

## How to Cluster the Barracuda Email Security Gateway

<https://campus.barracuda.com/doc/43224523/>

Note that clustered systems can be geographically dispersed and do not need to be located on the same network. Important: Every Barracuda Email Security Gateway in a cluster must meet the following requirements:

- They must be the same model (400 or higher).
- They must have the same version of firmware installed.
- They can be different form factors (i.e. Physical ESG connected to Virtual ESG)
- They must be configured for the same time zone.
- They each must have a unique external IP address. This means that every Barracuda Email Security Gateway behind a NAT must have a unique external IP address and must be reachable by that external IP address.

When replacing a failed system in a cluster, be sure to follow step #3 as described below under **Removing a Barracuda Email Security Gateway From a Cluster**.

### Set Up Clustered Systems

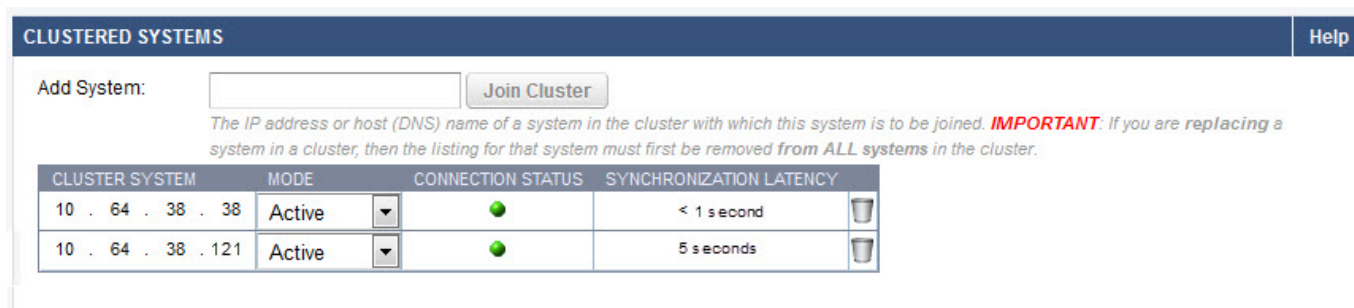
To cluster two Barracuda Email Security Gateways together, where one system is designated as "Barracuda1" and the other is designated "Barracuda2", do the following:

1. Complete the installation process for each system as described in [Step 2 - Install the Barracuda Email Security Gateway](#). Each Barracuda Email Security Gateway in a cluster must be the same model and be on exactly the same firmware version.
2. From the **ADVANCED > Task Manager** page on the Barracuda1 system, verify that no processes are running. Complete this step for the Barracuda2 system as well. No processes should be running when you add a system to a cluster.
3. From the **ADVANCED > Clustering** page on the Barracuda1 system, enter a **Cluster Shared Secret** password for the cluster, and click **Save**.
4. Optional: In the **Cluster Hostname** field on Barracuda1, enter the DNS/hostname (FQDN) by which other Barracuda Email Security Gateways in the cluster will attempt to communicate with this one. If this field is left blank, the IP address entered below will be used. This field is also useful for limiting user access to a cluster - see **Limiting Access to a Cluster** below.
5. From the **ADVANCED > Clustering** page on the Barracuda2 system, do the following:
  1. Enter the same **Cluster Shared Secret** password, and click **Save**.
  2. Optionally enter the DNS/hostname (FQDN) in the **Cluster Hostname** field for Barracuda2.
  3. In the Clustered Systems section, enter the IP address of the Barracuda1 system and click **Join Cluster**. At this point, the configuration of the Barracuda1 system will automatically



propagate to Barracuda2.

6. On each Barracuda system, refresh the **ADVANCED > Clustering** page, and verify that:
  1. Each system's IP address appears in the Clustered Systems list.
  2. The Connection Status of each server is green - see Figure 1 below.
7. Distribute the incoming mail traffic to each Barracuda Email Security Gateway using a Barracuda Load Balancer (preferred) or another load balancing device, or by using multiple DNS MX records of equal priority.

**Figure 1: Two servers in a cluster with a 'green' status.**



The screenshot shows the 'CLUSTERED SYSTEMS' section of the Barracuda management interface. At the top, there is a 'Help' button. Below it, an 'Add System:' field with a text input and a 'Join Cluster' button. A note below the button states: 'The IP address or host (DNS) name of a system in the cluster with which this system is to be joined. **IMPORTANT:** If you are replacing a system in a cluster, then the listing for that system must first be removed from ALL systems in the cluster.'

CLUSTER SYSTEM	MODE	CONNECTION STATUS	SYNCHRONIZATION LATENCY
10 . 64 . 38 . 38	Active		< 1 second
10 . 64 . 38 . 121	Active		5 seconds

## Add a Barracuda Email Security Gateway to a Cluster

Make a backup of the configuration of any system in the cluster. Then, perform the following steps on the Barracuda Email Security Gateway that you want to add to the existing cluster:

1. Complete the installation process and ensure that the new Barracuda Email Security Gateway is the same model# and running the same firmware version as all systems in the cluster.
2. From the **ADVANCED > Task Manager** page, verify that no processes are running. Do this on all other systems in the cluster as well.
3. From the **ADVANCED > Clustering** page, enter the **Cluster Shared Secret** password for the cluster, and click **Save**.
4. Optional: In the **Cluster Hostname** field, enter the DNS/hostname (FQDN) by which other Barracuda Email Security Gateways in the cluster will attempt to communicate with this one.
5. On a Barracuda Email Security Gateway that is already in the cluster: change any value in the configuration and click **Save**. This ensures proper synchronization of the configuration.
6. On the **ADVANCED > Clustering** page on the new Barracuda Email Security Gateway to be added to the cluster, enter the IP address of any system in the cluster in the **Add System** field and click the **Join Cluster** button. At this point, the configuration of the cluster will automatically propagate to the newly added system.

