

Configure an Email Security Appliance (ESA) Cluster

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Clusters on ESA](#)

[Create the Cluster](#)

[Create Cluster Over SSH](#)

[Create Cluster Over CCS](#)

[Join an Current Cluster Through SSH or CCS](#)

[Join Through SSH](#)

[Join Through CCS](#)

[What is Migrated in a Cluster Configuration](#)

[What isnot Migrated in a Cluster Configuration](#)

[How are Groups Configured in an ESA Cluster](#)

[Related Information](#)

Introduction

This document describes how to set up a cluster on a Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How to join appliances into a Cluster (Centralized Management).
- All ESAs must have the same AsyncOS versions (down to the revision).

 **Note:** In version 8.5+ the Centralized Management key is no longer required and also no longer be visible when added as it is an incorporated feature within the AsyncOS.

- If you create a cluster to use port 22 (easier to configure) ensure that there are no firewall or routing issues between the Appliances on port 22 traffic.
- If you create a cluster to use port 2222 (Cluster Communication Service) ensure that firewall rules are made to allow traffic on this port to be available without inspection or interruption.
- Cluster configuration options must be done via the CLI on the ESA and cannot be created or joined in the GUI.

- If you choose to use a hostname for communication, ensure DNS servers set on the appliances are able to resolve all the other appliances in your network, and that the IP addresses the hostnames resolve to are assigned to an interface that is configured to listen on the communications port selected.
- Ensure on your appliance Interfaces, the required port and service are enabled (SSH or CCS).

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

The problem is to avoid the continuous need for modification on each appliance whenever a configuration between a large group of ESAs needs to be centralized and kept in sync.

Clusters on ESA

The ESA centralized management feature allows you to manage and configure multiple appliances at the same time, to provide increased reliability, flexibility, and scalability within your network. This allows you to manage globally while at the same time you comply with local policies.

A cluster consists of a set of machines with common configuration information. Within each cluster, the appliances can be further divided into machine groups, where a single machine can be a member of only one group at a time.

Clusters are implemented in a peer-to-peer architecture with no primary/secondary relationship. You can log into any machine to control and administer the entire cluster or group. This allows the administrator to configure different elements of the system on a cluster-wide, group-wide, or per-machine basis, founded on their own logical groups

Create the Cluster

Once all requirements are met, to create the cluster, you need to begin in the command line (CLI) of the first appliance.

 **Tip:** Back up your current configuration on your appliance before you configure your cluster. From the GUI, **System Administration > Configuration File**. Uncheck the masked password box and save the configuration locally to your PC.

Create Cluster Over SSH

```
C370.lab> clusterconfig
```

Do you want to join or create a cluster?

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2

Enter the name of the new cluster.

[> NameOfCluster

Should all machines in the cluster communicate with each other by hostname or by IP address?

1. Communicate by IP address.

2. Communicate by hostname.

[2]> 1

What IP address should other machines use to communicate with Machine C370.lab?

1. 10.1.1.11 port 22 (SSH on interface Management)

2. Enter an IP address manually

[> 1

Other machines will communicate with Machine C370.lab using IP address 10.1.1.11 port 22. You can change this by using the COMMUNICATION subcommand of the clusterconfig command.

New cluster committed: DATE

Creating a cluster takes effect immediately, there is no need to commit.

Cluster NameOfCluster

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

Create Cluster Over CCS

C370.lab> clusterconfig

Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2

Enter the name of the new cluster.

[> Test

Should all machines in the cluster communicate with each other by hostname or by IP address?

1. Communicate by IP address.

2. Communicate by hostname.

[2]> 1

What IP address should other machines use to communicate with Machine C370.1ab?

1. 10.1.1.1 port 22 (SSH on interface Management)
 2. Enter an IP address manually
- ```
[> 2
```

Enter the IP address for Machine C370.1ab.

```
[> 10.1.1.1
```

Enter the port (on 10.66.71.120) for Machine C370.1ab.

```
[22]> 2222
```

Once this step is done, you have a cluster and all your configurations are moved from the Machine to the Cluster level. This is the configuration *all* other machines inherit when they are joined.

## Join an Current Cluster Through SSH or CCS

This section covers how to add any new appliances into your current cluster that you have previously or just created. Join a current cluster by either method is similar in approach, the only key point of difference is CCS requires an extra step to finalize it to allow the cluster to accept the newer appliance.

### Join Through SSH

---

 **Note:** The section indicated in **bold** in these next steps needs to be done exactly, with SSH, you must not say yes to CCS enabling.

