

# IBM QRadar Siem Installation


## 1- Search Qradar Community Edition on Google

The screenshot shows a Google search results page for the query 'qradar community edition'. The search bar at the top contains the text 'qradar community edition'. Below the search bar, the results show approximately 266,000 results found in 0.33 seconds. A tip suggests filtering results by language. The first result is from 'ibm.com' and is titled 'IBM Security QRadar Community Edition' with a green checkmark icon. The snippet below the title states: 'Community Edition is a fully-featured free version of QRadar that is low memory, low EPS, and includes a perpetual license. This version is limited to 50 ...'. Below this, there is a link to a PDF document titled 'QRadar Community Edition - IBM' with a green checkmark icon. The snippet for this PDF states: 'IBM QRadar Community Edition is a free version of IBM QRadar intended for individual use, and is released without a warranty. IBM QRadar Community Edition ...'.

## 2- Download Qradar Community Edition after Sign in IBM

The screenshot shows the IBM Security QRadar Community Edition download page. The page has a dark background with a pattern of small, colorful dots. The main heading is 'IBM Security QRadar Community Edition'. Below the heading, there is a sub-heading: 'Experiment, test, and develop on a fully featured version of the market leading SIEM'. There are two buttons: 'Download QRadar Community Edition V7.3.3' and 'Getting Started'. The 'Download QRadar Community Edition V7.3.3' button is highlighted with a red box. Below the buttons, there is a link: 'Request a Custom Demo →'. At the bottom of the page, there is a navigation bar with four items: '01 About', '02 Value', '03 Requirements', and '04 Getting Started'.

### 3- Download Qradar Community

 IBM MRS Tool

## Download the IBM QRadar Community Edition

Marketing Registration Services

### Downloads

By clicking `Download` you agree that you have had the opportunity to review the terms and conditions and that such terms and conditions govern this transaction


