Forcepoint

Remote Browser Isolation

22.11

On-Premises Deployment Guide

Revision A

Published 16 December 2022

Contents

Chapter 1

Introduction

Contents

Forcepoint Remote Browser Isolation (Forcepoint RBI) helps organizations experience a safer internet by proactively stopping web, email, and document-based threats. This document captures the prerequisites for an on-premises deployment of Forcepoint RBI. Details have been provided for recommended network port openings required for communication.

Forcepoint RBI has three major components:

- Control Center Cluster (Master & Worker): The Control Center cluster contains the Forcepoint RBI Admin Portal and Superadmin Portal. The Portal is responsible for policy management, user authentication, logging, dashboard, and reporting.
- RBC Cluster (Master & Worker): The Remote Browsing Containers (RBCs) house the remote browsers that connect to the Internet to fetch, execute, and render the content.
- Proxy: The proxy handles all traffic redirection from the end user's browser to the RBC.

This document provides the specifications required for the Virtual Machine and Network Communication. Refer to the *Sizing Guide* for hardware specifications for Forcepoint RBI.

Deployment prerequisites

Before deploying Forcepoint RBI in an on-premises environment, review these prerequisites.

- Virtualization platform should be based on any of the following virtualization products:
  - Virt-Manager (KVM)
  - Oracle VirtualBox
  - VMware
- Forcepoint RBI systems should be reachable from endpoint machines (end user systems).
- One IP address is to be assigned to each Forcepoint RBI component (master, worker, proxy).
- Public Wildcard SSL certificate or a Self-Signed SAN-based wild card certificate, including RBI servers IP address as SAN, is required for Forcepoint RBI. Public certificate, Private key, and CA certificates are required.
  For Self-Signed certificates, install the Root CA Chain Certificate on the endpoint machines under **Trusted Root CA Authority**.
- The FQDN names of Forcepoint RBI should be resolved by the endpoint machines by following one of these options:
  - Add DNS entries for Forcepoint RBI FQDNs and URLs to the respective domain.
  - Add the FQDN entries for Forcepoint RBI in the user's endpoint machine host file (`C:\windows\system32\drivers\etc\hosts`). This requires Admin access to the endpoint machine.

  - If there is a local/Internal DNS in place for resolving Intranet/Internal servers and it is configured as a DNS server in the user's endpoint machine, then create a zone for the domain of the FQDN in the Local/Internal DNS and add the host entries to it so that users can resolve the FQDNs through local/Internal DNS.
- The Forcepoint RBI instances need to be provided with DNS servers that can resolve Global domains.
- If a proxy server is in place, then the IP address and the port of the proxy server must be configured in Forcepoint RBI.
- Internet connectivity is required for setting up Forcepoint RBI and for browsing through Forcepoint RBI.
- For final deployment, the actual resource requirements are calculated based on the *Sizing Guide* and on the following:
  - User concurrency
  - Internet usage pattern
- The hardware specification requirement for production deployment will be in accordance with the *Sizing Guide*. Check the *Sizing Guide* details with your administrator or a Forcepoint representative for details on the resources required and number of VMs required for installing and configuring the Forcepoint RBI. The resource requirements are calculated based on the following:
  - User concurrency
  - Internet usage pattern
- The wildcard entry of the Forcepoint RBI base domain is to be bypassed (set exception) in the end user proxy settings.
- According to the *Sizing Guide*, RBI consists of the following components:

Admin Portal	RBC Cluster	RBI Proxy**
Master	Master	Proxy
Worker	Worker-RBC	
	Worker-File Scanning	
	Worker-Control Plane	

  ** RBI Proxy is applicable only in case of Proxy chaining.
- The Master and Worker for the respective cluster (Control Center and RBC) should be hosted in the same LAN segment. The Master and Workers should have no protocol or port restrictions.

Network communication requirements

Forcepoint RBI communicates with the endpoint using WebSocket on custom ports. This section shows the ports that needs to be opened for communication with Forcepoint RBI.

Connection	Required ports / URL
Endpoint machine to Forcepoint RBI Control Center Cluster	tcp 443 (Session initialization)
Endpoint machine to Forcepoint RBI RBC Cluster (including all RBC worker nodes).	tcp 443 (Session initialization) tcp 30000 – 32767 (Secure WebSocket connection (WSS) for Remote Browsing container)

Connection	Required ports / URL
Forcepoint RBI Cluster Communication (Control Center Cluster to RBC Cluster)	tcp 443 (RBI cluster communication)
Internet access to Forcepoint RBI Cluster (RBC Cluster to Internet)	tcp 443 (Internet access to RBC Cluster) tcp “Proxy IP & Proxy Port” (Proxy IP and Proxy port in case Internet access is provisioned through Enterprise Proxy.)
Terminal access (Admin user to Forcepoint RBI instances)	tcp 2200
Forcepoint Web Security Gateway/Proxy settings	Add base domain wildcard (e.g., *.rbi.forcepoint.com) to bypass list in end user Proxy settings.
CDR Service: API call to CDR service from Forcepoint RBI	tcp 80, 443 (destination *.threat-removal.deep-secure.com)
FTIS Service: API call to FTIS service from Forcepoint RBI	tcp 80, 443 (destination *. cloud.threatseeker.com)
Endpoint machine to LB (Admin and RBC)	443
Admin Portal LB to RBC LB	443
LB (Admin and RBC) to Masters	443
All VM's (Admin and RBC) to External NFS Server	tcp 2049 and udp 2049
All VM's (Admin and RBC) to External NFS Server (Portmapper Service)	tcp 111 and udp 111
Opscenter URL	https://opsportal.rbi.qa.forcepoint.com

Chapter 2

Deploying Forcepoint RBI

Contents

This chapter provides the instructions for deploying Forcepoint RBI in an on-premises environment.

Note

- Read the *Sizing Guide* for the hardware resources required for each VM component before beginning the deployment.
- The VMs and resources are to be provisioned based on the sizing exercise conducted to determine the total number of hardware resources (vCPU, Memory, Disk) needed. The *Sizing Guide* provides the total number of resources required as well resources required for each RBI component.
  - The maximum vCPU per VM/Physical server for Worker (for both Core and RBC) should be 64 vCPU.
  - The minimum vCPU per VM/Physical server for Worker (for both Core and RBC) should be 32 vCPU.

Based on a sample sizing, here is an illustration of the number of virtual machines required for each component:

	Admin Portal		RBC Cluster				RBI Proxy**	Final Total
	Master	Worker	Master	Worker-RBC*	Worker-File Scanning*	Worker-Control Plane*	Proxy	
vCPUs	20	36	20	1024	36	20	24	1180
Memory	80	144	80	4096	144	80	96	4720
Storage SSD (in GB)	40	180	40	1280			40	1580
DB Storage SSD (in GB)								
No.of Vms (64 vCPU each VM)	1 vm/20 vCPUs	1 vm/36 vCPUs	1 vm/20 vCPUs	16 vms/64 vCPU each	1 vm/36 vCPUs	1 vm/20 vCPUs	1 vm/24 vCPUs	
No.of Vms (32 vCPU each VM)	1 vm/20 vCPUs	1 vm/36 vCPUs	1 vm/20 vCPUs	32 vms/32 vCPU each	1 vm/36 vCPUs	1 vm/20 vCPUs	1 vm/24 vCPUs	

* During the RBI setup, specify the respective component name, that is *rbc*, *Control_plane*, or *File_scanning* in the **RBC Cluster Worker** section in the `cluster.yaml` file so that the respective labels are applied to the workers.

** RBI Proxy is applicable only in case of Proxy chaining, not applicable for URL based redirection.

- Provision the number of VMs as per the RBI sizing guide and after you have conducted the RBI sizing exercise.
- After all of the VMs are configured with IP addresses, proceed with the RBI setup.

Deploy Forcepoint RBI

This topic provides the procedure for deploying Forcepoint RBI in on-premises environments. Before deploying Forcepoint RBI, obtain the ISO from Forcepoint.

Steps

1) Install and deploy the Forcepoint RBI ISO obtained from Forcepoint.

2) Each Forcepoint RBI instance/VM is to be setup using the same ISO.

3) After the VM is ready, SSH to the VM using port 2200 with the login credentials (Username: maint Password: 7txaIJ3oko), and assign the static IP address to the VM.

Note

Keep a copy of the IP address, Netmask, Gateway, and DNS details. You will need these details later.

4) Set the IP addresses and network details:

   a) Open a command prompt or terminal and run the following two commands:

```
# cd scripts
# sudo ./setip.sh
```

```
maint@prod-kubemaster-1:~$ cd scripts
maint@prod-kubemaster-1:~/scripts$ sudo su
root@prod-kubemaster-1:/home/maint/scripts# ./setip.sh
```

   b) Select **interface 1** or the serial number against the interface name connected to the virtual network, then press **Enter**.

   c) For **Do you want to use DHCP for this interface (y/n)**, type **n**, then press **Enter**. (Please set the static IP address)

   d) Enter the **IP Address** (for example, **192.168.2.201**), then press **Enter**. (Please select your IP address)

   e) Enter the **Subnet mask** (for example, **255.255.255.0**), then press **Enter**. (Please select your subnet mask)

   f) Enter the **Gateway** (for example, **192.168.2.1**), then press **Enter**. (Please select your gateway)

g) Enter the **DNS IP** (for example, **8.8.8.8**), then press **Enter**. If you are entering multiple DNS IP addresses, separate the IP addresses with commas. (Please select your DNS)

h) Repeat these steps on all required VMs.

5) Verify the IP address with the following command:

```
ip a
```

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b9:ea:d8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.201/24 brd 192.168.2.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fd15:4ba5:5a2b:1002:20c:29ff:feb9:ead8/64 scope global tentative mngtmpaddr dynamic
       valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::20c:29ff:feb9:ead8/64 scope link
       valid_lft forever preferred_lft forever
```

6) Shut down the VM, then start the VM again.

```
sudo shutdown -h now
```

Note

- Make sure all the VMs required for the RBI components are created before you proceed with RBI setup and installation.
- Note down the IP address of all the VMs in a spread sheet.
- To relate the VMs to the RBI components, tag the respective VMs against the respective RBI component.
- Use one of the primary VMs from the RBI Admin portal Master component to download the RBI deb package and run the setup.
- Before running the RBI setup, make sure all the VMs are powered ON and reachable via port 2200.

7) To SSH to the primary VM:

a) For Windows:

- Download the `iso.ppk` file that is provided by Forcepoint, and then do the key based SSH to the primary VM (Admin Portal Master VM) by using the Putty application with the port 2200 and the login credentials (Username:maint)

b) For Mac/Linux:

i) Download the `iso.key` file that is provided by Forcepoint, and run the following command to change the file permission:

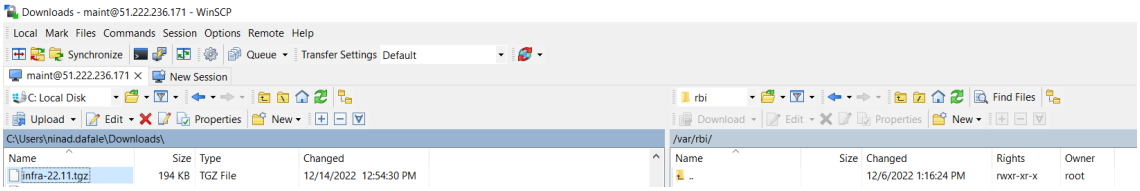
```
chmod 0400 <path of the iso.key>/iso.key
```

ii) To do the key based SSH to the primary VM (Admin Portal Master VM) using the port 2200 with the login credential (Username:maint), run the following command:

```
ssh -i <path of iso.key>/iso.key maint@<core_master_ip> -p 2200
```

8) Use key based WinSCP or key based scp to copy the archived infra file to Core master - `/var/rbi,` that is provided by Forcepoint.

For Windows:



- SSH to Core Master, then in the `/var/rbi` directory run the following command to untar the tar file:

```
tar -xf infra.tgz
```

For Mac/Linux:

- To copy the infra.tgz file to Core master IP, run the following command:

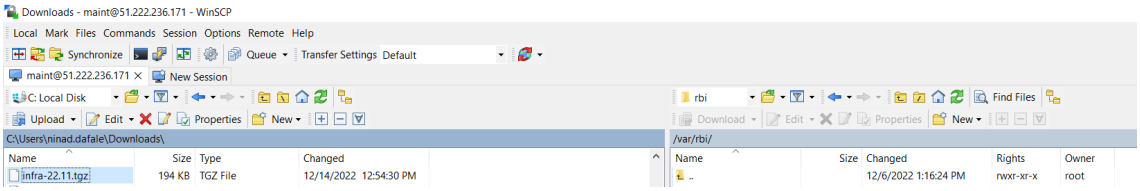
```
scp -r -i <path of iso.key>/iso.key -P 2200 infra.tgz maint@<core_master_ip>:/var/rbi/
```

- SSH to Core Master, then in the `/var/rbi` directory run the following command to untar the tar file:

```
tar -xf infra.tgz
```

9) Use key based WinSCP or key based scp to copy the mkauth file to Core master - `/var/rbi/infra/islasetup/keys/,` that is provided by Forcepoint.

For Windows:



For Mac/Linux:

- To copy the mkauth file to Core master IP, run the following command:

```
scp -r -i <path of iso.key>/iso.key -P 2200 mkauth maint@<core_master_ip>:/var/rbi/infra/
islasetup/keys/
```

10) To make the mkauth file executable, run the following command:

```
chmod +x /var/rbi/infra/islasetup/keys/mkauth
```

11) Update `/var/rbi/infra/islasetup/cluster.yaml` with the following required details:

```
nano /var/rbi/infra/islasetup/cluster.yaml
```

a) Add the client certificates.

```
kubernetes:
  certs:
    publickey: keys/fp.dev.crt
    privatekey: keys/fp.dev-domain.key
    ca: keys/fp.dev-CA.crt
```

Note

Use key based WinSCP or key based `scp` to copy the required certificate and key to `/var/rbi/infra/islasetup/keys`.

b) Add the Core master node 1 IP address (Admin Portal Master VM IP address):

```
masters:
- node: 1
  ip: 192.168.122.160
  sshport: 2200
  sshuser: maint
  reset: 0
  podsubnet: 10.244.0.0/16
```

Note

- The podsubnet defined is default and is used by Kubernetes for internal or interpod communication.
- It is recommended not to change the podsubnet unless there is a conflict with the subnet or network of your core masters or workers, RBC masters or workers, or end user network segment from where the user is accessing or browsing through RBI. The IP address of the master or worker is defined in the cluster.yaml file, and the IP address of the end user network must be different from that of the podsubnet network.
- In case, if you want to change the podsubnet because there is a conflict with your other subnet or network. It is must to configure a preferred subnet with /16 Classless Inter-Domain Routing (CIDR).

Note

For Single cluster Multi master setup (Core master IPs and RBC master IPs are same), or Multi cluster Multi master setup (Core master IPs and RBC master IPs are different). Also, do the following steps for RBC cluster in case of Multi cluster Multi master setup.

Prerequisites:

- It is recommend that you use your own Load Balancer. If you want to setup the RBI Load Balancer, then follow the below steps:

  i) Go to script placed in `/var/rbi/infra/islasetup/helperscripts/archive/loadbalancer.sh`

  ii) Run it on the server you want to configure as the Load Balancer in below format:

  ```
  ./loadbalancer.sh --ip lbip,master1_ip,matesr2_ip,master3_ip
  ```

- Three Master VM Nodes are required
  Perform the below steps in `cluster.yaml`

  i) Add the Load Balancer IP in `cluster.yaml`.

  ```
  loadbalancer:
    ip: "192.168.122.100"
  ```

  ii) Add two more Master node entries.

  ```
  masters:
  - node: 1
    ip: 192.168.122.220
    sshport: 2200
    sshuser: maint
    reset: 0
    podsubnet: 10.244.0.0/16
  - node: 2
    ip: 192.168.122.232
    sshport: 2200
    sshuser: maint
    reset: 0
    podsubnet: 10.244.0.0/16
  - node: 3
    ip: 192.168.122.188
    sshport: 2200
    sshuser: maint
    reset: 0
  ```

c) Add the Core worker node 1 IP address (Admin Portal Worker VM IP address):

```
workers:
- node: 1
  ip: 192.168.122.231
  sshport: 2200
  sshuser: maint
  reset: 0
```

If there are multiple workers, add entries for each worker (for example, from node to reset for each worker).

```
workers:
- node: 1
  ip: 192.168.122.186
  sshport: 2200
  sshuser: maint
  reset: 0
- node: 2
  ip: 192.168.122.200
  sshport: 2200
  sshuser: maint
  reset: 0
```

d) Add the RBC master node 1 IP address (RBC Cluster Master VM IP address):

```
masters:
- node: 1
  ip: 192.168.122.220
  sshport: 2200
  sshuser: maint
  reset: 0
  podsubnet: 10.244.0.0/16
```

Note

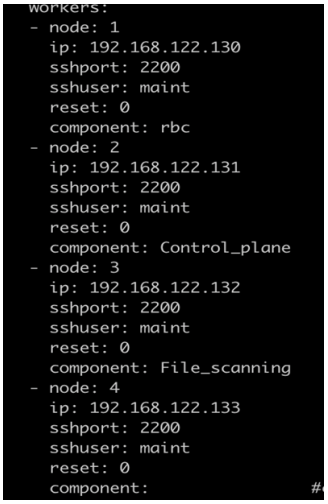
- In case of Multiple master setup, add 2 more master entries under RBC cluster.
- The podsubnet defined is default and is used by Kubernetes for internal or interpod communication.
- It is recommended not to change the podsubnet unless there is a conflict with the subnet or network of your core masters or workers, RBC masters or workers, or end user network segment from where the user is accessing or browsing through RBI. The IP address of the master or worker is defined in the cluster.yaml file, and the IP address of the end user network must be different from that of the podsubnet network.
- In case, if you want to change the podsubnet because there is a conflict with your other subnet or network. It is must to configure a preferred subnet with /16 Classless Inter-Domain Routing (CIDR).

```
rbc:
  masters:
  - node: 1
    ip: 192.168.122.41
    sshport: 2200
    sshuser: maint
    reset: 0
  - node: 2
    ip: 192.168.122.42
    sshport: 2200
    sshuser: maint
    reset: 0
  - node: 3
    ip: 192.168.122.43
    sshport: 2200
    sshuser: maint
    reset: 0
```

e) Add the RBC worker node 1 IP address (RBC Cluster Worker VM IP address):

```
workers:
- node: 1
  ip: 192.168.122.130
  sshport: 2200
  sshuser: maint
  reset: 1
  component:                #component can have values "rbc" or "Control_plane" or "File_scanning"
```

If there are multiple workers, add entries for each worker (for example, from node to reset for each worker).



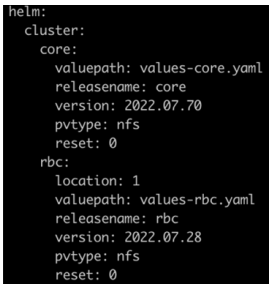
```
workers:
- node: 1
  ip: 192.168.122.130
  sshport: 2200
  sshuser: maint
  reset: 0
  component: rbc
- node: 2
  ip: 192.168.122.131
  sshport: 2200
  sshuser: maint
  reset: 0
  component: Control_plane
- node: 3
  ip: 192.168.122.132
  sshport: 2200
  sshuser: maint
  reset: 0
  component: File_scanning
- node: 4
  ip: 192.168.122.133
  sshport: 2200
  sshuser: maint
  reset: 0
  component:
```

Note

- During the RBI setup, specify the respective component name, that is *rbc*, *Control_plane*, or *File_scanning* for the **RBC Cluster Worker** node so that the respective labels are applied to the workers. If the component field is left blank, then all the component roles (*rbc*, *Control_plane*, and *File_scanning*) are applied to all RBC workers.

f) Add cluster information. For example:

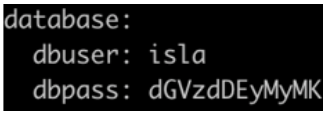
```
data:
                    core:
                        valuepath: values-on-prem.yaml ( File which needs to be used for
 helm core installation)
                        releasename: core (Name of the release for core)
                        version: default with the version that needs to be deployed
                        pvtype: nfs
                        reset: 0
                    rbc:
                        location: 1 ( Based on the region. USA = 1, UK = 2)
valuepath: values-on-prem.yaml ( File which needs to be used for helm rbc installation)
                        releasename: rbc (Name of the release for rbc)
                        version: default with the version that needs to be deployed
                        pvtype: nfs
                        reset: 0
```



Note

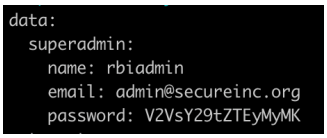
If the Core Master and RBC Master IP addresses are the same, then select **values-core-single.yaml** instead of **values-core.yaml** for core and select **values-rbc-single.yaml** instead of **values-rbc.yaml** for RBC.

g) Add database password (Default password is test123# encoded to base64).



h) Add super admin details under the data tag. For example:

```
data:
     superadmin:
           name: rbiadmin (This will become the superadmin url e.g. https://
rbiadmin.secureinc.org
          email: admin@secureinc.org (Administrators email address)
       password: Default password is “Welcome123#” encoded to base64.
```



i) Add tenant details under the data tag. For example:

```
tenants:
             host: rbi (This will become the tenant url e.g. https://rbi.secureinc.org
       proxychain: By default the value is set to 1. Set the value to 0, if RBI
                   proxy is not used as Parent proxy or proxy chaining.
                   In case of proxy chaining, leave it as 1.
        squidport: squidport is to be defined only if RBI is to be deployed in a
                   proxy chaining mode(as a parent proxy or upstreaming proxy to
                   Customer's existing proxy). For example, if you want to host
                   the RBI proxy on port 3134 then define 3134 against squidport.
                   Squid certificate needs to be installed on the customers
                   existing proxy(child proxy). Certificate can be found at
                   /home/maint/infra/islaproxy and file is squid-ca-cert-key.pem
                   Note: If you already have RBI deployed without RBI proxy and
                   want to deploy RBI proxy component only post RBI deployment
                   then edit the cluster.yaml file in the infra/islasetup directory,
                   specify the squid port, save the cluster.yaml file and then
                   run ./squid.sh cluster.yaml. This will install RBI proxy component.
                   Once the RBI proxy component is installed, the RBI proxy is
                   accessible on Core Clusters Master IP and the specified squidport
                   for example: 192.168.122.41:3134 (if the squidport specified as
                   3134 in cluster.yaml).
         icapport: for icap the default port is set to 1344. It is recommended not
                   to change the icap port unless you want to Integrate RBI with your
                   existing On-premises proxy with icap/icaps. To integrate RBI with
                   existing On-premises Proxy for icap/icaps based integration, ensure
                   that your existing proxy supports icap/icaps. To integrate with
                   icaps, define port 11344 in the cluster.yaml configuration, also
                   ensure to obtain the RBI ICAP Integration guide to configure your
                   On-premises proxy for icap/icaps based integration for RBI.
            email: admin@rbiinc.org (Administrators email address)
         password: Default password is "Welcome123#" encoded to base64.
```

```
  squidport: 3130
  proxychain: 0 ## 1 enable the proxy chain for squid / 0 enable the proxy mode for squid
  icapport: 1344  ##1344 or 11344
```

Note

Based on the selection for squidport and icapport, have the port open accordingly.

j) Add the IP address of the external NFS server in the **nfsserver** field, if you use an external NFS server. In case if you do not use an external NFS server leave the field empty.

