts, calendar information, and tasks.

If you use a phone that has Windows Mobile 5.0 with the Messaging Security and Feature Pack (MSFP) installed or a later version, your mobile phone will support Direct Push. Direct Push technology is built into Exchange ActiveSync and keeps a mobile phone continuously synchronized with an Exchange mailbox.

## ***Exchange Web Services (EWS)***

Exchange Web Services is a web services application programming interface (API) that can be used by 3rd party applications to access mailbox data. It is also used by various Microsoft produced applications and devices for integration with Exchange, for example Outlook 2007 and later, Entourage 2008 for Macintosh (Web Services Edition), Office Communicator, and the Office Communicator Phone.

## ***Exchange Control Panel (ECP)***

Exchange Control Panel - Administrators can use the Exchange Control Panel for Outlook Web App to manage some on-premises tasks. The following is a list of the administrative features available:

- Text messaging integration
- Voice messaging integration
- Multiple mailbox search
- Additional proxy addresses for mailboxes
- Moderation and approval for distribution list submission

In addition, users have self-service capabilities in that they can perform administrative tasks via the Exchange Control Panel. The ECP enables users to perform common tasks without having to call the help desk.

## ***Remote Powershell***

Remote Powershell is the administrative interface that enables you to manage your Microsoft Exchange Server 2010 organization from the command line.

## **Understanding Load Balancing in Exchange 2010**

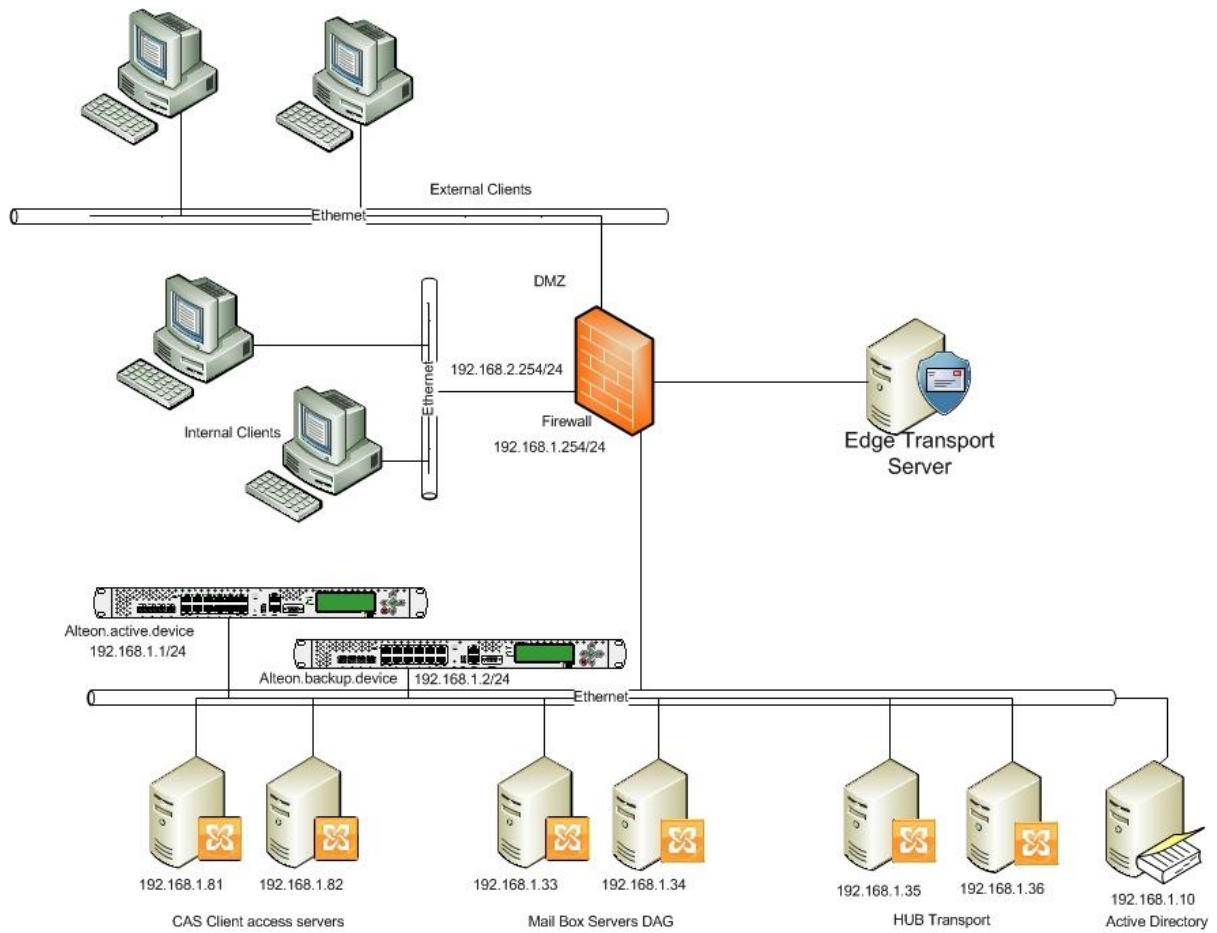
Load balancing is a way to manage which of your servers receive traffic. Load balancing provides failover redundancy to ensure your users continue to receive Exchange service in case of computer failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name for your clients.