Download the IBM QRadar Community Edition

English

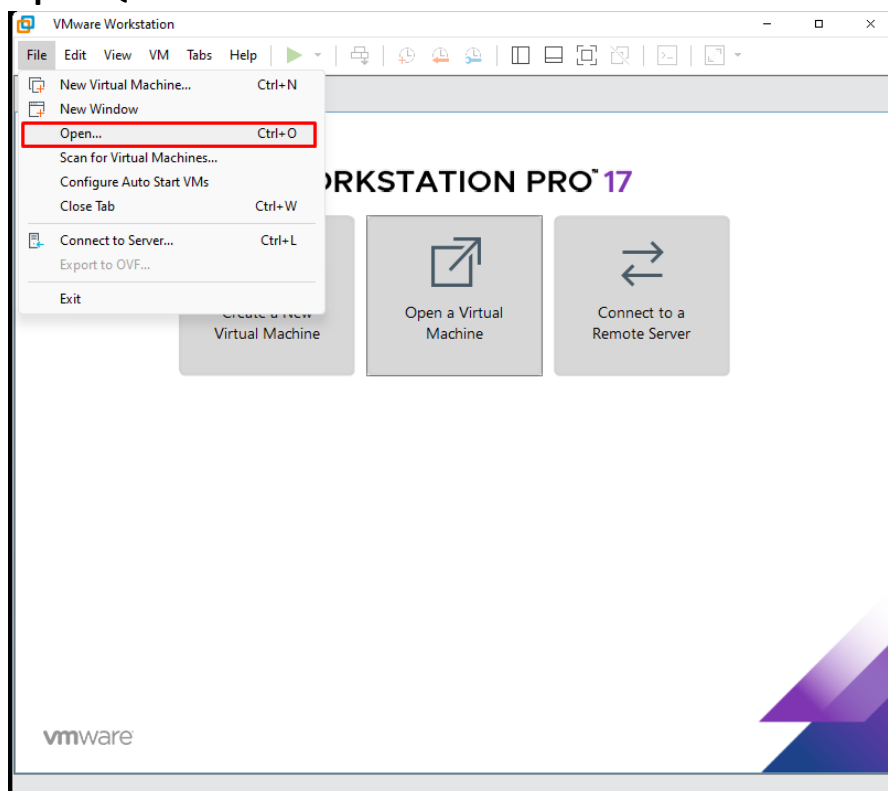
2020-02-11

Show  entries

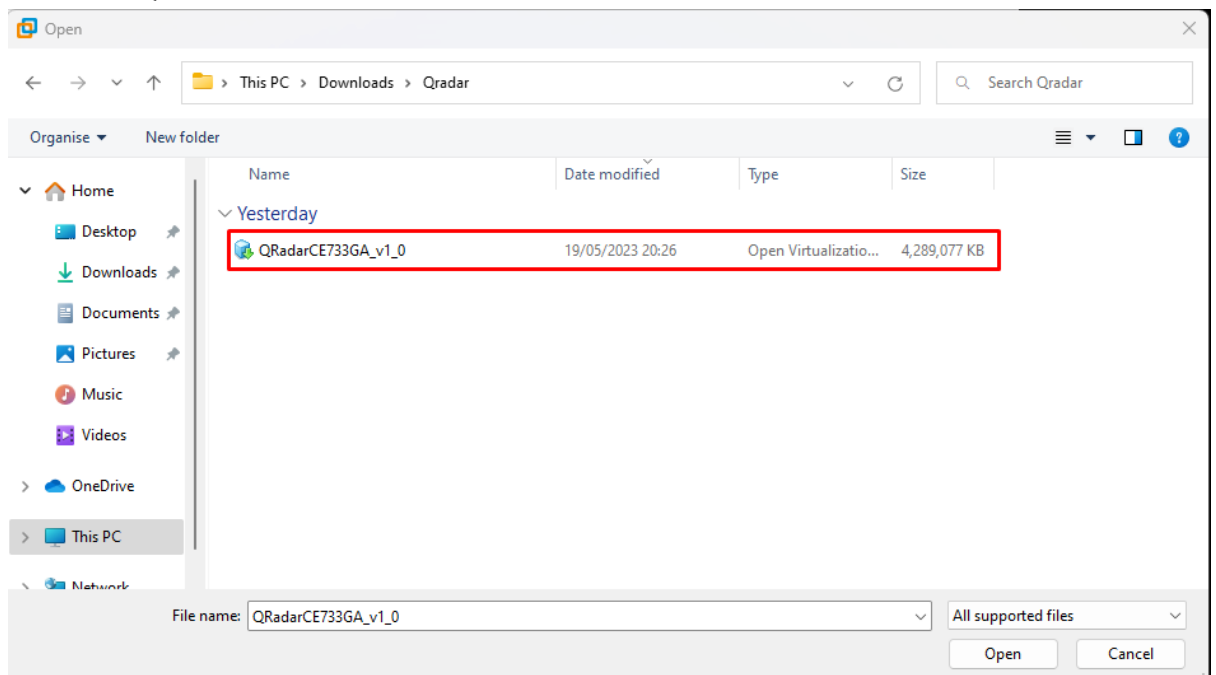
Search:

Description	Filename	Size	Action
QRadarCE733GA_v1_0.ova	QRadarCE733GA_v1_0.ova	4.1 GB	<a href="#">Download</a> 