```
nfsserver:              #Leave empty if you don't have external nfs server.
```

k) Add the tenant hostname in appliance-rbi:

```
appliances:
- name: appliance-rbi
  tenanthost: rbi
  minnodes: 2
  maxnodes: 2
  racversion: ract-direct:r89-5.5.11
  racurl: https://rbc-cluster-down.fp.dev
```

l) Add the **rac-url** (RBI server url) in **appliances-racurl**. Also, based on the license, modify the **minnodes** and **maxnodes**. For example, if the license is for 1,000 sessions, then minnodes can be 100 and maxnodes can be 1000.

```
  minnodes: 2
  maxnodes: 2
  racversion: ract-direct:beta-92-6.0.3
  racurl: rbc-cluster-gg.fp.dev
```

m) To add additional custom or self-signed root certificate authority to a remote browser container, add the custom CA certificates in the `/var/rbi/infra/islasetup/keys/racCA` folder. Also, specify the names of the certificates under the **racca** section, in the `cluster.yaml` file.

```
racca:
  - forcepoint.com-CA.crt
  - fp.dev-CA.crt
  - fp-rbi-go4labs-net-CA.crt
```

Note

i) If there are multiple CA certificates that needs to be added, specify it serially as displayed in the image above.

ii) All the unencrypted CA certificates must be added in the `/var/rbi/infra/islasetup/keys/racCA` folder.

n) If the deployment happens behind the proxy, add the following details under the **Clientproxy** section:

```
Clientproxy
Cert: The path of client proxy certs, if applicable
IP: IP address of the client proxy
Port: Proxy port number
User: If proxy is user based authenticated, then add the user name
Password: If proxy is user based authenticated, then add the proxy password encoded to
 base64
```

```
env:
  clientproxy:
    cert: ""
    ip: 192.168.122.3130
    port: 8888
    user: user
    password: V2VsY29tZTEyMyM=
    bypass: fp.dev
```

Note

To do deployment behind the proxy, on the proxy set the SSL interception to **OFF**.

12) Run the **islasetup** from `/var/rbi/infra/islasetup`.

```
./islasetup cluster.yaml
```

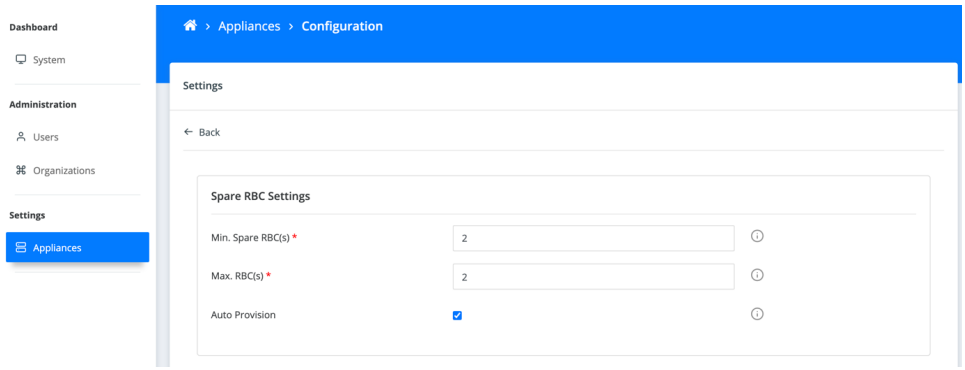
Note

- In case if you want to reset the deployment, consider the following points:
  - a) If the deployment is AllinOne (Core Master = Core Worker = RBC Master = RBC Worker), then set the **reset** value to 1 for Core Master, Core helm and RBC helm.
  - b) If you want to reset helm, then set the **reset** value to 1 for both the Core helm and RBC helm.
  - c) If the Core Master is not same, when compared to both the Core Worker and the RBC Master, then set the **reset** value to 1 for the Core Master, Core Worker, RBC Master, RBC Worker, Core helm and RBC helm.

13) Add the required host file entries in end user system if DNS is not added to the public domain. For example:

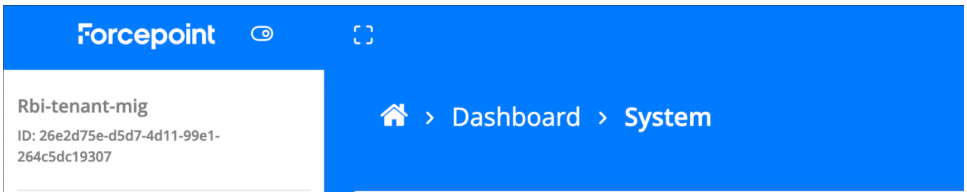
```
Core Master ip rbiadmin.secureinc.org rbi.secureinc.org
RBC Master ip rbi-cluster.secureinc.org
RBC Worker1 ip(say x.x.x.x) rbchost-x-x-x-x.secureinc.org
RBC Worker2 ip(say y.y.y.y) rbchost-y-y-y-y.secureinc.org
```

14) After the installation, sign in to the Forcepoint RBI superadmin portal and select **Auto Provision** under **Settings** > **Appliances**.



15) Login to **Admin Portal** > **Accept the EULA** > **Enter license key obtained from Forcepoint operations team.**

16) For anonymous browsing, the URL will be **https://<replace_With_tenant_url>/viewer/loader?tenantId=<replace_with_tenantid>&username=<replace_with_username>url=<replace_with_site_navigate>**. The Tenant ID can be found in the Forcepoint RBI Admin Portal.



Chapter 3

Post-deployment steps

Contents

As part of the post-deployment steps, this chapter discusses cipher implementation, and configuring SMTP.

Cipher implementation

This topic provides the procedure for implementing the Forcepoint-approved ciphers.

Steps

1) SSH to the Core Master and edit kubelet config.yaml:

```
sudo vim /var/lib/kubelet/config.yaml
```

2) Add the following content to the end of the file:

```
tlsCipherSuites: [TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384]
```

3) Restart kubelet.service:

```
sudo systemctl restart kubelet.service
```

4) Edit kube-apiserver.yaml:

```
sudo vim /etc/kubernetes/manifests/kube-apiserver.yaml
```

5) Add the following content at the end of the **Command** section:

```
- --tls-cipher-suites=TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

6) Check that the nodes are up:

```
kubectl get node
```

7) Repeat these cipher implementation steps for all Masters.

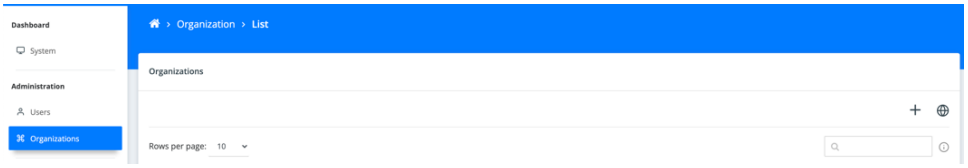
Configure SMTP

Simple Mail Transfer Protocol (SMTP) configuration enables email notifications to administrators through the Forcepoint RBI Portal.

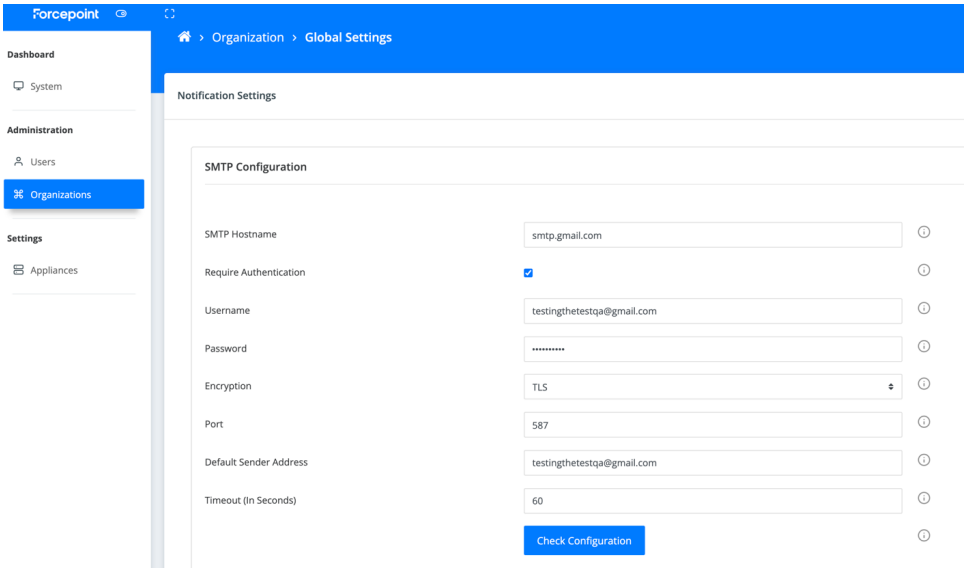
Steps

1) Sign in to the Forcepoint RBI superadmin portal and go to **Organizations**.

2) Click the globe icon to open Global Settings.



3) In **Global Settings**, enter the SMTP configuration shown in the following image:



4) Click **Check Configuration**. If the entered configuration settings are correct, then a **SMTP Configured Successfully** banner is shown at the top of the portal.

Note

If you are configuring a Gmail account to set up SMTP in the Control Center, then you need to enable **Less Secure App Access** under the account settings in Google.

Chapter 4

Upgrade and Rollback Process

Contents

This chapter provides information about the following processes:

- Upgrade Forcepoint RBI.
- Rollback Forcepoint RBI.

Upgrade Forcepoint RBI

This topic provides the procedure to upgrade Forcepoint RBI to the latest version in on-premises environment for the following:

- Upgrade Forcepoint RBI v22.08 to the latest available version
- Upgrade Forcepoint RBI v22.10 to the latest available version

Upgrade Forcepoint RBI v22.08 to the Latest Available Version

Steps

1) SSH to the Core Master.

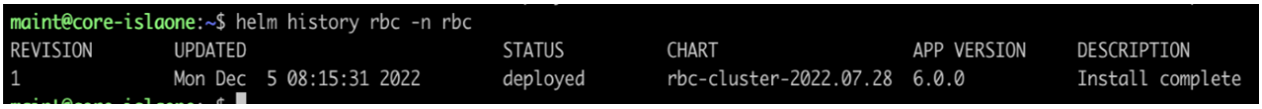
2) Validate the deployed version of the Forcepoint RBI:

   a) To validate the version of the core-cluster, run the following command:

```
helm history core -n core
```

   b) To validate the version of the rbc-cluster, SSH to RBC master, and then run the following command:

```
helm history rbc -n rbc
```



3) Download the latest infra package from the customer portal, and Winscp or scp the downloaded package to the /home/maint directory.

4) Rename the implemented infra package to infra_old_22.08. To rename run the following command:

```
mv infra/ infra_old_22.08
```

5) Run the following command to untar the latest infra package:

```
tar -xf infra.tgz
```

6) In the implemented `cluster.yaml` file, do the following (/home/maint/infra_old_22.08/islasetup directory):

   a) Copy the information in the **opscenter** section from the latest `cluster.yaml` file to the implemented `cluster.yaml` file.

   b) Copy the information in the **dbbackup** field under the **database** section from the latest `cluster.yaml` file to the **dbbackup** field under the **database** section in the implemented `cluster.yaml` file.

```
database:
  dbuser: isla
  dbpass: dGVzdDEyMyMK
  dbsync: 0
  dbbackup: /home/maint/dbbackup
```

   c) Replace the latest `cluster.yaml` file with the implemented `cluster.yaml` file in the latest infra package.

