How to Deploy with Microsoft Office Communications Server

https://campus.barracuda.com/doc/3538969/

This article refers to firmware 3.1 and higher, running on model 340 or higher, and Microsoft Office Communications Server 2007 R2 Enterprise Edition.

- This article assumes you are connected to the Barracuda Load Balancer web interface and have an activated subscription.
- The deployment tasks in this article are based on the example described in the article Microsoft Office Communications Server Deployment Example.
- For a description of supported deployment options, refer to Understanding Microsoft Office Communications Server Deployment.

If your Barracuda Load Balancers are clustered, the configuration between the active and passive systems is synchronized; there is no need to modify any passive Barracuda Load Balancers.

To deploy the Barracuda Load Balancer in an Office Communications Server environment, complete the following tasks:

Deployment Task	Where
Task 1. Modify TCP and UDP Connections Settings.	Do this on all active Barracuda Load Balancers, both internal and external. If your systems are clustered, the passive systems do not need to be configured separately.
Task 2. Configure Enterprise Pool Services.	Do this on the internal-facing Barracuda Load Balancers.
If you have an edge deployment, you must also complete the following tasks:	
Task 3. Configure Internal Edge Services.	Do this on the internal-facing Barracuda Load Balancers.
Task 4. Configure External Edge Services.	Do this on the external-facing Barracuda Load Balancers.
Task 5. Confirm the Configure Edge Server Wizard Setting.	Check this on all Edge Servers.
If you have deployed Director Servers, you must also do the following task:	
Task 6. Configure Director Services.	Do this on the Director Barracuda Load Balancers.
If you have deployed Communicator Web Access, you must also complete the following task:	
Task 7. Configure Communicator Web Access Services.	Do this on the CWA Barracuda Load Balancers.

Task 1. Modify the TCP and UDP Connections Settings

The Barracuda Load Balancer comes configured with default settings that work with most applications. Office Communications Server requires changes to the default advanced IP settings on the Barracuda Load Balancer to ensure it complies with Microsoft's specifications.

To modify the TCP and UDP Connections settings on the **System Settings** page:

1. Go to the **ADVANCED > System Settings** tab in the web interface.
2. In the **TCP Connections Timeout** box, enter **1800** (30 minutes).
3. In the **UDP Connections Timeout** box, enter **1800** (30 minutes).

Task 2. Configure Enterprise Pool Services

To configure all Services needed for an internal OCS deployment:

1. Go to the **BASIC > Services** page in the web interface.
2. Add each Service listed in the table using the steps that follow; all of these Services are *required* :

Service Name	Virtual IP Address	Protocol	Port	Real Servers
MTLS Front	IP for FQDN of Internal enterprise OCS Pool e.g., 192.168.1.11/24 for `frontpool.domain.local`	TCP	5061	IP addresses of your Front-End Servers (K and L from the example)
DCOM WMI Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	135	IP addresses of your Front-End Servers (K and L from the example)
Internal Conf Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	444	IP addresses of your Front-End Servers (K and L from the example)
HTTPS Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	443	IP addresses of your Front-End Servers (K and L from the example)

For the DCOM WMI Front Service *only*, edit each Real Server associated with the Service by

clicking the **Edit** icon next to each Real Server entry in the table. On the **Real Server Detail** page that appears:

1. In the **Server Monitor** section, set the **Testing Method** to **TCP Port Check**.
2. In the **Port** field, enter the value **5061**. It is better to test port 5061 for this Service because port 135 always passes the TCP port check even if OCS Services are not responding.

To add a Service:

1. In the **Service Name** box, enter the name for the **Service**.
2. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal OCS Pool.
3. Select the protocol and in the **Port** box, enter the port for the Service in the table.
4. In the **Real Servers** box, enter the IP address for every Front-End server in your OCS Pool.

The following Services are *optional* ; add each Service *only* if you have deployed that feature.

Service Name	Virtual IP Address	Protocol	Port	Real Servers
Application Sharing (optional)	IP for FQDN of Internal enterprise OCS Pool	TCP	5065	IP addresses of your Front-End Servers (K and L from the example)
QoE Agent (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5069	IP addresses of your Front-End Servers (K and L from the example)
Response Group Service (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5071	IP addresses of your Front-End Servers (K and L from the example)
Conferencing Attendant (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5072	IP addresses of your Front-End Servers (K and L from the example)
Conferencing Announcement (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5073	IP addresses of your Front-End Servers (K and L from the example)
Outside Voice Control (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5074	IP addresses of your Front-End Servers (K and L from the example)

For each Service created, edit the Service by clicking the **Edit** icon next to the Service entry in the table. On the **Service Detail** page that appears:

1. In the **General** section, set Service Type to **TCP Proxy**.
2. In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

Task 3. Configure Internal Edge Services

Complete this task if you have an edge deployment.

