

## How to Manage Ranges and Clusters

<https://campus.barracuda.com/doc/98210415/>

CloudGen Firewalls are organized into a two-level hierarchy on the Firewall Control Center: Ranges and Clusters.

These two levels are in a relation of 1:n. In other words, one range can include any number of clusters. The maximum number of ranges and clusters depends both on the type of Control Center and on the specific licenses that can be obtained additionally upon request.

The following Control Centers provide a different number of maximum ranges and clusters:

### VC Editions - Virtual appliances for use on hypervisor platforms

- **VC400 Standard Edition** - One range (tenant), three clusters (configuration groups), and unlimited managed firewalls. Additional ranges can be obtained through licenses.
- **VC610 Enterprise Edition** - Two ranges (tenants), unlimited clusters (configuration groups), and unlimited managed firewalls. Additional ranges can be obtained through licenses.
- **VC820 Global Edition** - Five ranges (tenants), unlimited clusters (configuration groups), and unlimited managed firewalls. Additional ranges can be obtained through licenses.

### VCC Editions - Virtual appliances for use in public clouds

- **VCC400 Standard Edition** - One range (tenant), three clusters (configuration groups), and unlimited managed firewalls.
- **VCC610 Enterprise Edition** - Two ranges (tenants), unlimited clusters (configuration groups), and managed firewalls.

## Usage of Ranges and Clusters

One common use is to create ranges for regions such as North America and EMEA, and then to create clusters for each country in the region. Configuration and default settings shared by multiple CloudGen Firewalls can be configured on the cluster or range level. To create reusable configurations for multiple firewalls, use a repository. The configuration of an individual system can then be linked or copied from a range or global repository, making it easy to deploy a change to all managed systems.

## Create a Range

You must create at least one range on a Control Center.

1. Click the **CONFIGURATION** tab.
2. Right-click **Multi-Range** and select **Create Range**.
3. Enter a **Range Number**.
4. (optional) Enter a **Description**.
5. (optional) Enter the contact details in the **Contact Info** field.
6. Configure the range properties as described in the **Specific Settings** section.
7. Click **Next**.
8. (optional) Enter the owner and purchase details in the information sections.
9. Click **Finish**.
10. Click **Activate**.

## Remove a Range

Deleting a range is final and will also remove all clusters and managed firewalls in the range. Create a backup before deleting a range.

1. Click the **CONFIGURATION** tab.
2. Right-click the range you wish to remove and click **Lock**.
3. Right-click the range and select **Remove Range**.
4. Click **OK** to confirm the deletion.
5. Click **Activate**.

## Create a Cluster

Unless you are using a Standard Edition Control Center, there is no limit on how many clusters you can create. For migration purposes only, Control Center editions allowing only one cluster allow the introduction of an additional migration cluster with the default name **migrate**. This cluster is not intended for production use.

1. Click the **CONFIGURATION** tab.
2. Expand **Multi-Range**, right-click your desired range, and select **Create Cluster**.
3. Select the software release of the CloudGen Firewalls that should be managed, and click **OK**.
4. Enter a **Cluster Name**. Cluster names must be unique in the range.
5. Enter a **Description**.

The cluster description is used as the cluster name and displayed wherever the cluster is visible in the interface if configured to do so in the **Admin and CC Settings**. For more information, see [Barracuda Firewall Admin Settings](#).

6. (optional) Enter the contact details.
7. (optional) Configure the cluster properties as described in the **Specific Settings** section.
8. Click **Next**.

9. (optional) Enter the owner and purchase details in the information sections.
10. Click **Finish**.
11. Click **Activate**.

## Remove a Cluster

Deleting a cluster is final and will also remove all clusters and managed firewalls. Create a backup before deleting a cluster.

1. Click the **CONFIGURATION** tab.
2. Navigate to the cluster you wish to remove.
3. Right-click the cluster and, in the context menu, select **Lock**.
4. Right-click the cluster and, in the context menu, select **Remove Cluster**.
5. Click **OK**.
6. Click **Activate**.

## Range-Specific and Cluster-Specific Settings

Each range and cluster can override global settings by using its own configuration interface. When enabling these settings, the scope is limited to the range or cluster it is set for.

Setting	Description
<b>Disable Update</b>	Enables/disables configuration updates for boxes from this range or cluster.
<b>Collect Statistics</b>	Triggers the Control Center to collect statistics from managed boxes within this range or cluster.
<b>Own Cook Settings</b>	Introduces the node <b>Statistics Cook Settings</b> where you can define the custom cook settings for the range (see <a href="#">How to Configure Statistics Processing and Maintenance</a> ). If the range or cluster requires special cook settings for statistical data, enable this parameter.
<b>Own Event Settings</b>	Introduces the node <b>Eventing</b> where you can define custom event settings for the range or cluster (see <a href="#">How to Configure Event Notifications</a> ). If the range or cluster requires special event settings, enable this parameter.
<b>Own Firewall Objects</b>	Enables range-specific/cluster-specific firewall objects and introduces the node <b>Range/Cluster Firewall Objects</b> where you can define range-specific/cluster-specific network objects (see <a href="#">Firewall Objects</a> and <a href="#">Network Objects</a> ).

