How to Deploy Microsoft Exchange Server 2010 in a One-Armed Configuration

Product Versions and Prerequisites

This article applies to the Barracuda Load Balancer ADC version 5.1 and above, with Microsoft® Exchange Server 2010.

For a full list of the prerequisites for this deployment, see Microsoft Exchange Server 2010 Deployment.

In a one-armed configuration, the ports that internal Outlook® clients use to communicate with the Exchange 2010 server using RPC must be preconfigured on both Exchange 2010 and the Barracuda Load Balancer ADC.

If you want to use a single VIP address and single FQDN for your Exchange deployment, you must use a one-armed configuration.

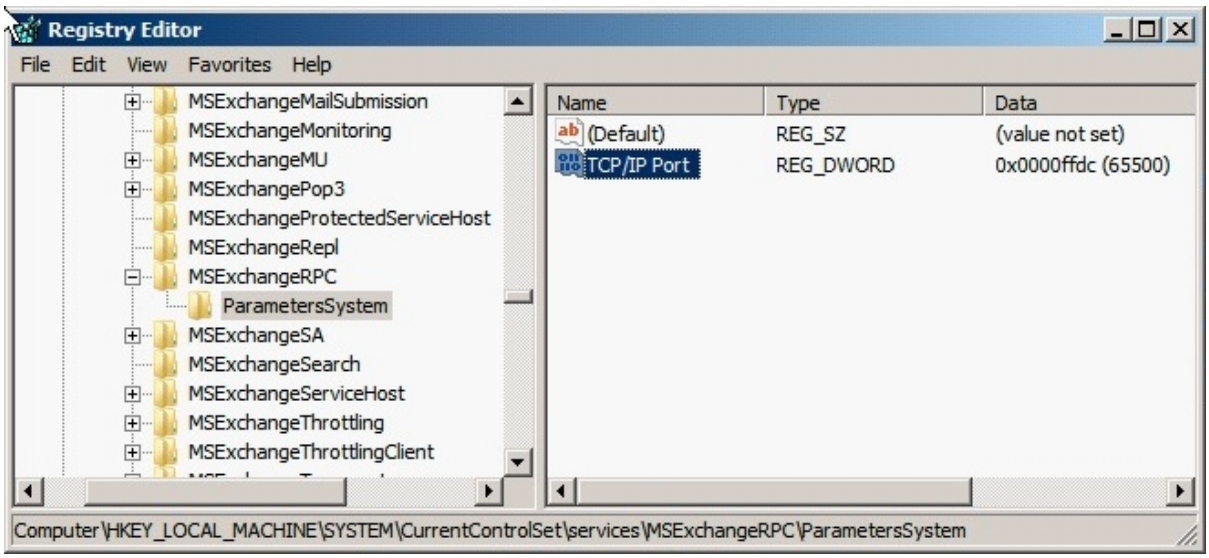
If your Barracuda Load Balancer ADCs are clustered, the configuration between the active and passive units is synchronized; you only need to configure the active Barracuda Load Balancer ADC.

Step 1. Configure Exchange 2010 to Use a Static Port

By default, the Exchange 2010 RPC client dynamically selects a port between 1024 and 65535. To allow for a one-armed deployment, configure Exchange to use a static port instead. For more detailed instructions on configuring Exchange 2010 with static ports and hardware Load Balancer ADCs, see the Microsoft TechNet article Load Balancing Requirements of Exchange Protocols.

On each CAS server, complete the following:

1. Configure the static port in the registry.
    1. Open the Registry Editor by typing regedit in the **Start** menu.
    2. Navigate to `HKEY_LOCL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeRpc\ParametersSystem`.
    3. Add a new **DWORD (32-bit) Value**, and name it `TCP/IP Port`.
    You might need to create the ParametersSystem key prior to adding the DWORD registry value. If prompted, change the Base to `Decimal` and set the value data to `65500` (or a port of your choice between 1024 and 65535):



4. If you have Public Folders in your deployment, repeat these steps to configure the static port in the registry of each server with the mailbox role installed that hosts a Public Folder.

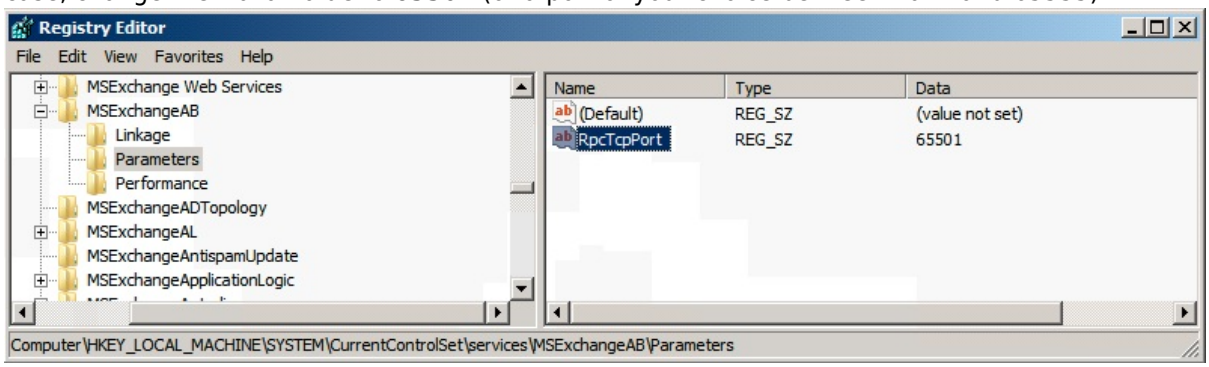
2. Change the port that clients use to connect for directory access. On each CAS server, complete the set of instructions for your Exchange version.