---

```
<#root>
```

```
C370.1ab> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 3
```

```
While joining a cluster, you will need to validate the SSH host key of the remote machine to which you
To get the public host key fingerprint of the remote host, connect to the cluster and run: logconfig ->
-> fingerprint.
```

```
WARNING: All non-network settings will be lost. System will inherit the values set at the group or clus
the non-network settings. Ensure that the cluster settings are compatible with your network settings (e
settings)
```

```
Exception: Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the clus
These settings on this machine will remain intact.
```

```
Do you want to enable the Cluster Communication Service on C370.1ab? [N]>
```

```
Enter the IP address of a machine in the cluster.
```

```
[> 10.66.71.120
```

```
Enter the remote port to connect to. This must be the normal admin ssh port, not the CCS port.
```

```
[22]>
```

Enter the name of an administrator present on the remote machine  
[admin]>

Enter password:  
Please verify the SSH host key for 10.66.71.120:  
Public host key fingerprint: d2:6e:36:9b:1d:87:c6:1f:46:ea:59:40:61:cc:3e:ef  
Is this a valid key for this host? [Y]>

After the check, the appliance joins the cluster successfully.

## Join Through CCS

This is similar in approach, the only difference is that before you decide to allow the new appliance into the current cluster, you need to log into the appliance that is active in the cluster.

On the active appliance in the cluster:

```
(Cluster test)> clusterconfig
```

```
Cluster test
```

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

```
[]> prepjoin
```

Prepare Cluster Join Over CCS

No host entries waiting to be added to the cluster.

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

```
[]> new
```

Enter the hostname of the system you want to add.

```
[]> ESA.lab
```

Enter the serial number of the host ESA.lab.

```
[]> XXXXXXXXXXXXXXX-XXXXXA
```

Enter the user key of the host ESA2.lab. This can be obtained by typing "clusterconfig prepjoin print" in the CLI on ESA.lab.

Press enter on a blank line to finish.

Once you enter the SSH fingerprint (which is obtained when you log into the appliance that attempts to join your cluster and with the command `clusterconfig prepjoin print`) in the previous code example and enter a blank line, it completes the prep join.

---

 **Note:** If you run the `PREPJOIN` option, you need to commit your changes to the primary ESA before you run `clusterconfig` on the secondary ESA and join that appliance to your newly configured cluster. This is noted from the output throughout the operation: to join this appliance to a cluster with pre-shared keys, log in to the cluster machine, run the `clusterconfig > prepjoin > new` **command**, enter the next details, and `commit` your changes.

---

Then you can begin the join process on the appliance that attempts to join in, for reference, call it **ESA2.lab** to match that of the previous step.

---

 **Note:** The SSH-DSS key is in the next example.

---

```
ESA2.lab> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 4
```

```
While joining a cluster, you will need to validate the SSH host key of the remote machine to which you .
To get the public host key fingerprint of the remote host, connect to the cluster and run: logconfig ->
-> fingerprint.
```

```
WARNING: All non-network settings will be lost. System will inherit the values set at the group or clus
the non-network settings. Ensure that the cluster settings are compatible with your network settings (e
settings)
```

```
Exception: Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the clus
These settings on this machine will remain intact.
```

```
In order to join a cluster over CCS, you must first log in to the cluster and tell it that this system
On a machine in the cluster, run "clusterconfig -> prepjoin -> new" with the following information and
```

```
Host: ESA2.lab
```

```
Serial Number: XXXXXXXXXXXX-XXXXXXA
```

```
User Key:
```

```
ssh-dss AAAAB3NzaC1kc3.....BrccM=
```

```
Choose the interface on which to enable the Cluster Communication Service:
```

1. ClusterInterface (10.1.1.2/24: ESA2.lab)

```
[1]> 1
```

```
Enter the port on which to enable the Cluster Communication Service:
```

```
[2222]
```

```
Enter the IP address of a machine in the cluster.
```

```
[> 10.1.1.1
```

```
Enter the remote port to connect to. This must be the CCS port on the machine "10.1.1.1",
not the normal admin ssh port.
```

```
[2222]>
```

Once this is confirmed, you see the SSH-DSS key. If it matches, you can accept the terms and the cluster is joined successfully.