**Note:** For more detailed information please refer to:

<http://technet.microsoft.com/en-us/library/ff625247.aspx>

<http://technet.microsoft.com/en-us/library/ff625248.aspx>

# Alteon and Microsoft Exchange 2010 Server Architecture



**Diagram 1.0 - Alteon and Microsoft Exchange 2010 Reference Architecture**

## Primary Front-End Alteon Configuration

### Network configuration

```
/c/port 1
  dis
/c/port 2
  pvid 205
/c/l2/vlan 1
  learn ena
  def 1
/c/l2/vlan 205
  ena
  name "TAG.192.168.1.x"
  learn ena
  def 2
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 205
/c/l3/if 2
  ena
  ipver v4
  addr 192.168.1.2
  vlan 205
/c/l3/gw 1
  ena
  ipver v4
  addr 192.168.1.254
```

## **VRRP Configuration**

```
/c/l3/vrrp/on
/c/l3/vrrp/vr 2
  ena
  ipver v4
  vrid 2
  if 2
  prio 200
  addr 192.168.1.1
  share dis
/c/l3/vrrp/vr 3
  ena
  ipver v4
  vrid 3
  if 2
  prio 200
  addr 192.168.1.209
```

## **Compression Configuration**

```
/c/slb/accel/compress
  on
/c/slb/accel/compress/comppol 2
  name "comp1"
  minsize 1
  ena
```

## **Caching Configuration**

```
/c/slb/accel/caching
  on
/c/slb/accel/caching/cachepol 1
  name "cache"
  ena
```

## **SSL Configuration**

```
/c/slb/ssl/certs/group 1
  name "cert1"
```



```
        type intermca
/c/slb/ssl
    on
/c/slb/ssl/sslpol 7
    name "Exchange.pol"
    ena
```

### **Sync Configuration**

```
/c/slb/sync
    prios d
    certs e
    state e
/c/slb/sync/peer 1
    ena
    addr 192.168.1.3
```

### **SLB Configuration**

```
/c/slb
    on
/c/slb/adv
    direct ena
/c/slb/adv
    submac "ena"
```

### ***Nat Configuration***

```
/c/slb/pip/type port
/c/slb/pip/add 192.168.1.99 2
```

### ***Real Servers Configuration***

```
/c/slb/real 21
    ena
    ipver v4
    rip 192.168.1.81
    name "Exchange.CAS.1"
/c/slb/real 22
    ena
    ipver v4
    rip 192.168.1.82
```

```
name "Exchange.CAS.2"
```

### ***Group Configuration***

```
/c/slb/group 32
  ipver v4
  metric phash 255.255.255.255
  add 21
  add 22
  name "https.group"
/c/slb/group 33
  ipver v4
  metric phash 255.255.255.255
  add 21
  add 22
  name "rpc.group"
/c/slb/group 34
  ipver v4
  metric phash 255.255.255.255
  add 21
  add 22
  name "imap.group"
/c/slb/group 35
  ipver v4
  metric phash 255.255.255.255
  add 21
  add 22
  name "pop3.group"
```