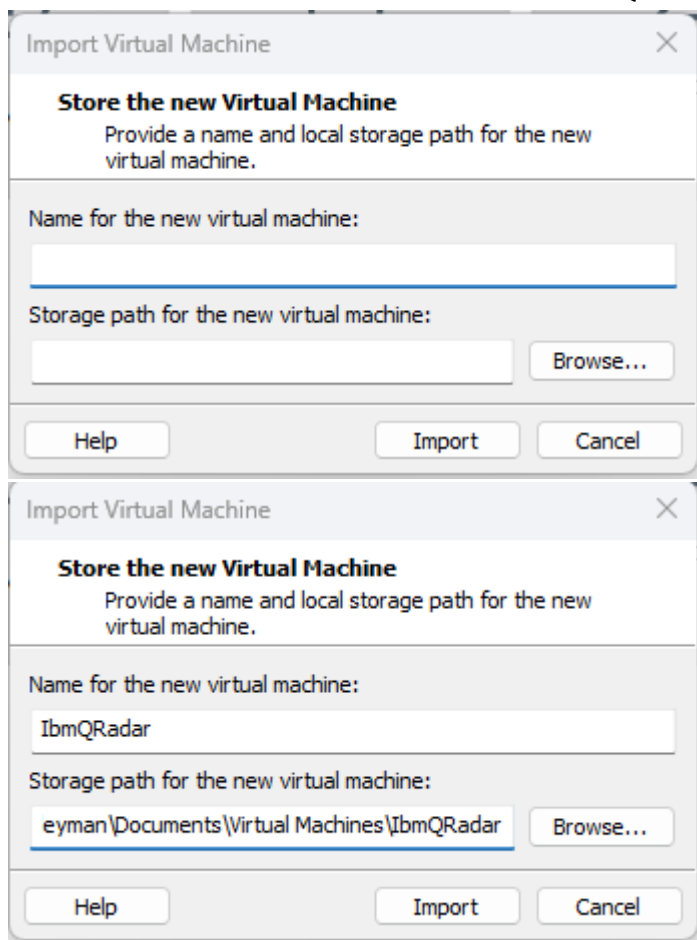
### 4- Open Qradar Ova File on Vmware



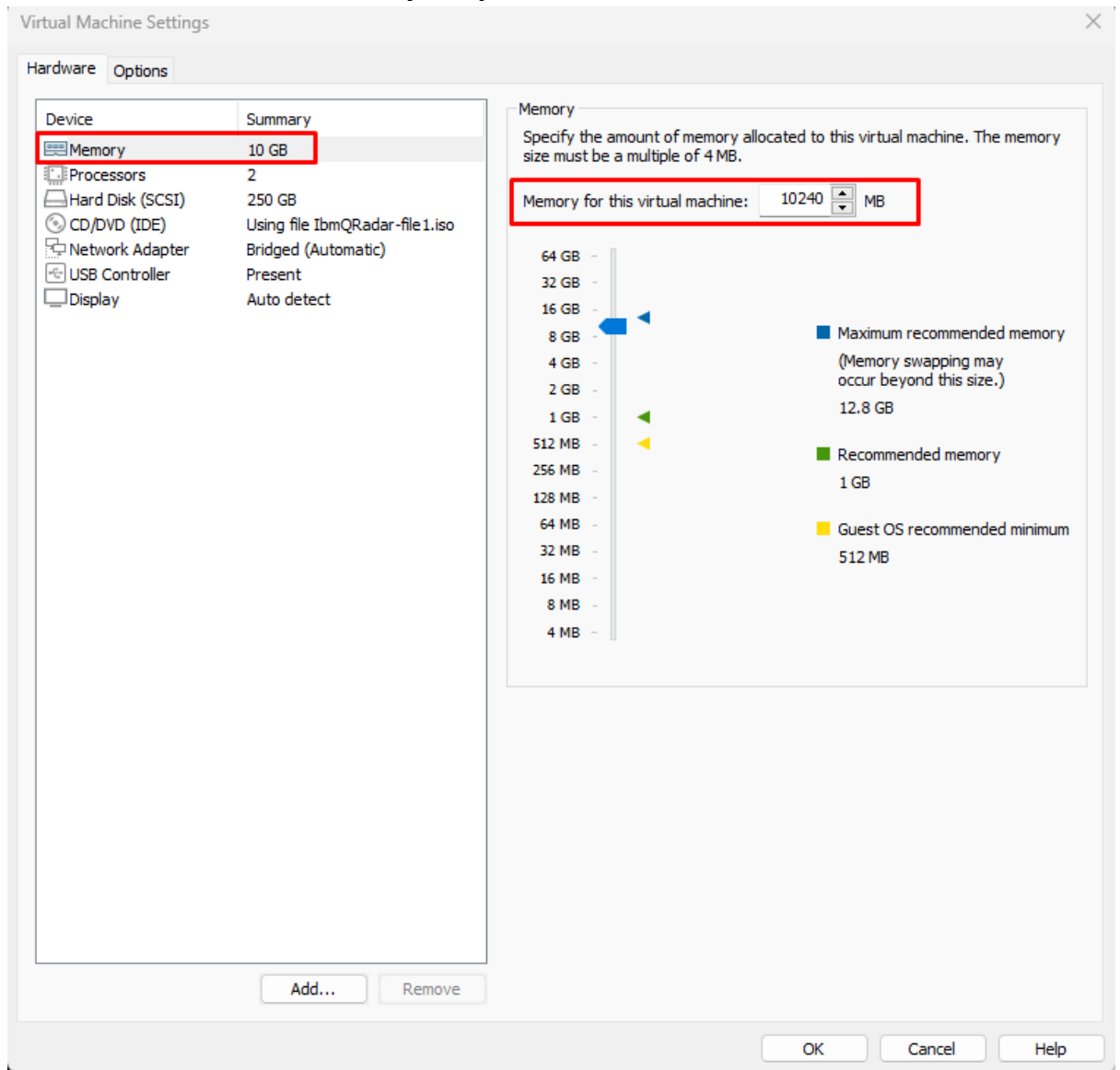
