Forcepoint Appliances: Changing the C Interface IP Address

Updated: 31-July-2017

Applies To:	Forcepoint™ V Series, X Series, and Virtual Appliances, version 8.4.0

If at all possible, do not change the appliance management interface (C) IP address of your appliance. What is affected and what must be done depends on the configuration of your appliance.

If your appliance hosts Forcepoint Email Security and you must change the C interface IP address, follow the procedure in this article.

If your appliance hosts Forcepoint Web Security, changing the C interface IP address requires a full reinstall (re-image) of the appliance. See the knowledge base article How to restore a Forcepoint appliance to a v8.4.x factory image.

Email Security: Changing the C interface IP address

Step-by-step instructions:

1. Perform a full backup of the appliance and all off-box components and save the backups to a network location.
2. If email Data Loss Prevention (DLP) is used:
   a. In the Email module of Forcepoint Security Manager, go to **Settings** > **General** > **Data Loss Prevention** and unregister DLP. Make a note of the TRITON Manager IP address. You must also know the administrator user name and password.
   b. In the DATA module of Forcepoint Security Manager, go to **Settings** > **Deployment** > **System Module** and delete the entry for the affected appliance.
3. On the appliance, change the C interface IP address:
   a. Log on to the appliance CLI and elevate to **config** mode.
   b. Use the **set interface ipv4** command to change the C interface IP address.

```
set interface ipv4 --interface c --ip <new_c_ip_address>
  --mask <subnet_mask> [--gateway <gateway_ip_address>
```

The gateway IP address is optional.

You are prompted to confirm the action. The prompt is similar to:

```
Changing the IP address of the C interface impacts other
TRITON components.
Do you want to continue? (yes/no):
```

Enter **yes** to confirm the action.

The change is applied to all appliance components.

4. In the Email module of Forcepoint Security Manager, go to **Settings** > **Personal Email** > **Notification Message**. In the Notification Message Links area, change the IP address to the new C IP address.
5. If your deployment uses Secure Message Delivery as the encryption method, and the IP address or hostname uses the C interface, go to **Settings** > **Inbound/Outbound** > **Encryption** and change the IP address. If the setting uses the E or P interface, no change is needed.
6. If Data Loss Prevention is used:
   a. In the Email module of Forcepoint Security Manager, go to **Settings** > **General** > **Data Loss Prevention** and register the appliance.
   b. Return to the Data module and deploy.
7. If you use the Hybrid Service and the C interface IP address is specified as an SMTP inbound server address, update the IP address for that entry. If the E or P IP address is specified, no change is needed.
   a. Go to **Main** > **Hybrid Service** and edit the Delivery Route configuration.
   b. Update the affected SMTP Inbound Server Address entry.
8. Update the Log Database configuration.
   a. On the Log Database host, open SQL Server Management Studio.
   b. Click **New Query**.
   c. In the query window, enter the following command:

      ```
      USE [esglogdb76]
      ```

      Select the **esg_device_id**, **admin_manage_ip**, and **device_c_port_ip** from the dbo.esg_device_list.
   d. Enter **GO**.
   e. Locate the **esg_device_id** associated with either the admin_manage_ip or the device_c_port_ip of the source appliance.
   f. Execute the following command using the values you obtained in the previous steps:

      ```
      UPDATE dbo.esg_device_list SET esg_name = '<host name>',
      admin_manage_ip = '<appliance management IP address>',
      device_c_port_ip = '<C IP address>' WHERE esg_device_id =
      '<device id>'
      ```
   g. Enter **GO**.
   h. Run the query.