To configure all the Services needed for a load balanced OCS Edge deployment, perform the following steps on the internal-facing Barracuda Load Balancer:

1. Go to the **BASIC > Services** page in the web Interface.
2. Add each Service listed in the table using the steps that follow; all Services are *required*:

Service Name	Virtual IP Address	Protocol	Port	Real Servers
MTLS Edge	IP for FQDN of Internal Enterprise OCS Pool e.g., 192.168.1.11/24 for `frontpool.domain.local`	TCP	5061	Internal IP addresses of your Edge Servers (I and J from the example)
AV Auth Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	5062	Internal IP addresses of your Edge Servers (I and J from the example)
RTP HTTP Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	443	Internal IP Addresses of your Edge Servers (I and J from the example)
WebConf Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	8057	Internal IP addresses of your Edge Servers (I and J from the example)
RDP Media Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	UDP	3478	Internal IP addresses of your Edge Servers (I and J from the example)

To add a Service:

1. In the **Service Name** box, enter the name for the **Service**.
2. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge OCS Pool.

3. Select the protocol and in the **Port** box, enter the port for the Service in the table.
4. In the **Real Servers** box, enter the internal IP address for every Edge server.

For each TCP Service created, edit the Service by clicking the **Edit** icon next to the Service entry in the table.

1. In the **General** section, set the **Service Type** to **TCP Proxy**.
2. In the **Advanced Options** section set **Session Timeout** to **0** (session never times out).

No change is required for RDP Media Edge, which is a UDP Service.

Task 4. Configure External Edge Services

Complete this task if you have an edge deployment.

The Real Servers should be physically connected to a switch which is connected to the LAN port of the Barracuda Load Balancer.

To configure all Services needed for a load balanced Edge Deployment of Office Communications Server, perform the following steps on the external-facing Barracuda Load Balancer:

1. Go to the **BASIC > Services** page in the web Interface.
2. Add each Service listed in the following table:

Service Name	**Virtual IP Address**	**Protocol**	**Port**	**Real Servers**
Access Edge	IP for FQDN of Access Edge e.g. IP address for `ocs.example.com`	TCP	443	IP address of Access Edge NICs on each Edge Server (C and F from the example)
WebConf Edge	IP for FQDN of WebConf Edge e.g. IP address for `webconf.example.com`	TCP	443	IP address of WebConf NICs on each Edge Server (D and G from the example)
AV Edge	IP for FQDN of AV Edge e.g. IP address for `av.example.com`	TCP	443	IP address of AV NICs on each Edge Server (E and H from the example)
AV UDP Edge	IP for FQDN of AV Edge e.g. IP address for `av.example.com`	UDP	3478	IP address of AV NICs on each Edge Server (E and H from the example)

To add a Service:

1. In the **Service Name** box, enter the name for the Service.
2. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge Lync Pool.
3. In the **Port** box, enter the port for that Service in the table.
4. In the **Real Servers** box, enter the internal IP address for every Edge Server.

No modifications need to be made to the default settings for these Services.

Task 5. Confirm the Configure Edge Server Wizard Setting

Complete this task if you have an edge deployment.

Verify the following on the Edge Servers:

When completing the Configure Edge Server Wizard, the **Internal Interface** dialog displays the following message:
“If you are using a load balancer, specify the IP address of the local server and the FQDN of the load balancer’s VIP."

In the **FQDN for the internal interface** field, enter the FQDN for the Access Edge DNS entry that external users are to use.

When correctly set, when the Edge Servers are queried for their host name strings, they return the FQDN of the VIP address for the external Access Edge instead of the FQDN of the internal interface. This ensures that the Subject Alternative Name (SAN) on the certificate assigned to this internal interface for the Access Edge matches the host string of the Edge server.

Task 6. Configure Director Services

Complete this task if you have deployed Director Servers.

To configure all the Services needed for Director Services, perform the following steps on the Director Barracuda Load Balancer:

1. Go to the **BASIC > Services** page in the web interface.
2. Add each Service listed in the following table:

Service Name	Virtual IP Address	Protocol	Port	Real Servers

Directory MTLS	IP for FQDN of the Director Service	TCP	5061	IP address of your Director Servers
Directory MTLS Legacy	IP for FQDN of the Director Service	TCP	5060	IP address of your Director Servers

To add a Service:

1. In the **Service Name** box, enter the name for the Service.
2. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Director Service.
3. In the **Port** box, enter the port for that Service in the table.
4. In the **Real Servers** box, enter the internal IP address for every Director Server.