## 5- Choose Qradar Ova File



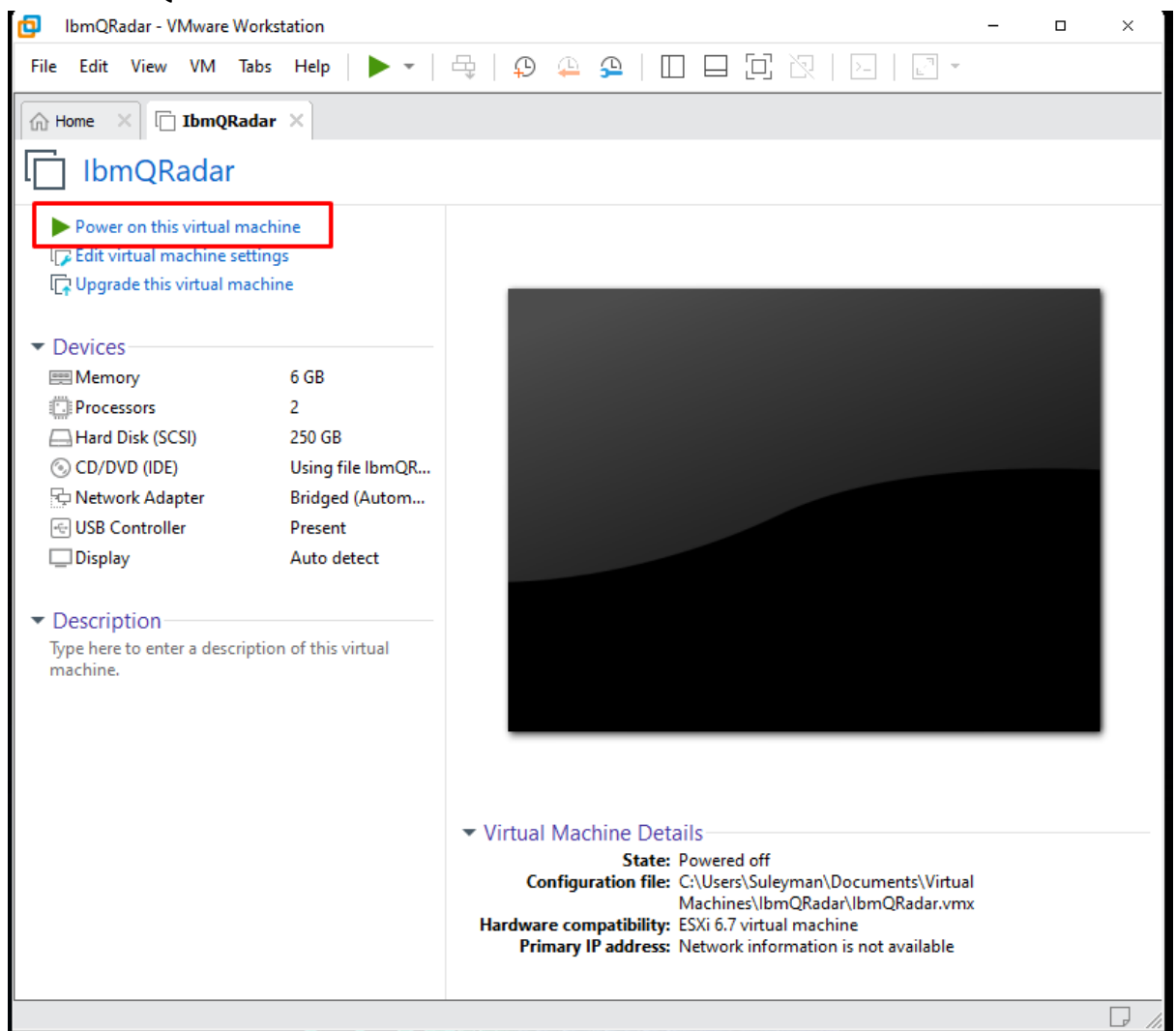
## 6- Write the name of Virtual Machine for Qradar Siem & import it.