## **What is Migrated in a Cluster Configuration**

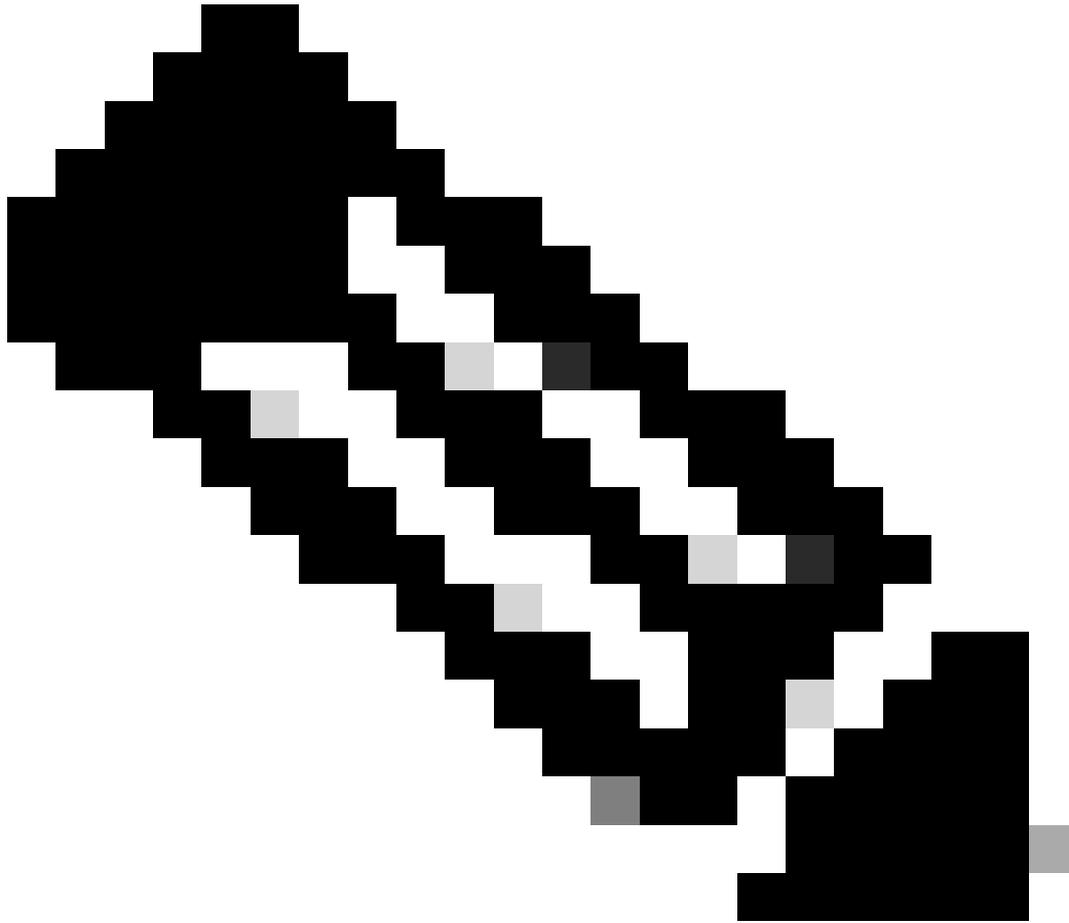
Cluster configuration migrates:

- Configured Policy Settings
- Content Filters
- Text Resources
- Content Dictionaries
- LDAP Settings
- Anti-spam And Anti-virus
- Global Settings
- Listener Settings
- SMTP Route Settings
- DNS Settings

## **What is not Migrated in a Cluster Configuration**

Cluster configuration does not migrate:

- Appliance Local Hostname.
- Configured IP Interfaces.
- Configured Routing Tables.
- Local Spam Quarantine Configuration.
- Local Policy, Virus and Outbreak Quarantine Configurations
- Settings under the `websecurityadvancedconfig` command in the Command Line (for versions 8.5 and newer).



**Note:** If you have content filters that reference quarantines that do not exist, they are invalidated until the referenced Policy Quarantine(s) has been configured on the machine.

---

## How are Groups Configured in an ESA Cluster

In certain scenarios, it can be required that few ESAs in the Cluster work in a particular way than the rest. To achieve this, you do not need to create a new cluster and you can proceed with creation of Groups.

---

**Note:** The configurations that are made at Group level, takes precedence over the Cluster level configuration.

---

For the creation of Groups, create it from the ESA CLI. To begin the configuration, use the command `clusterconfig --> ADDGROUP` :

```
(Machine esalab.cisco.com)> clusterconfig
```

```
This command is restricted to "cluster" mode. Would you like to switch to "cluster" mode? [Y]>
```

```
Cluster Cisco
```

```
Choose the operation you want to perform:
```

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.

- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

[]> ADDGROUP

Enter the name of the new cluster group to create.

[]> New\_Group

Cluster group New\_Group created.

To add ESAs from the current cluster to the new Group created, use the command SETGROUP:

(Machine esalab.cisco.com)> clusterconfig

This command is restricted to "cluster" mode. Would you like to switch to "cluster" mode? [Y]>

Cluster Cisco

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[> SETGROUP

Choose the machine to move to a different group. Separate multiple machines with commas.

1. esalab.cisco.com (group ESA\_Group)

[1]> 1

Choose the group that esalab.cisco.com must be a member of.

1. ESA\_Group

2. New\_Group

[1]> 2

esalab.cisco.com set to group New\_Group.