<b>Own VPN GTI Editor</b>	Enables a range-specific/cluster-specific VPN GTI Editor and introduces the node <b>VPN GTI Editor(range/cluster name)</b> . For more information, see <a href="#">How to Create a VPN Tunnel with the VPN GTI Editor</a> .
<b>Own Access Control Objects</b>	Enables range-specific/cluster-specific policy server objects and introduces the node <b>Access Control Objects</b> containing the files <b>Welcome Message, Personal Firewall Rules, Pictures, and Registry Checks</b> (like <b>Access Control Service</b> ).
<b>Own Traffic Shaping Settings</b>	Enables range-specific/cluster-specific traffic shaping settings and introduces the node <b>Range/Cluster Shaping Trees</b> (see <a href="#">Traffic Shaping</a> ).
<b>Own Certificate Store</b>	Enables the node for a range-specific/cluster-specific certificate store. This node will be subordinated to the node <b>Range Settings</b> with the name <b>Certificate Store</b> . Note that this node will be displayed only if the related option <b>Own Certificate Store</b> is enabled in the node <b>Range Properties/Cluster Properties</b> in the section <b>Specific Settings</b> .
<b>Send Statistics to Reporter (legacy)</b>	Sends central statistics data to the legacy Barracuda NG Reporter appliance.

## Migrating the Configuration

Migration can only be performed at the next major firmware version (5.4 > 6.0 > 6.1 > 6.2 > 7.0 > 7.1 > 7.2 > 8.0 > etc).

You must migrate your configuration in the following order:

1. Update the Control Center firmware.
2. Update all managed firewalls within a cluster.
3. Migrate the cluster version.

### Migrating a Repository-Linked Firewall

If you are using a repository, you must prepare the repository-linked firewalls before migration.

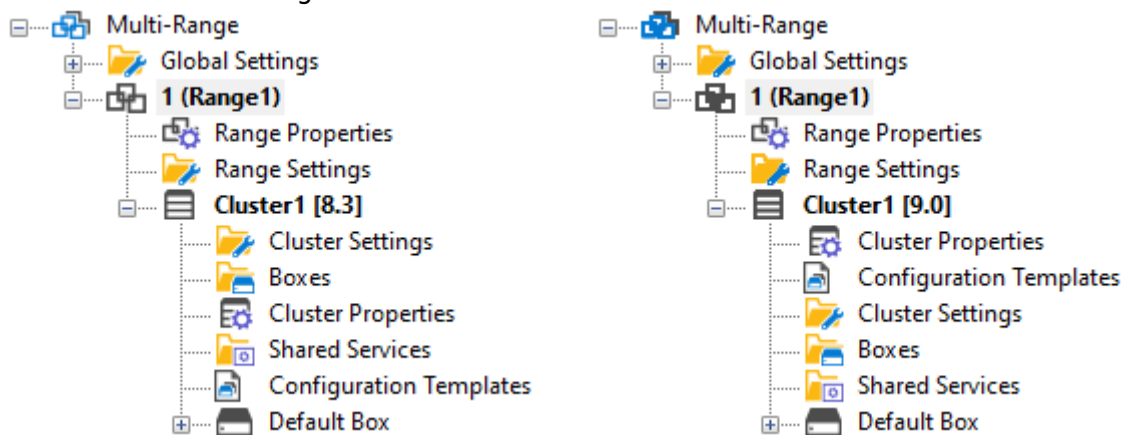
For information, see [How to Prepare Repository Linked Box Configurations for Migration](#).

1. Click the **CONFIGURATION** tab.
2. Expand **Multi-Range** and navigate to the desired object in the **Repository** tree.
3. Right-click the object and click **Lock**.
4. Right-click the object and select **Migrate Node**.
5. Select the destination major firmware version.
6. Click **OK**.
7. Click **Activate**.

### Migrate a Cluster or Range

Clusters can only be migrated to a higher firmware version. You cannot downgrade a cluster configuration.

1. Click the **CONFIGURATION** tab.
2. Navigate to the cluster or range you wish to migrate.
3. Right-click the cluster or range and click **Lock**.
4. Right-click the cluster and select **Migrate Cluster / Migrate Range**.
5. Choose the version number as the migration destination, and click **OK** to confirm the migration.
6. Review the future configuration.