### ***Virt Configuration***

#### ***RPC LB (Client Access and Address Book services)***

The RPC services listen on 2 TCP ports, as defined in the server configuration (see Appendix). Make sure to use the same port numbers in the following service configuration.

```
/c/slb/virt 51
  ena
  ipver v4
  vip 192.168.1.150
  vname "Exchange.cas"
/c/slb/virt 51/service 443 https
```

```

group 32
rport 80
pbind clientip norport
dbind forceproxy
/c/slb/virt 51/service 443 https/http
  comppol 2
/c/slb/virt 51/service 443 https/ssl
  svrcert cert 1
  sslpol 7
/c/slb/virt 51/service 135 basic-slb
  group 33
  pbind clientip norport
/c/slb/virt 51/service 59532 basic-slb
  group 33
  pbind clientip norport
/c/slb/virt 51/service 59531 basic-slb
  group 33
  pbind clientip norport
/c/slb/virt 51/service 143 imap
  group 34
  pbind clientip norport
/c/slb/virt 51/service 110 pop3
  group 35
  pbind clientip norport
/c/slb/virt 51/service 80 http
  action redirect
  group 1
  rport 0
  redirect "https://$HOST/$PATH/"
  dbind ena
/c/sys/access/https/cert WebManagementCert
/c/sys/access/https/https e
Backup Alteon Configuration

```

### **Network configuration**

```

/c/port 2
  pvid 205
/c/l2/vlan 1
  learn ena
  def 1
/c/l2/vlan 205
  ena
  name "205"

```

```
learn ena
def 2
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 205
/c/sys/sshd/ena
/c/sys/sshd/on
/c/l3/if 2
ena
ipver v4
addr 192.168.1.3
vlan 205
/c/l3/gw 1
ena
ipver v4
addr 192.168.1.254
```

### **VRRP Configuration**

```
/c/l3/vrrp/on
/c/l3/vrrp/vr 2
ena
ipver v4
vrid 2
if 2
addr 192.168.1.1
share dis
/c/l3/vrrp/vr 3
ena
ipver v4
vrid 3
if 2
addr 192.168.1.209
```

## **Appendices**

### **Appendix 1 – SSL Configuration for CAS servers**

#### **Exchange SSL Offload Settings**

As a requirement of SSL offload to the Alteon, a minor change needs to be made to the CAS servers. When a SSL connection is terminated on the ADC, all connections from the Alteon to the CAS servers are made via standard http.

Exchange server settings are detailed under <http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx>

## Appendix 2 – Exchange CAS Array Configuration

Another requirement to support hardware load balancing for your CAS servers is the configuration of a CAS array. In its configuration you must create a CAS array through the Exchange Management Shell that groups your CAS servers together. Then make sure the name of your CAS array is a DNS registered name that points to the Alteon load balancer virtual IP.

1. On your domain controller, create a forward lookup entry that maps your Alteon load balancer virtual IP to the fully-qualified domain name that you assign to your CAS array in the next step.
2. Then, create the CAS array with the command "New-ClientAccessArray -Name <NameoftheArray> -FQDN <NameoftheArray.Fully-qualified domain name> -Site <ADSiteName>".
3. For each of the mailbox databases that will be front-ended by your CAS servers, you need to assign the CAS array as the RPC Client Access server setting for each mailbox database. To see a list of all your mailbox database names, use the "Get-MailboxDatabase" command.
4. If you need to find out what each of your Mailbox databases is using as its CAS server, use the command "GET-MailboxDatabase "dbase4" | fl RpcClientAccessServer".
5. Set the CAS server setting for each mailbox database to be the newly created CAS array with the command "Set-MailboxDatabase <database name/id> -RpcClientAccessServer <NameoftheArray.Fully-qualified domain name>".
6. When you initiate a connection from your Exchange user, be sure to specify the CAS array fully-qualified domain name (which is the same as the Alteon load balancer VIP fully-qualified domain name) as the server to which you are connecting. The connection then goes to the Alteon to be load-balanced amongst the CAS servers in your CAS array.