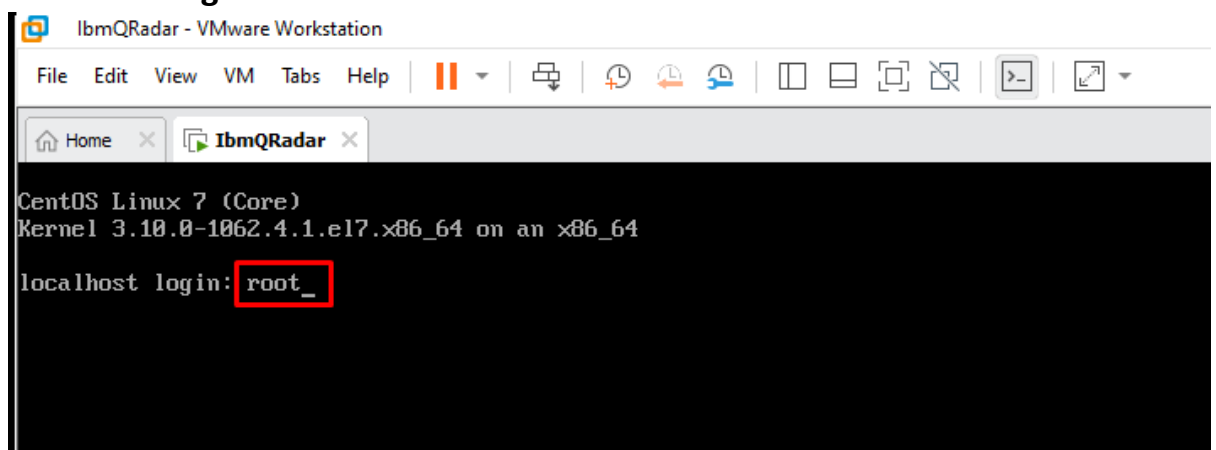
## 7- Set Virtual Machine Memory & Cpu then OK.