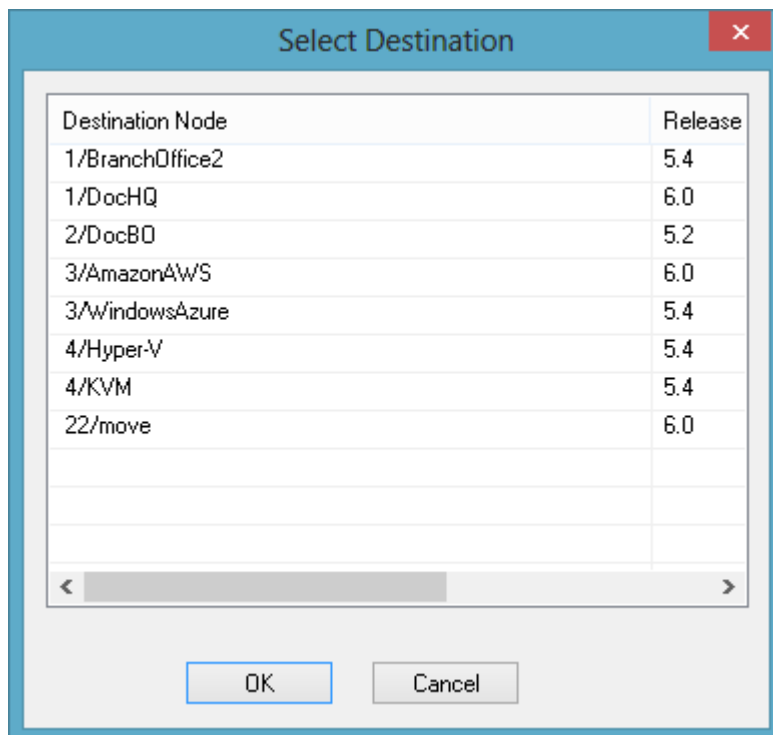


The **MailGW Settings** and the **Service Configuration** nodes will be changed during this migration process. Open the nodes to look at the new configuration dialogs.

7. Click **Activate**.

### Migrate Multiple Clusters and Ranges

1. Click the **CONFIGURATION** tab.
2. Right-click **Multi-Range** and select **Migrate Clusters / Migrate Ranges** from the context menu.
3. Select the nodes to be migrated while holding down the **SHIFT** key.

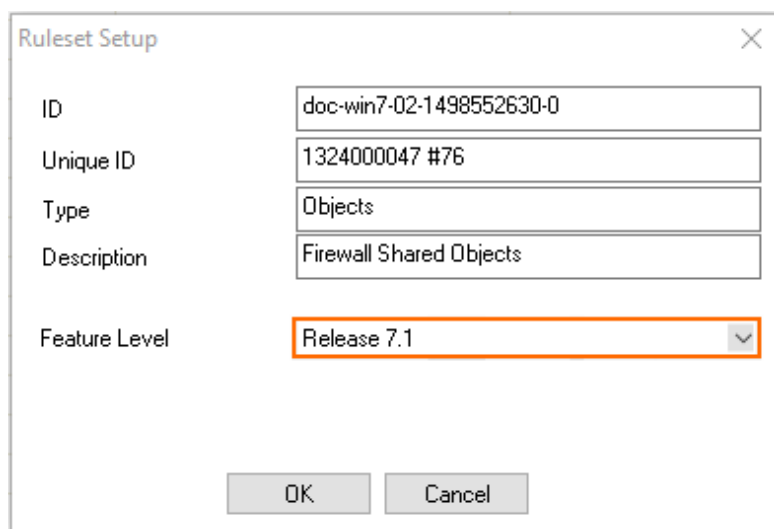


4. Click **OK** to confirm the migration.
5. Click **Activate**.

## Migrate Global Firewall Objects

When upgrading a firewall to a newer version, you must also migrate the ruleset and the global firewall objects to the new feature level.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Firewall Objects**.
2. Click **Lock**.
3. Expand the **Settings** menu on the left and select **Setup**. The **Ruleset Setup** window opens.
4. Select the new **Feature Level** from the drop-down list.



The image shows a 'Ruleset Setup' dialog box with the following fields and values:

Field	Value
ID	doc-win7-02-1498552630-0
Unique ID	1324000047 #76
Type	Objects
Description	Firewall Shared Objects
Feature Level	Release 7.1

At the bottom of the dialog are 'OK' and 'Cancel' buttons. The 'Feature Level' dropdown is highlighted with an orange border.

5. Click **OK** to confirm the migration.
6. Click **Send Changes** and **Activate**.

## Figures

1. conf\_tree\_cluster\_83.png
2. conf\_tree\_cluster\_90.png
3. mig\_config.png
4. change\_feature\_level.png

© 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.