   If you are running Microsoft Exchange 2010 RTM (including RTM Rollup 1 - 4), click here...

   1. In Windows Explorer, navigate to the **Microsoft.exchange.addressbook.service.exe.config** file. This file is located in the **\Bin** folder in the root directory of your Exchange 2010 install.
   2. Open this file in Notepad.
   3. In line 13, change the default value of **0** to **65501** (or a port of your choice within the prior specified range). The entry appears as follows:
      `<add key="RpcTcpPort" value="65501" />`

   If you are running Microsoft Exchange 2010 SP1, click here...

   1. Open the Registry Editor by typing `regedit` in the **Start** menu.
   2. Navigate to `HKEY_LOCL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters`.
   3. Add a new **String Value** (REG_SZ type), and name it `RpcTcpPort` .
      You might need to create the `Parameters` key prior to adding the REG_SZ registry value. In this case, change the **Data** value to `65501` (or a port of your choice between 1024 and 65535).



3. Restart the **Microsoft Exchange Address Book** and the **Microsoft Exchange RPC Client Access** services on all the CAS and Mailbox servers that you modified.
4. To verify that your Client Access servers are using ports 65500 and 65501, open a Windows command prompt and run:
   `netstat -na`
   In the output, look for **TCP** entries marked as **LISTENING** with ports 65500 and 65501. An entry is marked as **LISTENING** for 0.0.0.0:65500 and 0.0.0.0:65501.

Step 2. Configure CAS Services on the Barracuda Load Balancer ADC

On each active Barracuda Load Balancer ADC that handles traffic for CAS services, complete the following steps.

1. Log into the Barracuda Load Balancer ADC, and go to the **BASIC > Services** page.
2. Add all of the services listed in Table 1. For each service, add all the real servers in the CAS array. To add a service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.
   Table 1. CAS Services

Name	Type	IP Address	Port	Session Timeout	SSL Settings	Certificates	Load Balancing	Real Server Port
MAPI-DCOM	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local` **Note**: This service is helpful in cases where there is no port restriction.	135	1200	N/A	N/A	◦ **Persistence Type**: Source IP ◦ **Persistence Time**:1200	135
MAPI-RPC_Client_Access	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local` **Note**: This service is helpful in cases where there is no port restriction.	65500	1200	N/A	N/A	◦ **Persistence Type**: Source IP ◦ **Persistence Time**:1200	65500
MAPI-Global_Address_Book	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local` **Note**: This service is helpful in cases where there is no port restriction.	65501	1200	N/A	N/A	◦ **Persistence Type**: Source IP ◦ **Persistence Time**:1200	65501
Exchange_Web_Services	Instant SSL	VIP address for the FQDN that clients use to access the CAS array for example, `exchange.domain.local` **Note**: ◦ This service is useful when there are port restrictions, and traffic is allowed only for port 443. ◦ To create an HTTP redirect service automatically, you must create an Instant SSL service. Changing an HTTPS service to an Instant SSL service does not automatically create a HTTP redirect service. For more information about Instant SSL, see Instant SSL Service.	Port: 443 HTTP Service Port: 80	1200	◦ **Secure Site Domain** – Enter the domain name of your Exchange server. If the internal and external domain are different, you can use wildcard characters. For example: `*.barracuda.com` ◦ If your Barracuda Load Balancer ADC is running version *5.1.1 and above*, set the **Rewrite Support** option to **On**. For versions *below 5.1.1*, this option is named **Instant SSL**.	Select the certificate that you uploaded when preparing your environment for SSL offloading. See Step 2 in the "Deploying Exchange Services on the Barracuda Load Balancer ADC" section of Microsoft Exchange Server 2010 Deployment.	◦ **Persistence Type**: HTTP Header ◦ **Persistence Time**:1200 ◦ **Header Name**: Authorization	80

3. If you have the Barracuda Load Balancer ADC 640 and above, you can enable **Application Security** for Exchange_Web_Services.
   1. For **Application Security**, select **Enable**.
   2. For **Security Mode**, select the **Passive** mode. It is recommended that you run the service in Passive mode before going active.
   3. From the **Security Policy** list, select **owa2010**. This policy is predefined for all Exchange applications. If you want to edit the policy settings, go to the **SECURITY > Security Policies** page

4. You need to modify the default **owa2010** policy. Go to the **SECURITY > Security Policies** page and select the **owa2010** security policy. In the **Cookie Security** section, set **Tamper Proof Mode** to **None**.