To rename a current Group in the ESA Cluster, use the command RENAMEGROUP:

(Machine esalab.cisco.com)> clusterconfig

This command is restricted to "cluster" mode. Would you like to switch to "cluster" mode? [Y]>

Cluster Cisco

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEDGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- CONNSTATUS - Show the status of connections between machines in the cluster.

- COMMUNICATION - Configure how machines communicate within the cluster.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[> RENAMEGROUP

Choose which group you wish to rename.

1. ESA\_Group

2. New\_Group

[1]> 2

Enter the new name of the group.

[New\_Group]> Cluster\_Group

Group New\_Group renamed to Cluster\_Group.

To delete a current group from the ESA Cluster, use the command `DELETEGROUP`

(Machine esalab.cisco.com)> clusterconfig

This command is restricted to "cluster" mode. Would you like to switch to "cluster" mode? [Y]>

Cluster Cisco

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

[ ]> DELETEGROUP

Choose which group you wish to remove.

1. Cluster\_Group

2. ESA\_Group

[1]> 1

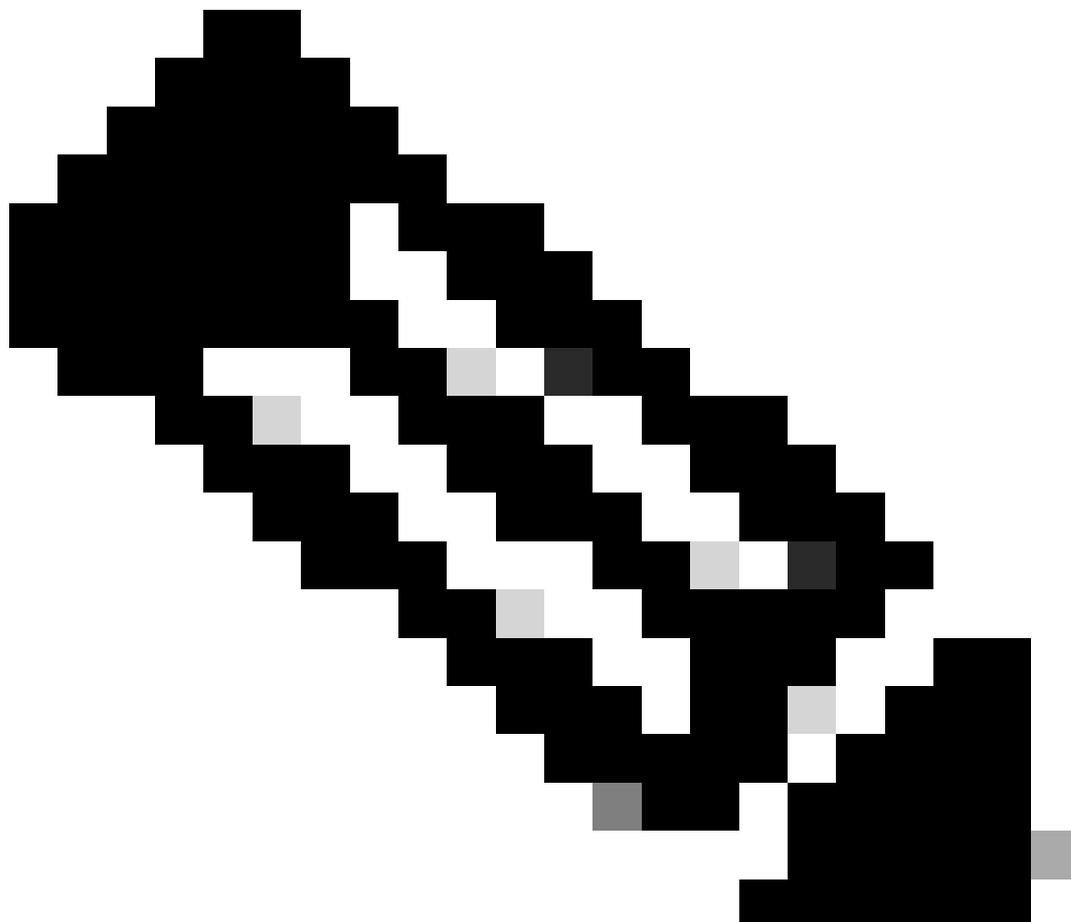
Choose the group that machines in Cluster\_Group must be moved to.

1. ESA\_Group

[1]> 1

Group Cluster\_Group removed.

---



**Note:** When you add / remove machines in Cluster, the changes apply instantly to the appliances without a `commit`. Whereas for ESA Groups, any actions related to it is applied to the ESAs only after a `commit`.

---

## Related Information

- [Cisco Technical Support & Downloads](#)