7) Copy the latest `mkauth` file to the rbc cluster master. To copy the `mkauth` file, run the following command.

```
scp -P 2200 home/maint/islasetup/keys/mkauth maint@<ip of rbc master>:~/.
```

8) Copy the `/home/maint/.islakube/valuecore.yaml` file to the `/home/maint/infra/islasetup` directory and rename the copied `valuecore.yaml` file to `values-core.yaml`.

> **Note**
>
> If the core master and rbc master IP addresses are same then rename the copied `valuecore.yaml` file to `values-core-single.yaml`.

9) Scp the `/home/maint/.islakube/valuerbc.yaml` file from Rbc Master to Core Master in the `/home/maint/infra/islasetup` directory and rename the copied `valuerbc.yaml` file to `values-rbc.yaml`..

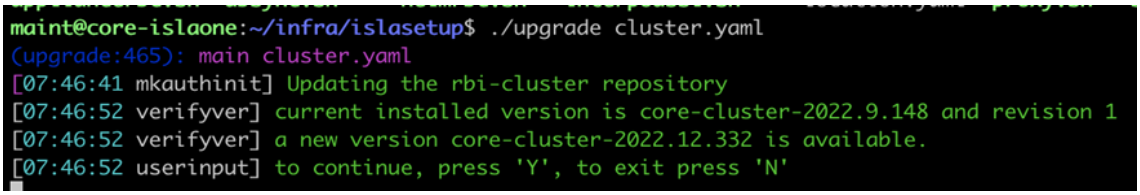
```
scp -P 2200 maint@<rbc master IP>:~/.islakube/valuerbc.yaml /home/maint/infra/islasetup/
```

> **Note**
>
> If the core master and rbc master IP addresses are same then rename the copied `valuerbc.yaml` file to `values-rbc-single.yaml`.

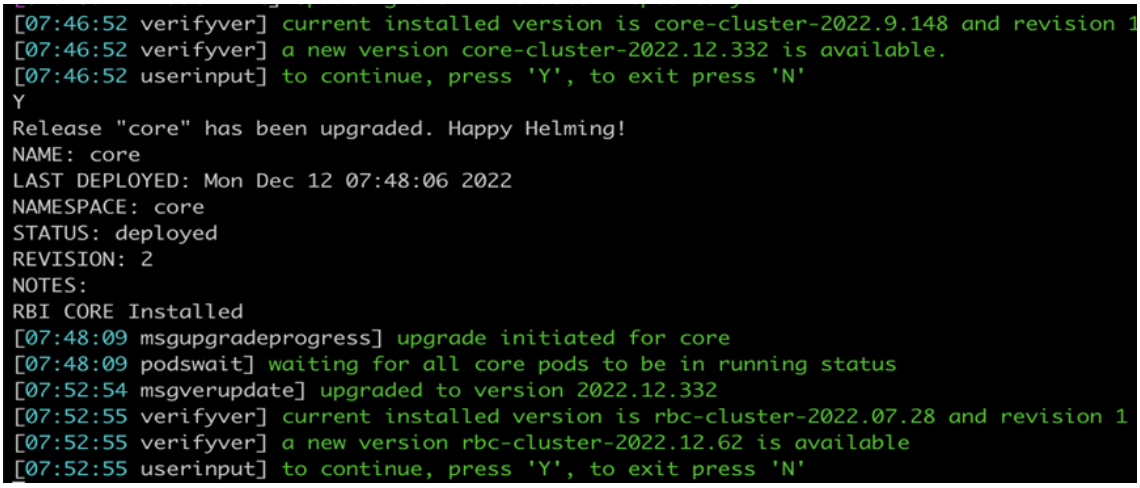
10) To initiate the upgrade process, run the following command from the latest infra package (`/home/maint/infra/islasetup directory`):

```
./upgrade cluster.yaml
```

11) Press **Y** to confirm the core-cluster upgrade, or press **N** to exit.



12) Press **Y** to confirm the rbc-cluster upgrade, or press **N** to exit.



13) After you confirm the rbc-cluster upgrade, immediately SSH to RBC master and run the following command:

```
./mkauth k8s rbc
```

```
maint@core-islaone:~/test/islasetup/keys$ ./mkauth k8s rbc
secret "rbi-jfrog-registry-key" deleted
k8s:rbc:Ok
```

14) Wait for the upgrade process to complete. Once the upgrade process is completed successfully, output similar to the following is displayed.

```
maint@core-islaone:~/infra/islasetup$ ./upgrade cluster.yaml
(upgrade:465): main cluster.yaml
[07:46:41 mkauthinit] Updating the rbi-cluster repository
[07:46:52 verifyver] current installed version is core-cluster-2022.9.148 and revision 1
[07:46:52 verifyver] a new version core-cluster-2022.12.332 is available.
[07:46:52 userinput] to continue, press 'Y', to exit press 'N'
Y
Release "core" has been upgraded. Happy Helming!
NAME: core
LAST DEPLOYED: Mon Dec 12 07:48:06 2022
NAMESPACE: core
STATUS: deployed
REVISION: 2
NOTES:
RBI CORE Installed
[07:48:09 msgupgradeprogress] upgrade initiated for core
[07:48:09 podswait] waiting for all core pods to be in running status
[07:52:54 msgverupdate] upgraded to version 2022.12.332
[07:52:55 verifyver] current installed version is rbc-cluster-2022.07.28 and revision 1
[07:52:55 verifyver] a new version rbc-cluster-2022.12.62 is available
[07:52:55 userinput] to continue, press 'Y', to exit press 'N'
Y
Release "rbc" has been upgraded. Happy Helming!
NAME: rbc
LAST DEPLOYED: Mon Dec 12 07:56:05 2022
NAMESPACE: rbc
STATUS: deployed
REVISION: 2
NOTES:
Deployed RBI rbc
[07:56:08 msgupgradeprogress] upgrade initiated for rbc
[07:56:09 podswait] waiting for all rbc pods to be in running status
[07:59:32 msgverupdate] upgraded to version 2022.12.62
(upgrade:466): set +x
```

Note

If the upgrade fails, do not proceed to next steps and manually initiate the rollback process. For more information on rollback process, refer to the **Rollback Forcepoint RBI to the last Implemented 22.08 version** section.

15) After the upgrade process is completed successfully, validate the upgraded version of the Forcepoint RBI:

- To validate the version of the core-cluster, run the following command:

```
helm history core -n core
```

```
maint@core-islaone:~/infra/islasetup$ helm history core -n core
REVISION        UPDATED                         STATUS          CHART                           APP VERSION     DESCRIPTION
1               Mon Dec  5 08:09:04 2022        superseded      core-cluster-2022.9.148         6.0.0           Install complete
2               Mon Dec 12 07:48:06 2022        deployed        core-cluster-2022.12.332        6.0.0           Upgrade complete
maint@core-islaone:~/infra/islasetup$
```

- To validate the version of the rbc-cluster, SSH to RBC Master, and then run the following command:

```
helm history rbc -n rbc
```

```
maint@core-islaone: ~/test/islasetup/keys (ssh)
maint@core-islaone:~/test/islasetup/keys$ helm history rbc -n rbc
REVISION        UPDATED                         STATUS          CHART                   APP VERSION     DESCRIPTION
1               Mon Dec  5 08:15:31 2022        superseded      rbc-cluster-2022.07.28  6.0.0           Install complete
2               Mon Dec 12 07:56:05 2022        deployed        rbc-cluster-2022.12.62  6.0.0           Upgrade complete
```

16) Update the rac version information. For more information on how to update the rac version, refer to the **Update the RAC Version** section.

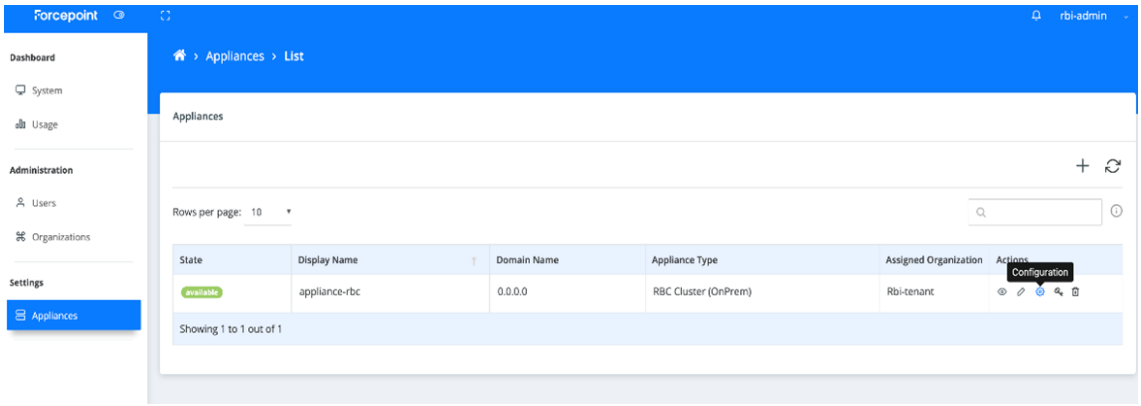
Update the RAC Version

To update the rac version, do the following:

Steps

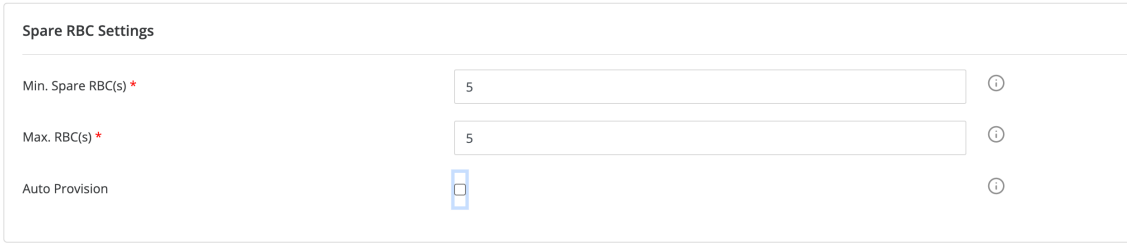
1) Sign-in to the **Forcepoint RBI Super Admin Portal**.

2) Go to the **Settings** > **Appliances** page.