For each Service created, edit the Service by clicking the **Edit** icon next to the Service entry in the table. On the **Service Detail** page that appears, complete the following:

1. In the **General** section, set **Service Type** to **TCP Proxy**.
2. In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

Task 7. Configure Communicator Web Access Services

Complete this task if you have deployed Communicator Web Access.

Communicator Web Access (CWA) is an optional feature of Office Communication Server that allows users who do not have access to the Office Communicator Client to access many of the features of Office Communications Server from a browser. Installations of CWA that have greater than 5000 users should deploy a load balancer for this feature. Microsoft recommends that you dedicate one or more load balancers that are used only for CWA for acceptable performance.

Configure the CWA servers to use HTTP rather than HTTPS. This allows the Barracuda Load Balancer to do SSL offloading, which improves the performance of the CWA Service. Also, this allows end user connections to be maintained using cookies, as recommended by Microsoft.

To configure the Services needed for a load balanced Communicator Web Access Server, perform the following steps on the Communicator Web Access Barracuda Load Balancer:

1. Go to the **BASIC > Certificates** page in the web interface, and upload the CWA certificate to the Barracuda Load Balancer.
2. Go to the **BASIC > Services** page in the web interface.
3. Add the Service listed in the following table:

Service Name	Virtual IP Address	Protocol	Port	Real Servers
CWA	IP for FQDN of CWA e.g. IP address for `cwa.domain.local`	TCP	443	IP address of CWA Servers

To add a Service:

1. In the **Service Name** box, enter the name for the Service.
2. In the **Virtual IP Address** box, enter the IP address for the FQDN of your CWA Service.
3. In the **Port** box, enter the port for that Service in the table.
4. In the**Real Servers** box, enter the internal IP address for every CWA Server.

Edit the Service by clicking the **Edit** icon next to the Service entry in the table. On the **Service Detail** page that appears, complete the following:

1. In the **General** section, set **Service Type** to **Layer 7 - HTTP**.
2. In the **Service Monitor** section, in the **Testing Method** list, click **HTTP**. In the **Test Target** box, enter http://*<fqdn of your CWA website>*/
3. For example, `http://cwa.domain.local/`
4. In the **Test Match** box, enter **Microsoft Corporation**.
5. In the **Persistence** section, change the **Persistence Type** to **HTTP Cookie**.
6. In the **SSL Offloading** section, set **Enable HTTPS/SSL** to **Yes**. In the **SSL Certificate** list, select the name of the certificate you uploaded for CWA.
7. In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

For each Real Server added, edit the Real Server by clicking the **Edit** icon next to each Real Server entry in the table. In the **Real Server Detail** section, change the value for **Port** to **80**.

To create a rewrite rule, go to the **Advanced > URL Rewrites** page in the web interface and create a rule to replace outgoing http://*<fqdn of your CWA Web site>* with https://*<fqdn of your CWA Web site>*. This rewrites absolute paths written by CWA so that they all appear as encrypted links; this rule prevents unsecure content errors in the browser:

1. In the **Layer 7 - HTTP Services** section, select the **CWA Service** from the list.
2. In the **Response Body Rewrite** section, create a new rule with the following options:
   - **Rule Name**: **cwa**
   - **Rule Order**: **1**
   - **Host Match**: *<fqdn of your CWA Web site>*, e.g. `cwa.domain.local`
   - **URL Match**: **/cwa/client/***
   - **Search String**: http://*<fqdn of your CWA Web site>*, e.g. `http://cwa.domain.local`
   - **Replace String**: https://*<fqdn of your CWA Web site>*, e.g. `https://cwa.domain.local`

Create the CWA Redirect Service; this Service ensures that end users are redirected from HTTP to the

HTTPS Service:

1. Go to the **BASIC > Services** page in the web interface.
2. In the **Service Name** field, enter the CWA Redirect Service name.
3. In the **Virtual IP Address** field, enter the IP address for the FQDN for your CWA Service.
4. Select the protocol **TCP**, and in the **Port** field enter **80**.

Edit the CWA Redirect Service by clicking the **Edit** icon next to the Service entry in the table:

1. In the **General** section, set the **Service Type** to **Layer 7 - HTTP**.
2. Set **Enable HTTP Redirect** to**Yes**.

Test the CWA installation:

1. Open a browser and enter: https://*<fqdn of your CWA Web site>*, e.g. `https://cwa.domain.local`
2. Ensure that all images load and that you are able to log into the CWA application without errors.

Your installation is now complete.

Refer to the Microsoft TechNet online library for more information on the following topics:

- Load Balancing Requirements for Office Communications Server 2007 Enterprise Pools
- Load Balancers for Office Communications Server 2007 R2
- Load Balancer Requirements for Edge Servers
- Using a Load Balancer to Increase Capacity and Availability