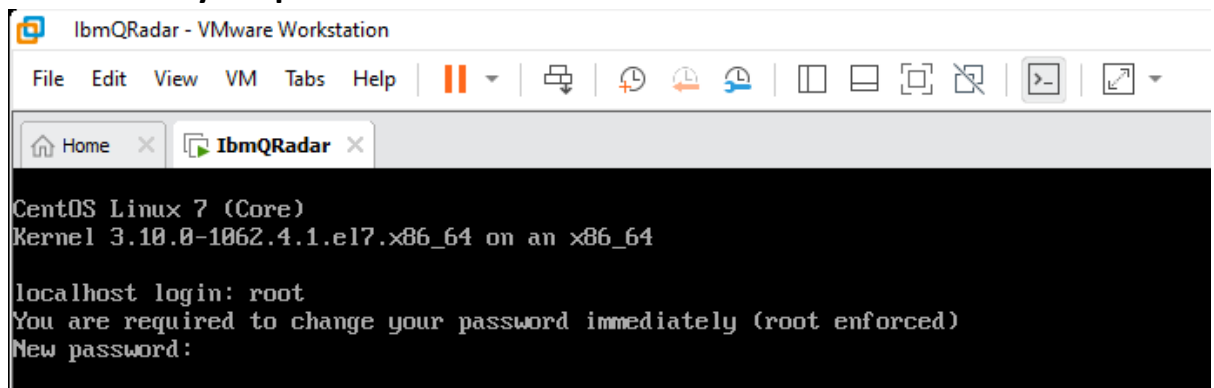
## 8- Start the Qradar



## 9- Local host login: root

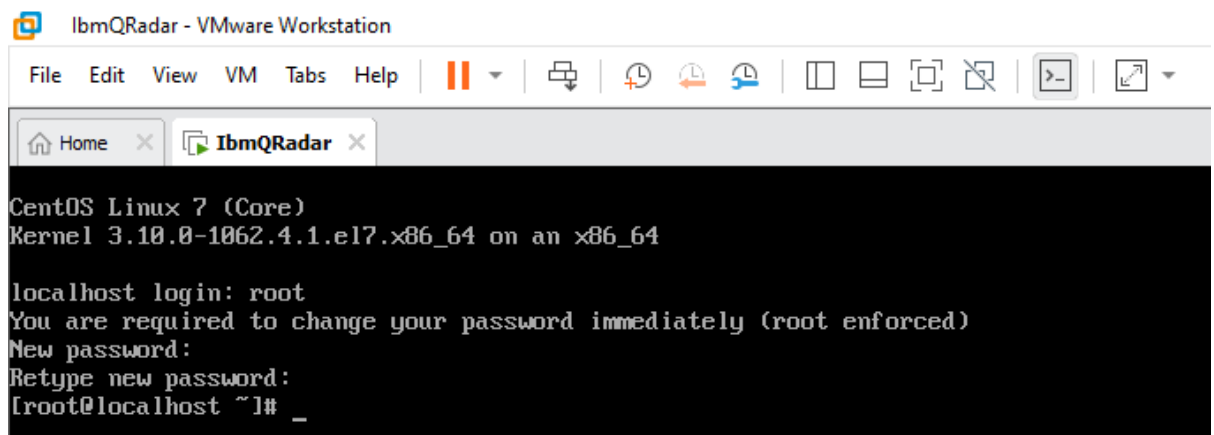


## 10- Enter your password



CentOS Linux 7 (Core)  
Kernel 3.10.0-1062.4.1.el7.x86\_64 on an x86\_64

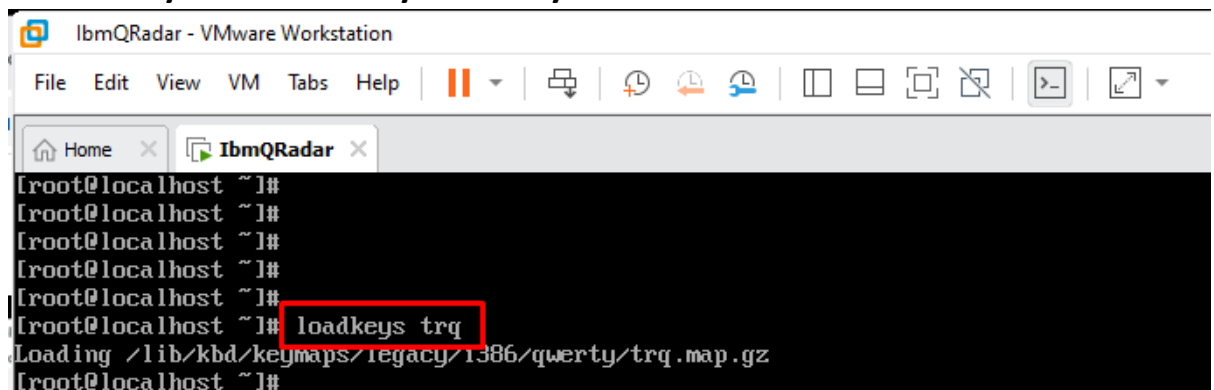
localhost login: root  
You are required to change your password immediately (root enforced)  
New password:



CentOS Linux 7 (Core)  
Kernel 3.10.0-1062.4.1.el7.x86\_64 on an x86\_64

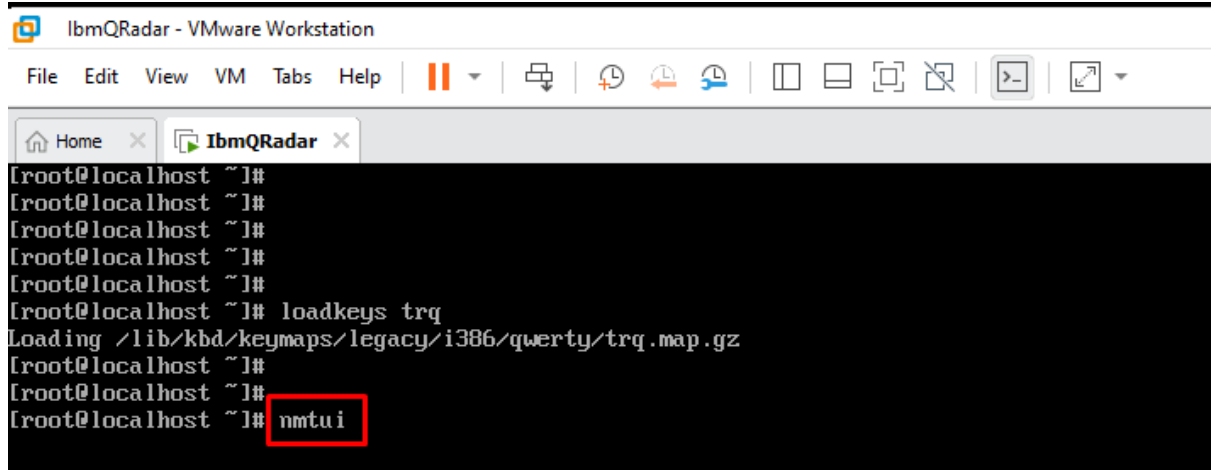
localhost login: root  
You are required to change your password immediately (root enforced)  
New password:  
Retype new password:  
[root@localhost ~]# \_