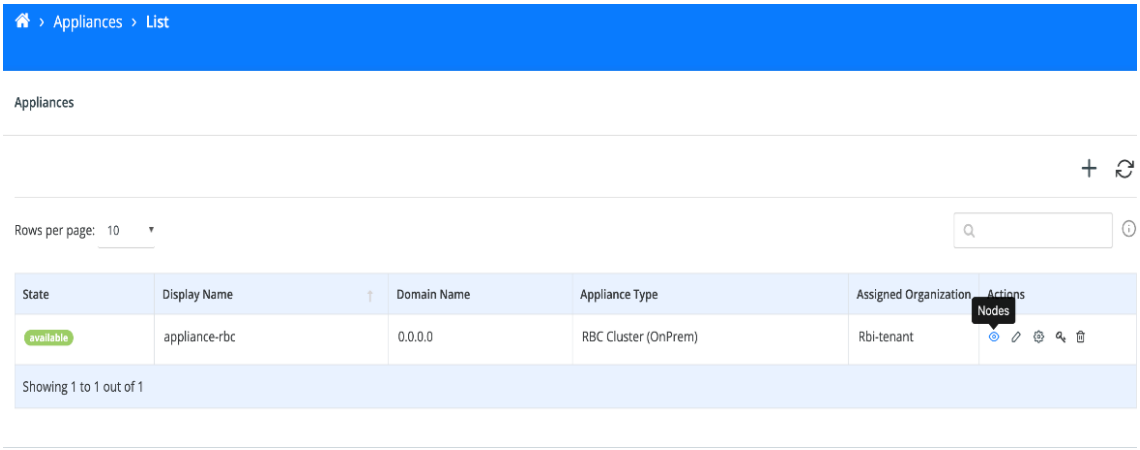


3) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

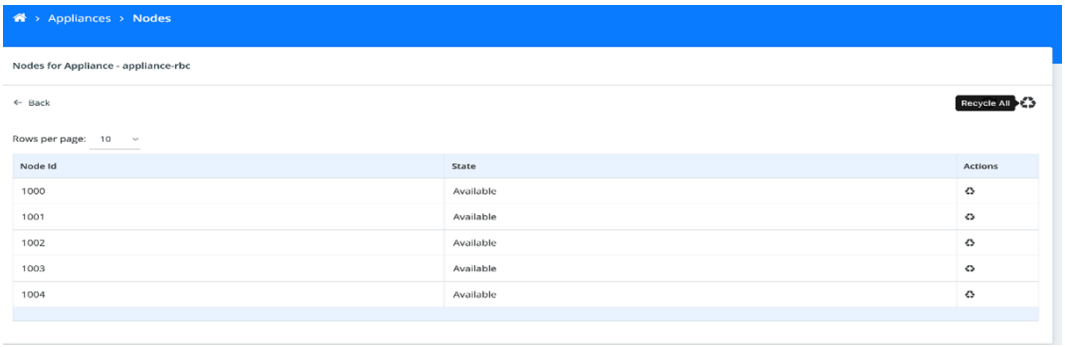
4) Clear the **Auto Provision** checkbox, and then click the **Save** button.



5) Go to the **Appliances** page, and then for the rbc cluster click the **Nodes** icon in the **Actions** column.



6) On the **Nodes** page, click the **Recycle All** icon.



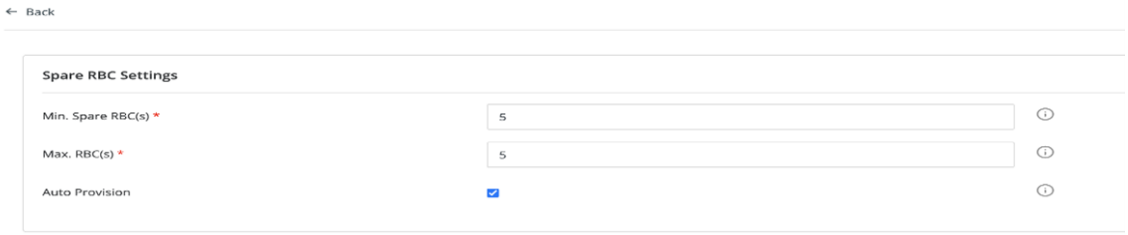
Note

Verify that the state of all nodes has changed to **Offline** from **Available**.

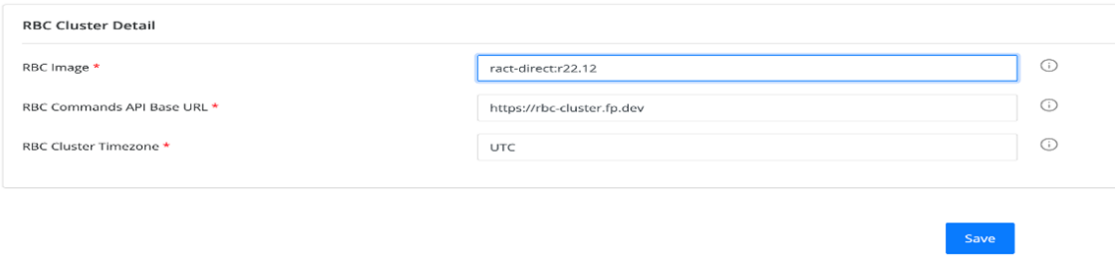
7) Go to the **Appliances** page.

8) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

9) Check the **Auto Provision** checkbox.



10) Under **RBC Cluster Detail**, update the rac version to *ract-direct:r22.12* in the **RBC Image** field.



11) Click the **Save** button.

Upgrade Forcepoint RBI v22.10 to the Latest Available Version

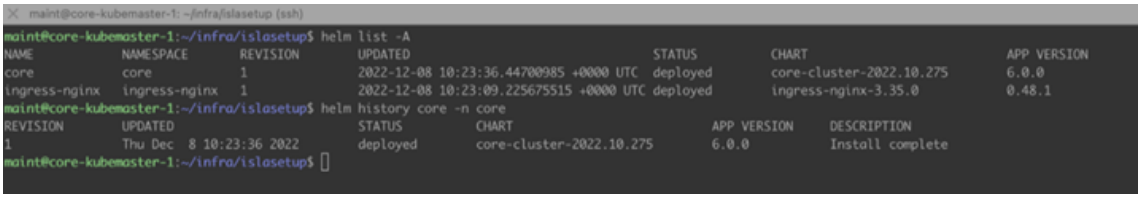
Steps

1) SSH to the Core Master.

2) Validate the deployed version of the Forcepoint RBI:

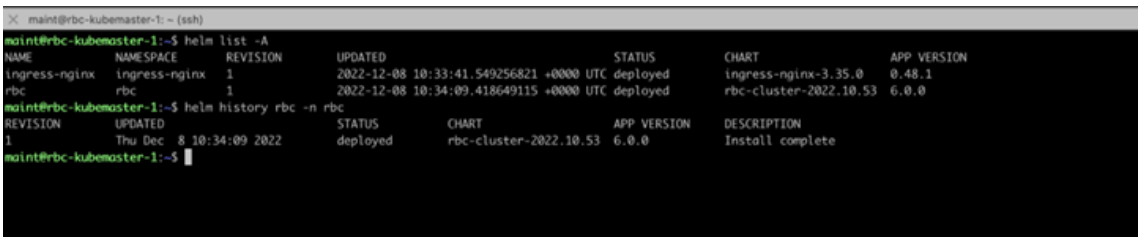
a) To validate the version of the core-cluster, run the following command:

```
helm history core -n core
```



b) To validate the version of the rbc-cluster, SSH to RBC master, and then run the following command:

```
helm history rbc -n rbc
```



3) Download the latest infra package from the customer portal, and Winscp or scp the downloaded package to the /home/maint directory.

4) Rename the implemented infra package to infra_old_22.10. To rename run the following command:

```
mv infra/ infra_old_22.10
```

5) Run the following command to untar the latest infra package:

```
tar -xf infra.tgz
```

6) In the implemented `cluster.yaml` file, do the following (`/home/maint/infra_old_22.10/islasetup` directory):

   a) Copy the information in the **opscenter** section from the latest `cluster.yaml` file to the implemented `cluster.yaml` file.

```
opscenter:
  opsurl: "opsportal.rbi.qa.forcepoint.com"
  opsip: "3.108.136.139"
  opskey: "T1RNd05XSm1ZV010WVdGbU9TMDBZV00xTFRsa09Ea3RNamxtTW1GbU16ZGpaamxsLjU4MzFiZjY0YTVjM2FhODlmOGEwZTRkNTIxNjlkMTQ2NWQzNDAzMzEzZTI2ZTNiMTNiZDBlMzVhYjE5NTE4ZjYK"
```

   b) Copy the information in the **dbbackup** field under the **database** section from the latest `cluster.yaml` file to the **dbbackup** field under the **database** section in the implemented `cluster.yaml` file.

```
database:
  dbuser: isla
  dbpass: dGVzdDEyMyMK
  dbsync: 0
  dbbackup: /home/maint/dbbackup
```

   c) Replace the latest `cluster.yaml` file with the implemented `cluster.yaml` file in the latest infra package.

7) Copy the `/home/maint/.islakube/valuecore.yaml` file to the `/home/maint/infra/islasetup` directory and rename the copied `valuecore.yaml` file to `values-core.yaml`.

> **Note**
>
> If the core master and rbc master IP addresses are same then rename the copied `valuecore.yaml` file to `values-core-single.yaml`.

8) Scp the `/home/maint/.islakube/valuerbc.yaml` file from Rbc Master to Core Master in the `/home/maint/infra/islasetup` directory and rename the copied `valuerbc.yaml` file to `values-rbc.yaml`..

```
scp -P 2200 maint@<rbc master IP>:~/.islakube/valuerbc.yaml /home/maint/infra/islasetup/
```

> **Note**
>
> If the core master and rbc master IP addresses are same then rename the copied `valuerbc.yaml` file to `values-rbc-single.yaml`.

9) To initiate the upgrade process, run the following command from the latest infra package (`/home/maint/infra/islasetup` directory):

```
./upgrade cluster.yaml
```

10) Press **Y** to confirm the core-cluster upgrade, or press **N** to exit.

```
maint@core-kubemaster-1:~/infra/islasetup$ ./upgrade cluster.yaml
(upgrade:465): main cluster.yaml
[11:36:21 mkauthinit] Updating the rbi-cluster repository
[11:36:33 verifyver] current installed version is core-cluster-2022.10.275 and revision 1
[11:36:33 verifyver] a new version core-cluster-2022.12.332 is available.
[11:36:33 userinput] to continue, press 'Y', to exit press 'N'
```

11) Press **Y** to confirm the rbc-cluster upgrade, or press **N** to exit.

```
maint@core-kubemaster-1:~/infra/islasetup$ ./upgrade cluster.yaml
(upgrade:465): main cluster.yaml
[11:36:21 mkauthinit] Updating the rbi-cluster repository
[11:36:33 verifyver] current installed version is core-cluster-2022.10.275 and revision 1
[11:36:33 verifyver] a new version core-cluster-2022.12.332 is available.
[11:36:33 userinput] to continue, press 'Y', to exit press 'N'
Y
Release "core" has been upgraded. Happy Helming!
NAME: core
LAST DEPLOYED: Thu Dec  8 11:37:30 2022
NAMESPACE: core
STATUS: deployed
REVISION: 2
NOTES:
RBI CORE Installed
[11:37:33 msgupgradeprogress] upgrade initiated for core
[11:37:33 podswait] waiting for all core pods to be in running status
[11:39:41 msgverupdate] upgraded to version 2022.12.332
[11:39:42 verifyver] current installed version is rbc-cluster-2022.10.53 and revision 1
[11:39:43 verifyver] a new version rbc-cluster-2022.12.62 is available
[11:39:43 userinput] to continue, press 'Y', to exit press 'N'
```

12) Wait for the upgrade process to complete. Once the upgrade process is completed successfully, output similar to the following is displayed.

```
maint@core-islaone:~/infra/islasetup$ ./upgrade cluster.yaml
(upgrade:465): main cluster.yaml
[07:46:41 mkauthinit] Updating the rbi-cluster repository
[07:46:52 verifyver] current installed version is core-cluster-2022.9.148 and revision 1
[07:46:52 verifyver] a new version core-cluster-2022.12.332 is available.
[07:46:52 userinput] to continue, press 'Y', to exit press 'N'
Y
Release "core" has been upgraded. Happy Helming!
NAME: core
LAST DEPLOYED: Mon Dec 12 07:48:06 2022
NAMESPACE: core
STATUS: deployed
REVISION: 2
NOTES:
RBI CORE Installed
[07:48:09 msgupgradeprogress] upgrade initiated for core
[07:48:09 podswait] waiting for all core pods to be in running status
[07:52:54 msgverupdate] upgraded to version 2022.12.332
[07:52:55 verifyver] current installed version is rbc-cluster-2022.07.28 and revision 1
[07:52:55 verifyver] a new version rbc-cluster-2022.12.62 is available
[07:52:55 userinput] to continue, press 'Y', to exit press 'N'
Y
Release "rbc" has been upgraded. Happy Helming!
NAME: rbc
LAST DEPLOYED: Mon Dec 12 07:56:05 2022
NAMESPACE: rbc
STATUS: deployed
REVISION: 2
NOTES:
Deployed RBI rbc
[07:56:08 msgupgradeprogress] upgrade initiated for rbc
[07:56:09 podswait] waiting for all rbc pods to be in running status
[07:59:32 msgverupdate] upgraded to version 2022.12.62
(upgrade:466): set +x
```

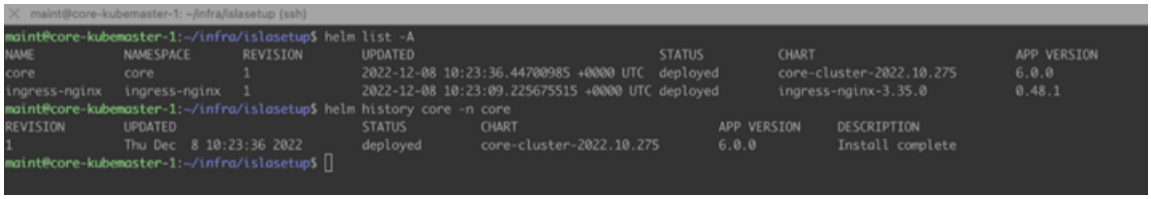
Note

If the upgrade fails, do not proceed to next steps and manually initiate the rollback process. For more information on rollback process, refer to the **Rollback Forcepoint RBI to the last Implemented 22.10 version** section.