## Appendix 3 – RPC Client Access

With Exchange Server 2010, Outlook clients connect using native MAPI to the new RPC Client Access service, which runs on Client Access servers, rather than directly to Mailbox servers.

**Note:** When you upgrade your organization to Exchange 2010, your clients running Outlook 2007 or later versions will automatically be compatible with the change to RPC Client Access, since they support RPC encryption by default. Outlook 2003 doesn't use RPC encryption, however, and RPC Client Access requires it by default. If you haven't turned off RPC encryption, your users will need to configure Outlook 2003 for RPC encryption or you'll need to use a Group Policy to force Outlook 2003 to use RPC encryption.

**Note:** Because the RPC Client Access Service requires the traffic to be passed to the Client Access servers on a large number of ports, we recommend that you use a firewall to permit only internal networks to access the RPC Client Access virtual server IP address.

### Configuring Static Port Mapping For RPC-Based Services

The static port for the RPC Client Access Service is configured via the registry. The following registry key should be set on each Client Access Server to the value of the port that you wish to use for TCP connections for this service.

```
Key:  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeRPC\Parameters\System  
Value: TCP/IP Port  
Type: DWORD
```

Note that this will only affect connections for “internal” connections via TCP and will not affect Outlook Anywhere connections that take advantage of RPC/HTTP tunneling. Outlook Anywhere connections to the RPC Client Access Service will occur on port 6001 and this is not configurable.

The static ports for the two RPC endpoints maintained by the Exchange Address Book Service are set in the Microsoft.Exchange.AddressBook.Service.Exe.config file which can be found in the bin directory under the Exchange installation path on each Client Access Server. The “RpcTcpPort” value in the configuration file should be set to the value of the port that you wish to use for TCP connections for this service. This port will handle connections for both the Address Book Referral (RFR) interface and the Name Service Provider Interface (NSPI).

N

ote that the values for the “NspiHttpPort” and “RfrHttpPort” configuration options should not be changed as Outlook is configured to use these ports by default. Changing these values may result in unwanted delay when attempting to establish Outlook Anywhere connections.

**Note:** For Exchange 2010 SP1 please refer to:  
<http://social.technet.microsoft.com/wiki/contents/articles/configuring-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>

## RPC Client Access Configuration requirements

Please refer to Microsoft documentation regarding the configuration of the RPC Client Access service and mailboxes for each site. To work with a load balancer, complete the following steps.

1. In the Microsoft Exchange Management Shell, create a new Client Access Array and associate it with the same FQDN that you will be using.

example:

```
New-ClientAccessArray -Name "Internal Client Array" -FQDN outlook.radware.com
```

```
New-ClientAccessArray [-Name <String>] -Fqdn <Fqdn> -Site  
<AdSiteIdParameter> [-Confirm [<SwitchParameter>]] [-DomainController  
<Fqdn>] [-WhatIf [<SwitchParameter>]]  
New-ClientAccessArray -Name "Internal Client Array" -FQDN outlook.radware.com
```

2. You must modify the attributes of any pre-existing mailbox databases to use the new array.

```
Set-MailboxDatabase "Mailbox Database" -RpcClientAccessServer CAS-Array.radware.com
```

**Note:** You can only configure one Client Access Array (one FQDN) per site.

**Note:** In the configuration example below, the static port for the RPC Client Access Service is configured via the registry to port 135. Please see Deployment notes above for instructions on how to configure the registry. In case the default port is changed, make sure to change the port number from 135 to the new static port in all of the following configuration settings.



## Appendix 4 – POP3 and IMAP4

POP3 and IMAP4 enable a variety of clients to connect to the Exchange server. These include Outlook, Outlook Express, and third-party clients such as Eudora or Mozilla Thunderbird.