   If you want to use Integrated Windows Authentication with the Exchange service, go to the **Request Limits** section of the security policy settings and increase the **Max Header Value Length** to `800`.

4. If you require any of the protocols in Table 2, add the service for the protocol.
   Table 2. Protocol Services.

Name	Type	IP Address	Port	Real Server Port
IMAP4	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local`	143	143
IMAP4 SSL	TCP Proxy	VIP address for FQDN that resolves to CAS array for example, `exchange.domain.local`	993	993
POP3	TCP Proxy	VIP address for FQDN that resolves to CAS array for example, `exchange.domain.local`	110	110
POP3_SSL	TCP Proxy	VIP address for FQDN that resolves to CAS array for example, `exchange.domain.local`	996	996

Step 3. Configure the Real Servers for Exchange_Web_Services

For Exchange_Web_Services *only*, configure health checks for all of its real servers :

1. On the **BASIC > Services** page, click **Edit** next to the entry of the real server.
2. Scroll to the **Server Monitor** section, and enter the values in the corresponding fields.

Testing Method	Port	Test Target	Test Match	Additional Headers	Status Code	Test Delay
Simple HTTPS	443	/owa/auth/logon.aspx (unless you modified the default path of logon.aspx)	Microsoft Corporation	User-Agent: Barracuda Load Balancer ADC Server Monitor	200	30

3. Click **Save Changes**.

Step 4. Create Content Rules for Exchange_Web_Services

Create content rules for Exchange_Web_Services to maintain persistence for Outlook Web Access, Exchange Control Panel and Exchange Web Services.

1. On the **BASIC > Services** page, add the rules in Table 3. To add a rule, click **Add Content Rule** under Exchange_Web_Services in the left pane. Then enter the values in the corresponding fields.

   Table 3. Content Rules for Exchange_Web_Services

Name	Host Match	URL Match	Persistence Method	Persistence Time	Cookie Name
OWA	*	/owa/*	Cookie Insert	1200	sessionid
ECP	*	/ecp/*	Cookie Insert	1200	sessionid
EWS	*	/ews/*	Cookie Insert	1200	sessionid

2. If you are using Outlook Anywhere (HTTPS only, not RPC over HTTPS), you must also add the following content rule for the Offline Address Book.

Name	Host Match	URL Match	Persistence Method	Persistence Time	Cookie Name
OAB	*	/oab/*	Cookie Insert	1200	sessionid

3. For each of the Content Rules you have configured, you need to add the appropriate Microsoft Exchange server(s). Select each Content Rule and click **Add Server** and specify your Microsoft Exchange server(s).

4. If SNI is enforced on the Microsoft Exchange server(s), then you need to configure the following options. Go to the **BASIC > Services** page and click **Edit** for each affected server.

    1. Change the port on the server to 443.

    2. Navigate to the **SSL** section and set **Server uses SSL** to **On**.

    3. Expand **Settings** and set **Enable SNI** to **Yes**.

Step 5. Configure Hub Transport Services on the Barracuda Load Balancer ADC

On each active Barracuda Load Balancer ADC that handles traffic for Hub Transport Services, configure Hub Transport Services for Exchange 2010.

If your real servers are consolidated with both the CAS and HUB roles installed, add each server for each service that you create. If the Hub Transport role is installed on separate servers (other than those with the CAS role), add only the servers with the Hub role installed. The created services load balance the SMTP traffic to the Hub transport servers for incoming client SMTP connections.

Never configure the Exchange Hub Transport to communicate with other internal Microsoft Exchange Hub Servers via the Barracuda Load Balancer ADC. Only use the service on the Barracuda Load Balancer ADC for client connections or inbound connections from other organizations.

On the **BASIC > Services** page, add the following SMTP service and, optionally, the SMTP-SSL service. To add a service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Name	Type	IP Address	Port	Real Server Port
SMTP	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local`	25	25
(Optional) SMTP-SSL	TCP Proxy	VIP address for the FQDN that resolves to the CAS array for example, `exchange.domain.local`	587	587

Step 6. Configure an HTTP Request Rewrite Rule

To simplify access to the Outlook Web Access site for your users, configure a rewrite rule to add `/owa` to the end of the URL.

1. Go to the **TRAFFIC > Web Translations** page.
2. From the **Service** list, select **Exchange_Web_Services**.

3. In the **HTTP Request Rewrite** section, add the following rule. Click **Add Rule** and enter the values in the corresponding fields.

Rule Name	Sequence number	Action	Old Value	Rewrite Value	Rewrite Condition
OWA	3	Redirect URL	/	/owa	*

4. Click **Save**.

Next Steps

Your installation is complete. You can now test your setup and configure access control to your applications. For instructions, see:

- How to Test the Microsoft Exchange Server 2010 Deployment Configuration
- Access Control

Figures