## 11- Set your Turkish keyboard Layout



[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# loadkeys trq  
Loading /lib/kbd/keymaps/legacy/1386/qwerty/trq.map.gz  
[root@localhost ~]#

## 12- Write nmtui then set your IP address & Localhost

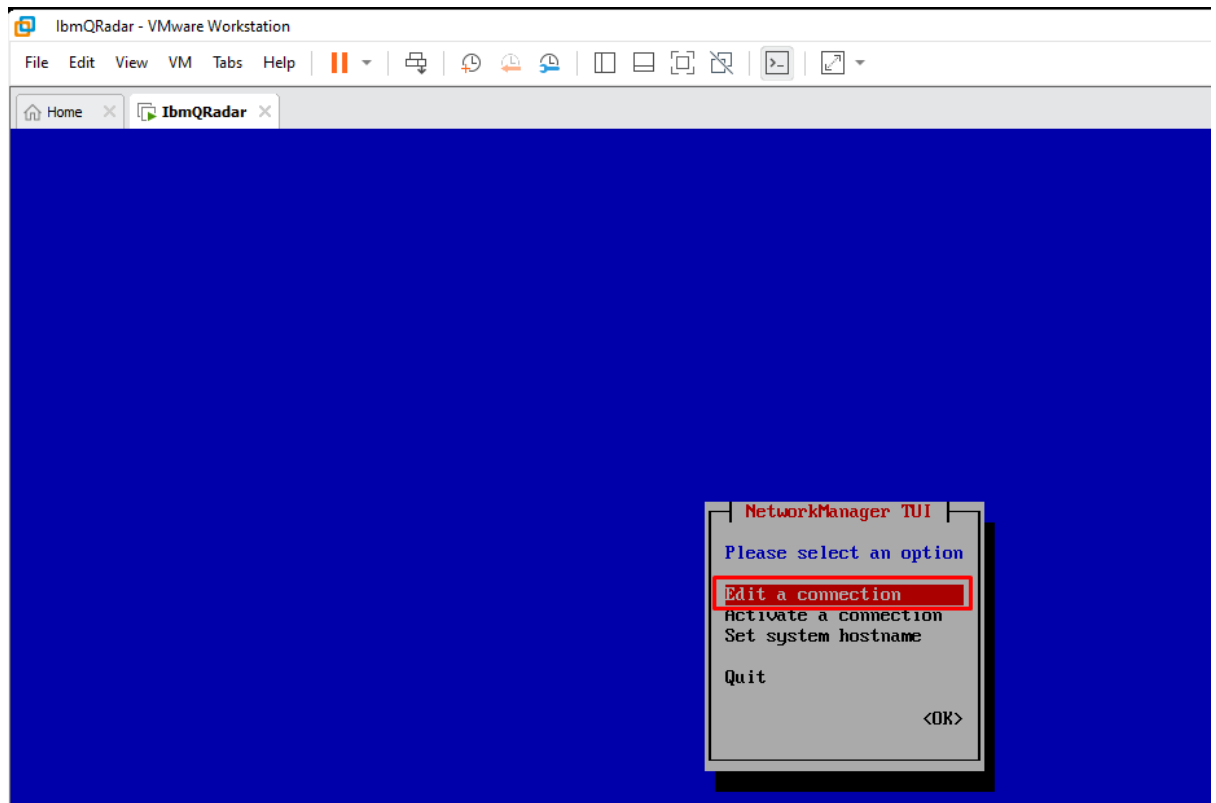


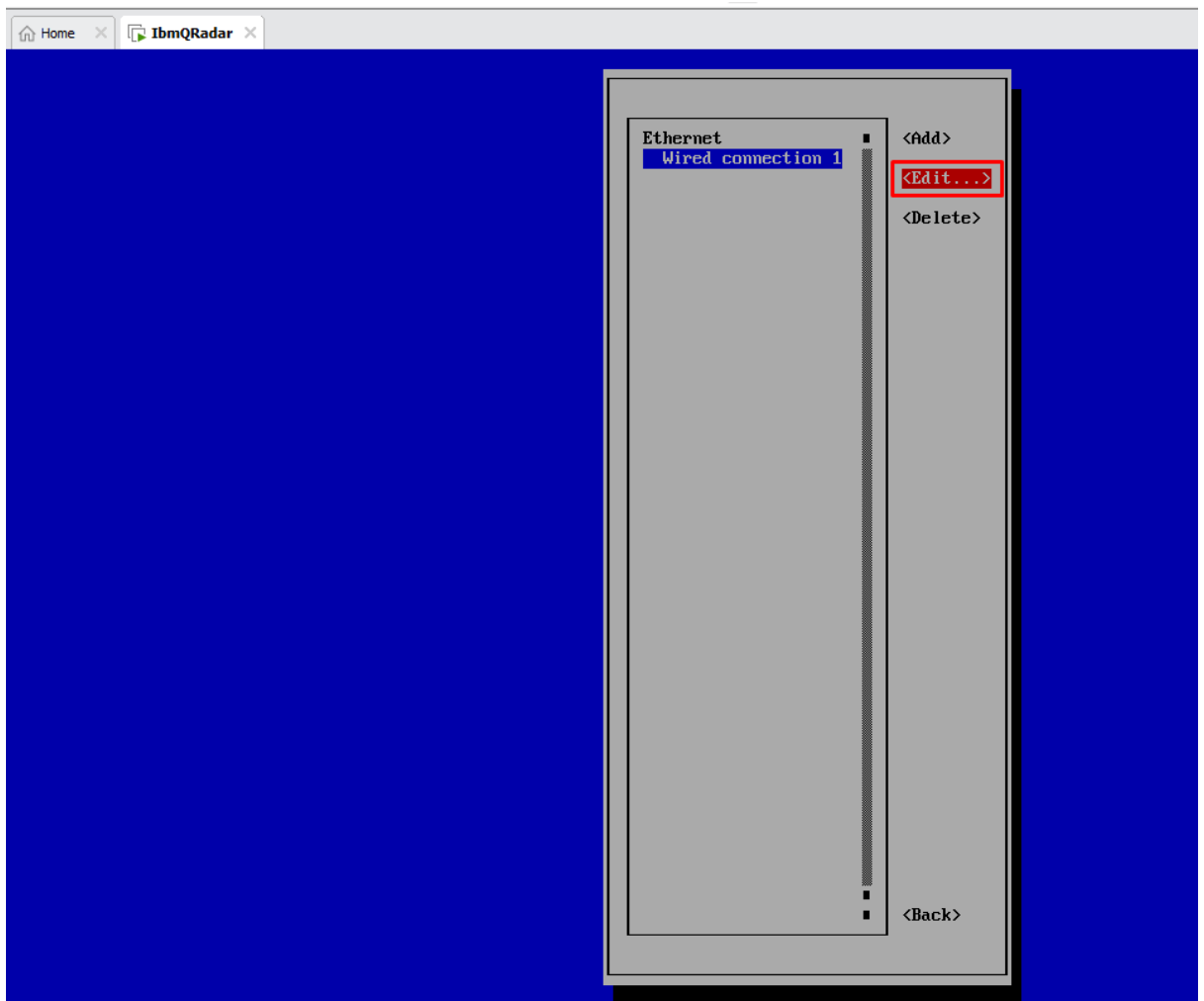
The screenshot shows a terminal window titled 'IbmQRadar - VMware Workstation'. The terminal output is as follows:

```
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# loadkeys trq  
Loading /lib/kbd/keymaps/legacy/i386/qwerty/trq.map.gz  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# nmtui
```

The command `nmtui` is highlighted with a red box.