By default, POP3 and IMAP4 are disabled in Microsoft Exchange Server 2010. To support clients that still rely on these protocols, you must first start the POP3 and IMAP4 services on the Exchange 2010 Client Access server. You must also configure SMTP for your POP3 and IMAP4 clients to send e-mail.

For detailed steps about how to enable the POP3 and IMAP4 services, see Links below:

Enable POP3 in Exchange 2010

<http://technet.microsoft.com/en-us/library/bb124934.aspx>

Enable IMAP4 in Exchange 2010

<http://technet.microsoft.com/en-us/library/bb124489.aspx>

For more information about how to manage POP3 and IMAP4 in Exchange 2010, see Understanding POP3 and IMAP4 on Microsoft TechNet at

<http://technet.microsoft.com/en-us/library/bb124107%28EXCHG.140%29.aspx>

The following section shows how to configure the secure versions of POP3 and IMAP4, known as POP3S and IMAPS.

### IMAP Configuration

By default, the Exchange 2010 IMAP4 service requires encrypted connections. Since Alteon will be terminating the SSL Connection you must first change the default setting on each Client Access server. You can either change the default setting from the Exchange Management Console or the Management Shell.

#### To change the default setting using the Exchange Management Console

1. Expand Server Configuration, then Client Access.
2. In the list of Client Access servers, select a server to which you will be sending IMAP4 traffic.
3. Select the IMAP4 protocol, right-click, and select Properties.
4. On the Authentication tab, change the setting to one of the plain text login methods (Basic or Integrated Windows) as appropriate for your environment and clients.
5. Click OK.
6. Restart the IMAP4 service on that Client Access server.

7. Repeat for each of the Client Access servers to which you will be sending IMAP4 connections.

### **To change the default setting using the Exchange Management Shell**

1. Type one of the following commands, substituting the name of a Client Access server for “**servername**”:

For Basic authentication:

```
Set-ImapSettings -Server "servername" -LoginType PlainTextLogin
```

For Windows Integrated authentication

```
Set-ImapSettings -Server "servername" -LoginType PlainTextAuthentication
```

2. Restart the IMAP4 service on that Client Access server.
3. Repeat for each of the Client Access servers to which you will be sending IMAP4 connections.

### **POP Configuration**

By default, the Exchange 2010 POP service requires encrypted connections. Since Alteon will be terminating the SSL Connection you must first change the default setting on each Client Access server. You can either change the default setting from the Exchange Management Console or the Management Shell.

### **To change the default setting using the Exchange Management Console**

1. Expand Server Configuration, then Client Access.
2. In the list of Client Access servers, select a server to which you will be sending POP3 traffic.
3. Select the POP3 protocol, right-click, and select Properties.
4. On the Authentication tab, change the setting to one of the plain text login methods (Basic or Integrated Windows) as appropriate for your environment and clients.
5. Click OK.
6. Restart the POP3 service on that Client Access server.
7. Repeat for each of the Client Access servers to which you will be sending POP3 connections.

### **To change the default setting using the Exchange Management Shell**

1. Type one of the following commands, substituting the name of a Client Access server for “servername”:

For Basic authentication:

```
Set-PopSettings -Server "servername" -LoginType PlainTextLogin
```

For Windows Integrated authentication

```
Set-PopSettings -Server "servername" -LoginType PlainTextAuthentication
```

2. Restart the POP3 service on that Client Access server.
3. Repeat for each of the Client Access servers to which you will be sending POP3 connections.

## **Appendix 4 – Alteon VA deployment**

Customers can use the Alteon VA as a VMware Virtual Appliance that runs on the server hardware and provides full availability and scalability to the multiple Exchange 2010 virtual machines.

Alteon VA documentation is available at:

<http://www.radware.com/Products/ApplicationDelivery/Alteonva.aspx>

## **Technical Support**

Radware offers technical support for all of its products through the Radware Certainty Support Program. Please refer to your Certainty Support contract, or the Radware Certainty Support Guide available at:

<http://www.radware.com/content/support/supportprogram/default.asp>

For more information, please contact your Radware Sales representative  
or: U.S. and Americas: (866) 234-5763

International: +972(3) 766-8666

© 2008 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks or trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.