13) After the upgrade process is completed successfully, validate the upgraded version of the Forcepoint RBI:

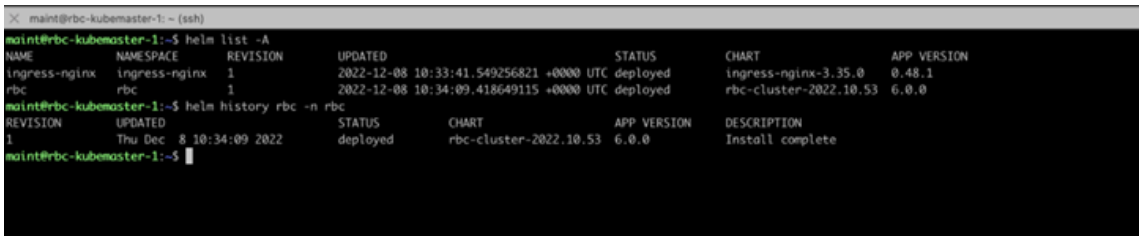
- To validate the version of the core-cluster, run the following command:

```
helm history core -n core
```



- To validate the version of the rbc-cluster, SSH to RBC Master, and then run the following command:

```
helm history rbc -n rbc
```



14) Update the rac version information. For more information on how to update the rac version, refer to the **Update the RAC Version** section.

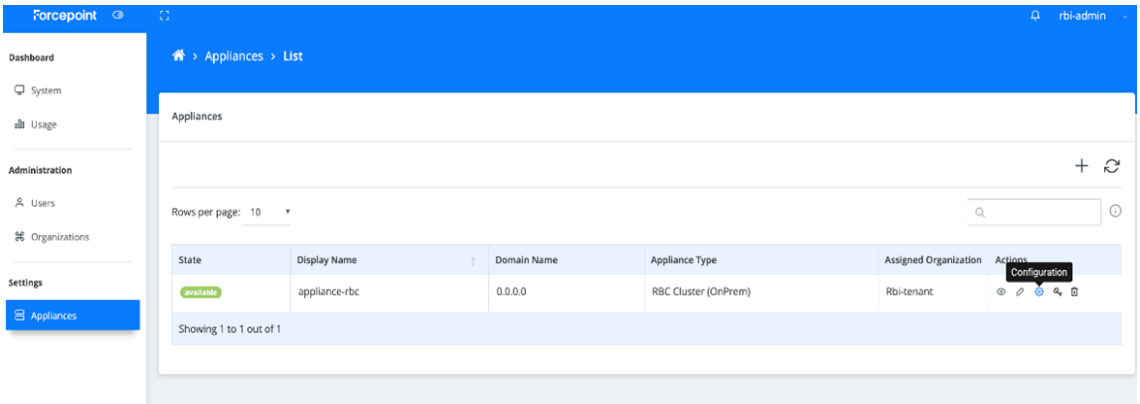
Update the RAC Version

To update the rac version, do the following:

Steps

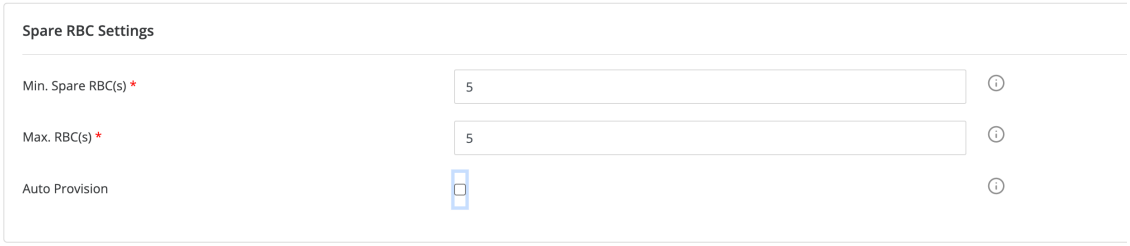
1) Sign-in to the **Forcepoint RBI Super Admin Portal**.

2) Go to the **Settings** > **Appliances** page.

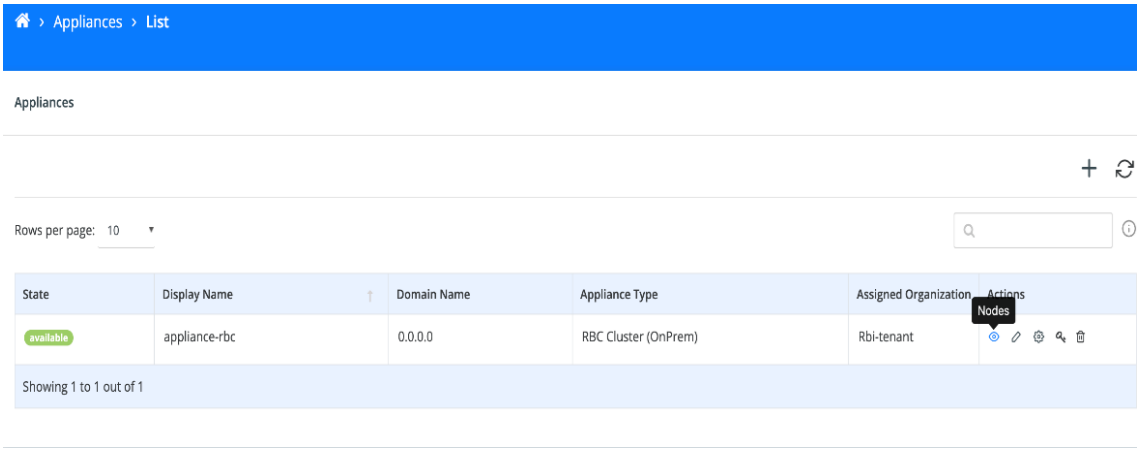


3) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

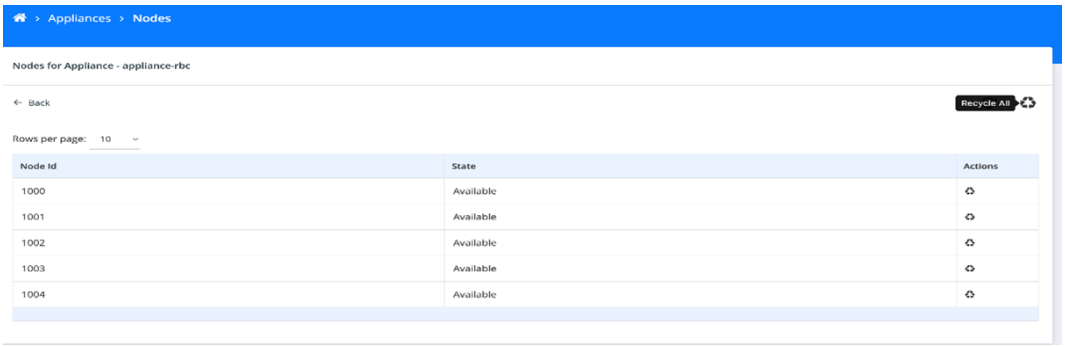
4) Clear the **Auto Provision** checkbox, and then click the **Save** button.



5) Go to the **Appliances** page, and then for the rbc cluster click the **Nodes** icon in the **Actions** column.



6) On the **Nodes** page, click the **Recycle All** icon.



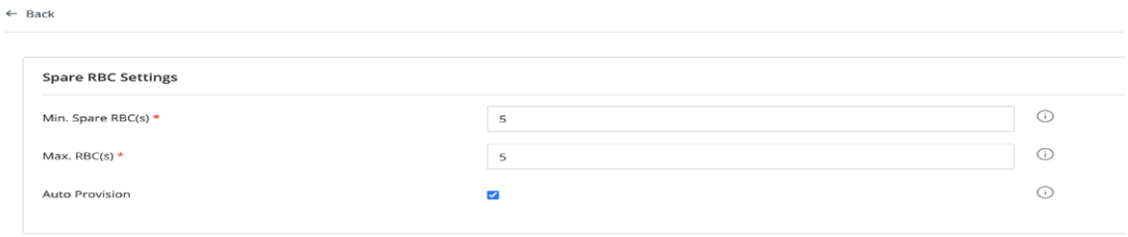
Note

Verify that the state of all nodes has changed to **Offline** from **Available**.

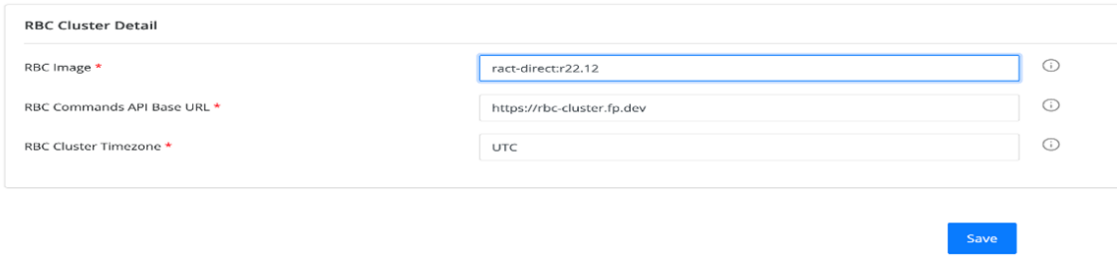
7) Go to the **Appliances** page.

8) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

9) Check the **Auto Provision** checkbox.



10) Under **RBC Cluster Detail**, update the rac version to *ract-direct:r22.12* in the **RBC Image** field.



11) Click the **Save** button.