## Bayesian Analysis on Clustered Systems

When the Barracuda Email Security Gateway is clustered, resetting the Bayesian database must be done on each system individually. However, messages classified as *SPAM* or *NOT SPAM* will synchronize across the clustered systems.

---

### Limiting End-User Access to the Cluster

You can dedicate a single Barracuda Email Security Gateway as the Quarantine Host to serve up the end-user interface through which users will access their quarantine inboxes, even though their actual quarantine inbox (primary or secondary) may be hosted by another Barracuda Email Security Gateway in the cluster. By not directing email to the Quarantine Host, you can:

- Enhance network security by limiting end-user access (port 8000 by default) and administration to only one Barracuda Email Security Gateway on the Internet
- Insulate the user interface performance from any peaks in email volume

To configure one Barracuda Email Security Gateway as the Quarantine Host, from the **BASIC > Quarantine** page, enter that system's hostname in the **Quarantine Host** field.

---

### Removing a Barracuda Email Security Gateway From a Cluster

1. Log into the system to be removed and change or clear the **Cluster Shared Secret** on the **ADVANCED > Clustering** page. Click Save Changes. Changing the cluster shared secret prevents the systems in the cluster from communicating with one another.
2. On the same system, delete all other systems from the **Clustered Systems** list.
3. On any system that remains in the cluster, go to the **ADVANCED > Clustering** page. In the **Clustered Systems** list, delete the system to be removed from the cluster. This step is very important when removing a failed Barracuda Email Security Gateway from a cluster.

---

### Exporting the Message Log

In a clustered environment, the maximum number of lines in a Message Log export is 10,000. To export more lines, use the Date Range feature in your Message Log search. For more information, see [How to Export the Message Log](#).

---

### Centralized Policy Management With a Quarantine Host

You can optionally designate one Barracuda Email Security Gateway as the "host" of the cluster such that all administration of configuration settings and access to per-user quarantine for the cluster can only be accessed and set from that node. This option has two advantages: it provides for additional security by limiting access to administration of the cluster, and it protects the user interface from mail processing load since, with this configuration, you do not direct any email traffic to the host node.

To assign one Barracuda Email Security Gateway as the host of the cluster, enter the hostname of that device in the Quarantine Host field on the **BASIC > Quarantine** page and do not direct any email to that device.

## Redundancy of User Quarantine Data on the Cluster

Each user account has a primary and backup server in the cluster. Regardless of how many Barracuda Email Security Gateways there are in the cluster, there are always two appliances that have the same quarantine information (configuration and quarantine messages).

## Data Not Synchronized Across the Cluster

Clustering provides 100% redundant coverage of the propagated data. However, for practical reasons, some data is not propagated to the other clustered systems when a new system joins. Energize updates do not synchronize across systems in a cluster. The following Barracuda Email Security Gateway configurations are considered unique and will not sync to match other Barracuda Email Security Gateways in a cluster:

Note: For firmware version 9.0.0.005 and later, the *admin* password is synchronized across clustered systems. Previous to that firmware version, the *admin* password was not synchronized.

- IP Address, Subnet Mask, and Default Gateway (on the **BASIC > IP Configuration** page)
- Primary DNS Server and Secondary DNS Server (on the **BASIC > IP Configuration** page)
- Serial number (this will never change)
- Hostname (on the **BASIC > IP Configuration** page)
- Any advanced IP configuration (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Advanced Networking** page)
- Guest password
- Time Zone (on the **BASIC > Administration** page)
- Cluster hostname (on the **ADVANCED > Clustering** page)
- Cluster Shared Secret, though this must be the same for the cluster to work properly (on the

## **ADVANCED > Clustering** page)

- Local Host Map (on the **ADVANCED > Clustering** page)
- SMTP Welcome Banner (on the **ADVANCED > Email Protocol** page)
- Web Interface HTTP Port (on the **BASIC > Administration** page)
- Web Interface HTTPS/SSL port (on the **ADVANCED > Secure Administration** page)
- Any other secure administration configuration, including saved certificates (on the **ADVANCED > Secure Administration** page)
- Quarantine Host (on the **BASIC > Quarantine** page)
- All SSL/TLS information, including saved certificates (on the **ADVANCED > Secure Administration** page)
- Whether to only display local messages in the message log (Only view local messages on the **BASIC > Message Log > Preferences** page)
- Whether the latest release notes have been read
- All customized branding (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Appearance** page)
- The explicit users list (if enabled and used, on the **Advanced > Explicit Users** page)
- The Valid Recipients list (3.5.11 and above only, on the **Domains > Edit Domain** pages)

## Figures

### 1. ClusteredSystems.jpg

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.