Rollback Forcepoint RBI

This topic provides the procedure to rollback Forcepoint RBI to the last implemented version in the on-premises environment for the following:

- Rollback Forcepoint RBI to the last implemented 22.08 version
- Rollback Forcepoint RBI to the last implemented 22.10 version

Rollback Forcepoint RBI to the Last Implemented 22.08 Version

Steps

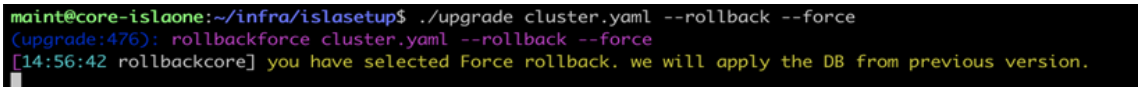
1) SSH to the RBC Master, and run the following command:

```
kubectl delete secrets -n rbc rbi-jfrog-registry-key
```

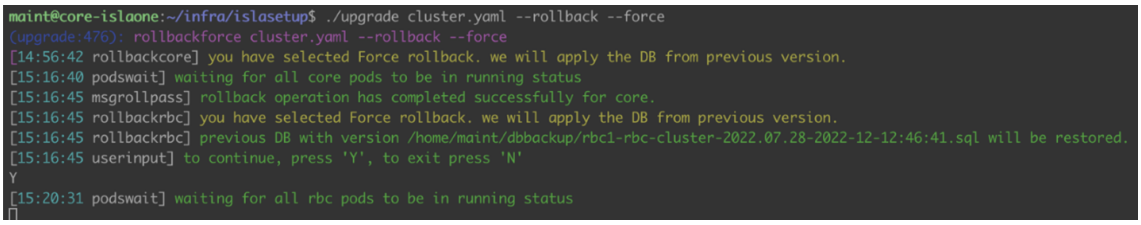
```
maint@core-islaone:~/infra/islasetup$ kubectl delete secrets -n rbc rbi-jfrog-registry-key
secret "rbi-jfrog-registry-key" deleted
```

2) To initiate the RBI rollback process, SSH to Core Master, and then run the following command from the Core master in the latest infra directory (`/home/maint/infra/islasetup`):

```
./upgrade cluster.yaml --rollback --force
```



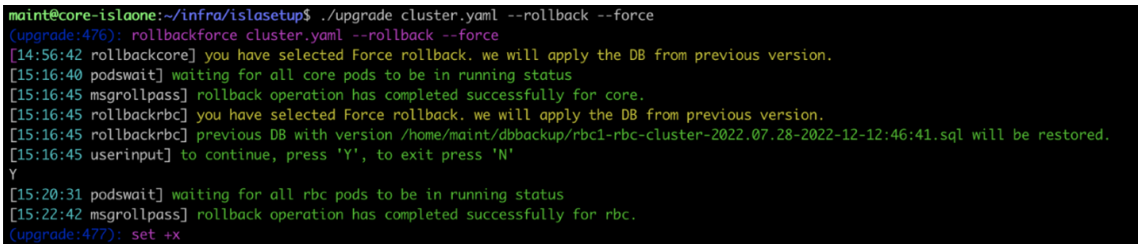
3) Press **Y** to confirm and continue, or press **N** to exit.



4) After you confirm the rollback process, immediately SSH to RBC master and run the following command:

```
./mkauth k8s rbc
```

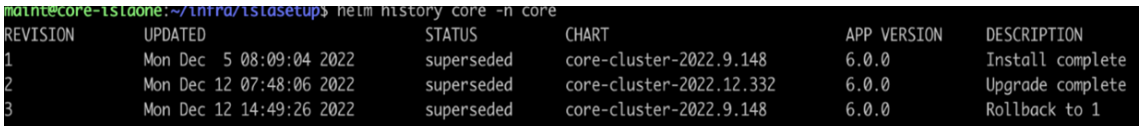
5) Wait for the rollback process to complete. Once the rollback process is completed successfully, output similar to the following is displayed.



6) After the rollback process is completed successfully, validate the rollbacked version of the Forcepoint RBI:

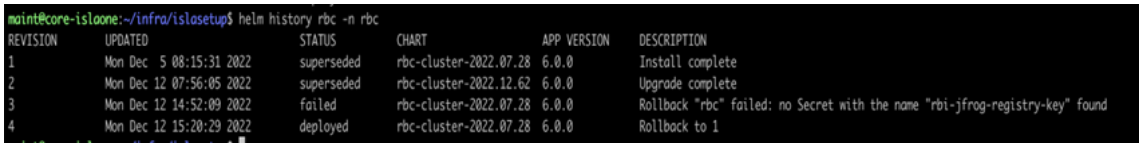
- To validate the version of the core-cluster, SSH to Core Master, and then run the following command:

  ```
  helm history core -n core
  ```

- To validate the version of the rbc-cluster, SSH to RBC Master, and then run the following command:

  ```
  helm history rbc -n rbc
  ```

7) Update the rac version information. For more information on how to update the rac version, refer to the **Rollback Forcepoint RBI v22.08 RAC Version update** section.

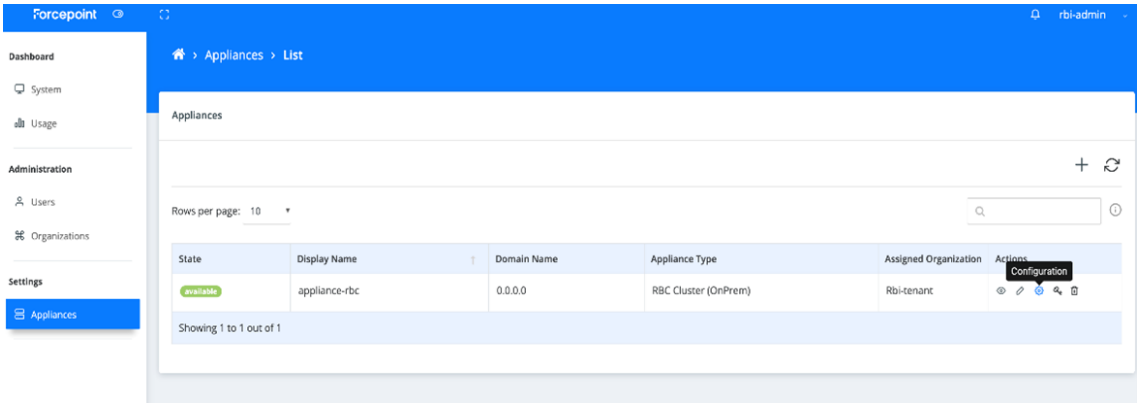
Rollback Forcepoint RBI v22.08 RAC version update

To update the rac version, do the following:

Steps

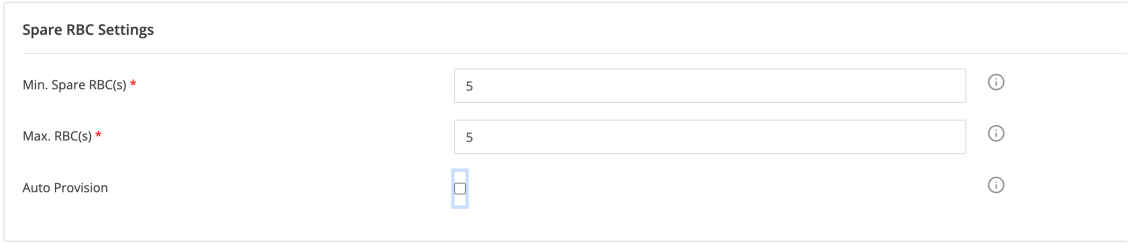
1) Sign-in to the **Forcepoint RBI Super Admin Portal**.

2) Go to the **Settings** > **Appliances** page.

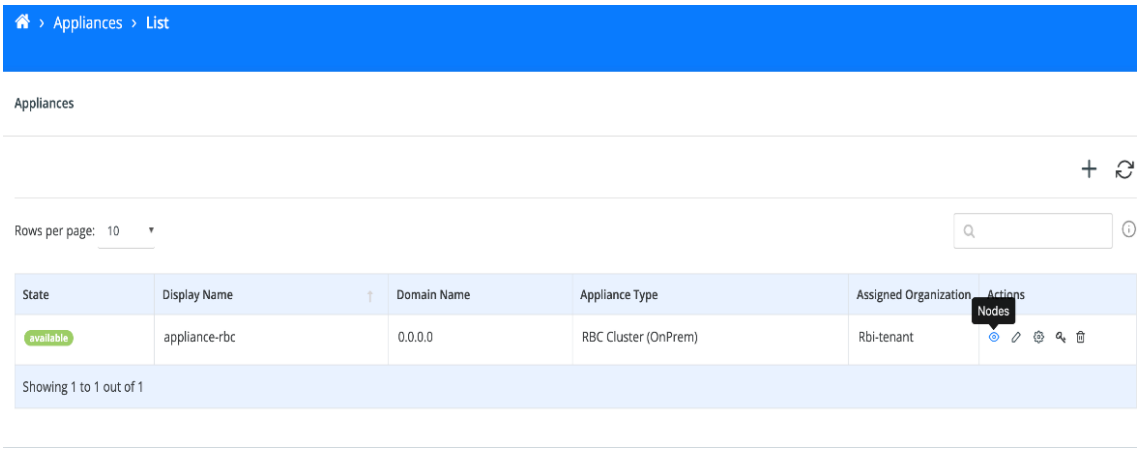


3) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

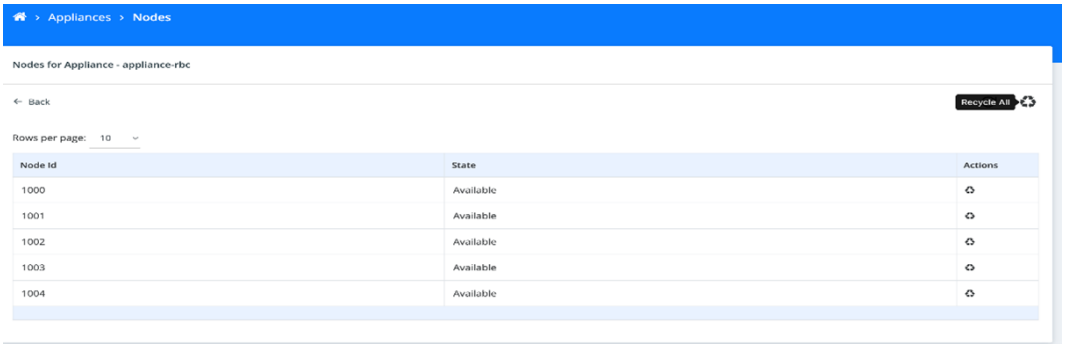
4) Clear the **Auto Provision** checkbox, and then click the **Save** button.



5) Go to the **Appliances** page, and then for the rbc cluster click the **Nodes** icon in the **Actions** column.



6) On the **Nodes** page, click the **Recycle All** icon.



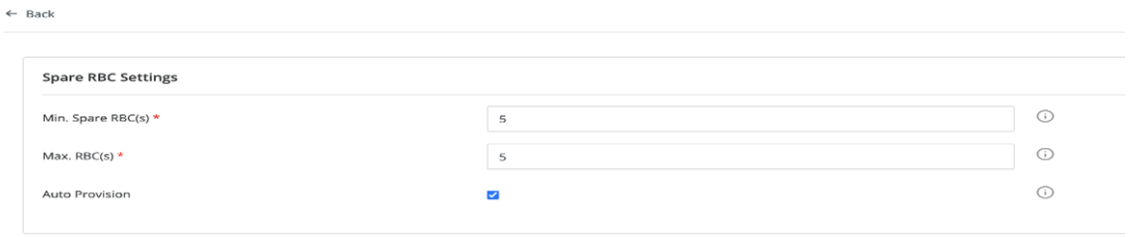
Note

Verify that the state of all nodes has changed to **Offline** from **Available**.

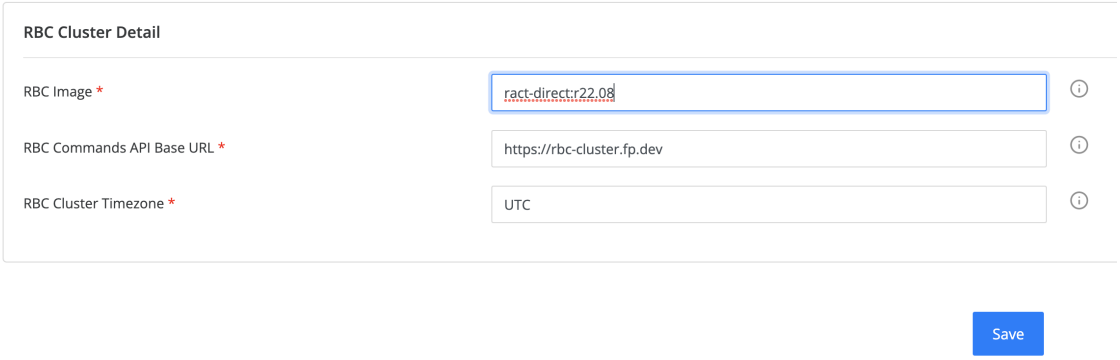
7) Go to the **Appliances** page.

8) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

9) Check the **Auto Provision** checkbox.



10) Under **RBC Cluster Detail**, update the rac version to *ract-direct:r22.08* in the **RBC Image** field.



11) Click the **Save** button.

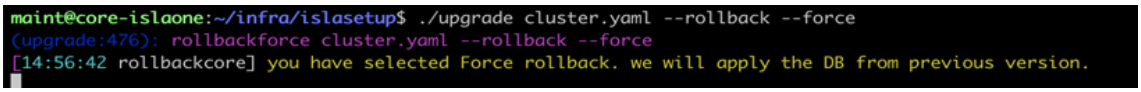
Rollback Forcepoint RBI to the Last Implemented 22.10 Version

Steps

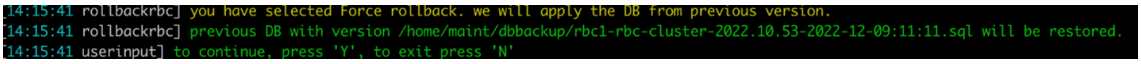
1) SSH to the Core Master.

2) To initiate the RBI rollback process, run the following command from the Core master in the latest infra directory (`/home/maint/infra/islasetup`):

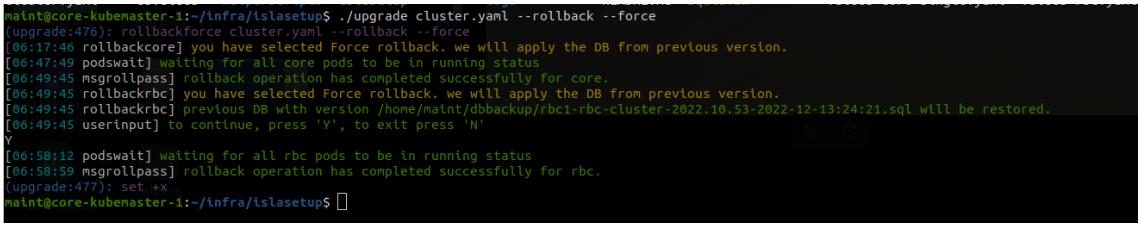
```
./upgrade cluster.yaml --rollback --force
```



3) Press **Y** to confirm and continue, or press **N** to exit.



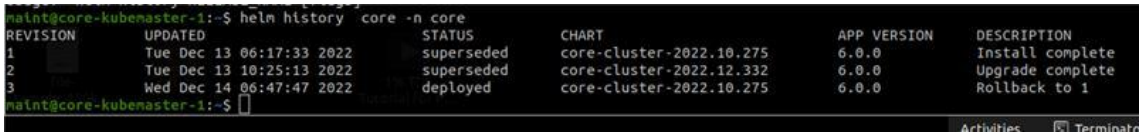
4) Wait for the rollback process to complete. Once the rollback process is completed successfully, output similar to the following is displayed.



5) After the rollback process is completed successfully, validate the rollbacked version of the Forcepoint RBI:

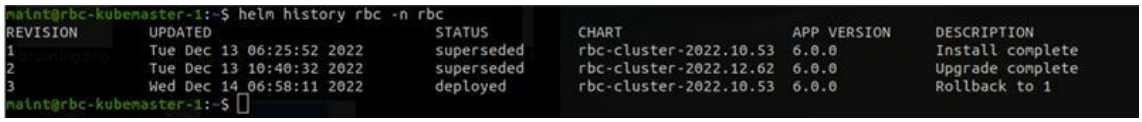
- To validate the version of the core-cluster, SSH to Core Master, and then run the following command:

```
helm history core -n core
```



- To validate the version of the rbc-cluster, SSH to RBC Master, and then run the following command:

```
helm history rbc -n rbc
```



6) Update the rac version information. For more information on how to update the rac version, refer to the **Rollback Forcepoint RBI v22.10 RAC Version Update** section.

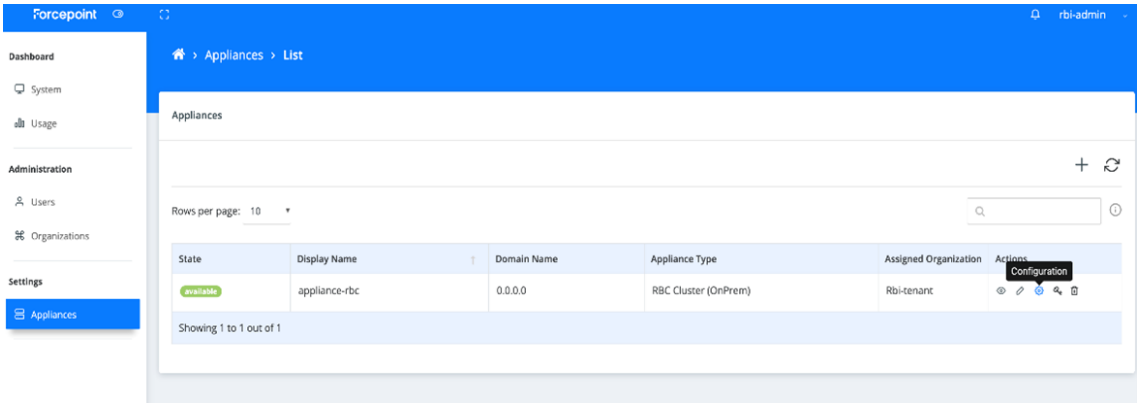
Rollback Forcepoint RBI v22.10 RAC version update

To update the rac version, do the following:

Steps

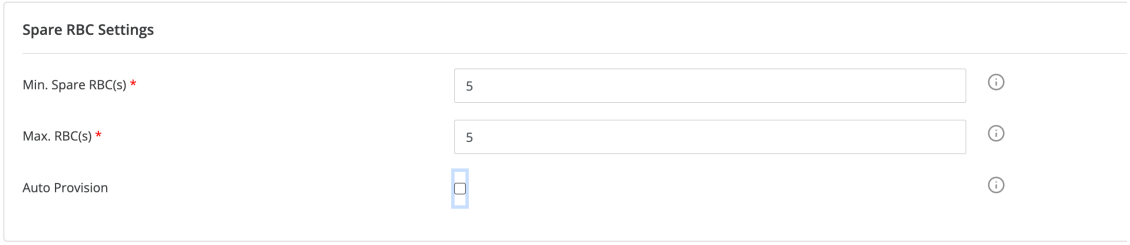
1) Sign-in to the **Forcepoint RBI Super Admin Portal**.

2) Go to the **Settings** > **Appliances** page.

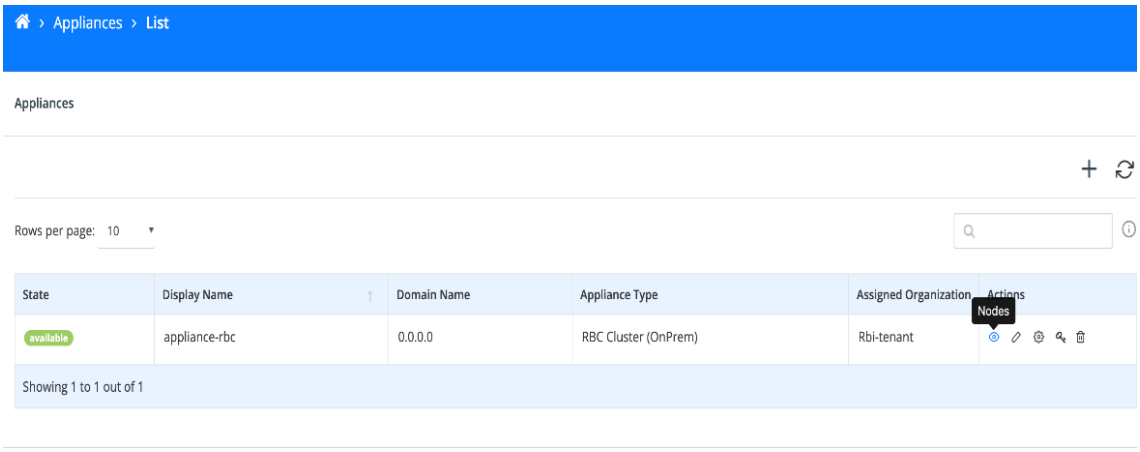


3) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

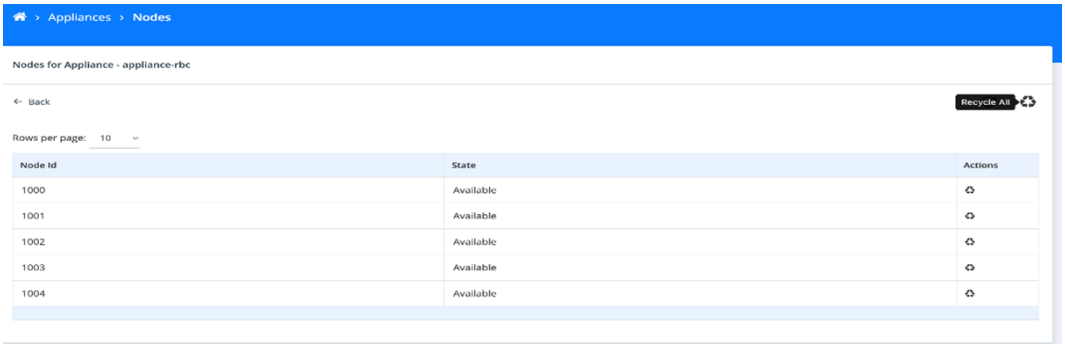
4) Clear the **Auto Provision** checkbox, and then click the **Save** button.



5) Go to the **Appliances** page, and then for the rbc cluster click the **Nodes** icon in the **Actions** column.



6) On the **Nodes** page, click the **Recycle All** icon.



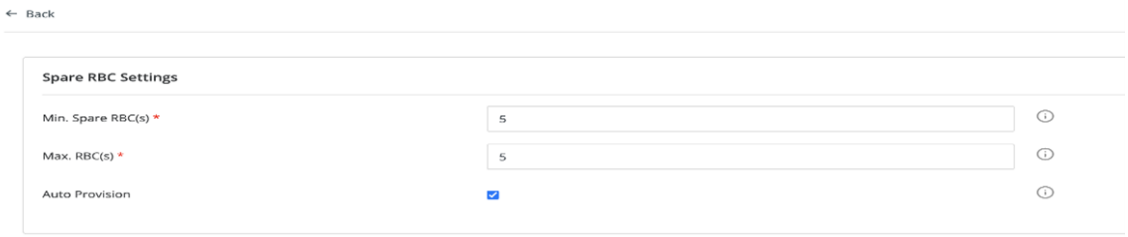
Note

Verify that the state of all nodes has changed to **Offline** from **Available**.

7) Go to the **Appliances** page.

8) In the **Actions** column for the rbc cluster, click the **Configuration** icon.

9) Check the **Auto Provision** checkbox.



10) Under **RBC Cluster Detail**, update the rac version to *ract-direct:r22.10* in the **RBC Image** field.

11) Click the **Save** button.