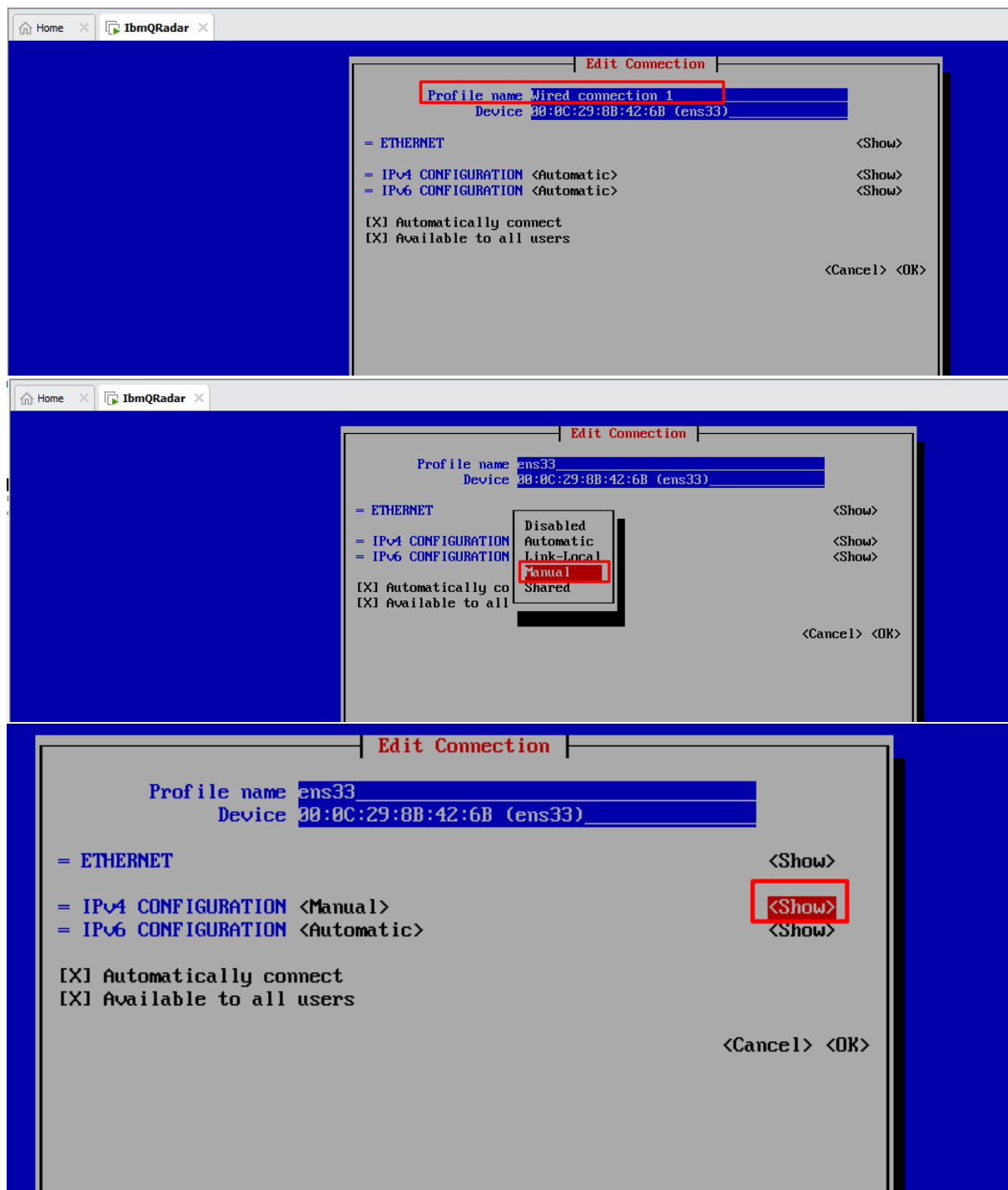
## 13- Edit a Connection







## 14- Change profile name & Set Ip address & Ignore IPv6



Edit Connection	
Profile name	ens33
Device	00:0C:29:8B:42:6B (ens33)
= ETHERNET <span style="float: right;">&lt;Show&gt;</span>	
■ IPv4 CONFIGURATION <Manual>	<Hide>
Addresses	<Add...>
Gateway	
DNS servers	<Add...>
Search domains	<Add...>
Routing (No custom routes) <Edit...> <input type="checkbox"/> Never use this network for default route <input type="checkbox"/> Ignore automatically obtained routes <input type="checkbox"/> Ignore automatically obtained DNS parameters <input type="checkbox"/> Require IPv4 addressing for this connection	
= IPv6 CONFIGURATION <Automatic> <span style="float: right;">&lt;Show&gt;</span>	
<input checked="" type="checkbox"/> Automatically connect <input checked="" type="checkbox"/> Available to all users	
<Cancel> <OK>	

Edit Connection	
Profile name	ens33
Device	00:0C:29:8B:42:6B (ens33)
= ETHERNET <span style="float: right;">&lt;Show&gt;</span>	
■ IPv4 CONFIGURATION <Manual>	<Hide>
Addresses	192.168.0.123 <span style="float: right;">&lt;Remove&gt;</span>
	<Add...>
Gateway	192.168.0.1
DNS servers	8.8.8.8 <span style="float: right;">&lt;Remove&gt;</span>
	<Add...>
Search domains	<Add...>
Routing (No custom routes) <Edit...> <input type="checkbox"/> Never use this network for default route <input type="checkbox"/> Ignore automatically obtained routes <input type="checkbox"/> Ignore automatically obtained DNS parameters <input type="checkbox"/> Require IPv4 addressing for this connection	
= IPv6 CONFIGURATION	<div style="border: 1px solid black; padding: 2px;">             Ignore              Automatic              Automatic (DHCP-only)              Link-Local              Manual           </div> <span style="float: right;">&lt;Show&gt;</span>
<input checked="" type="checkbox"/> Automatically connect <input checked="" type="checkbox"/> Available to all	
<Cancel> <OK>	

## Edit Connection

Profile name **ens33**

Device **00:0C:29:8B:42:6B (ens33)**

= ETHERNET

<Show>

■ IPv4 CONFIGURATION <Manual>

<Hide>

Addresses **192.168.0.123** <Remove>

<Add...>

Gateway **192.168.0.1**

DNS servers **8.8.8.8** <Remove>

<Add...>

Search domains <Add...>

Routing (No custom routes) <Edit...>

☐ Never use this network for default route

☐ Ignore automatically obtained routes

☐ Ignore automatically obtained DNS parameters

☐ Require IPv4 addressing for this connection

= IPv6 CONFIGURATION <Ignore>

<Show>

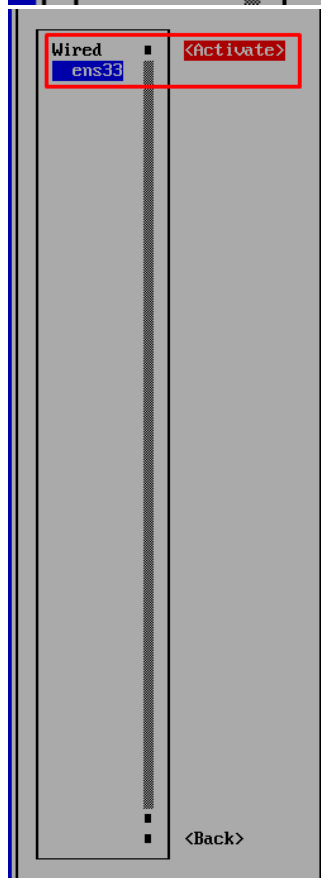
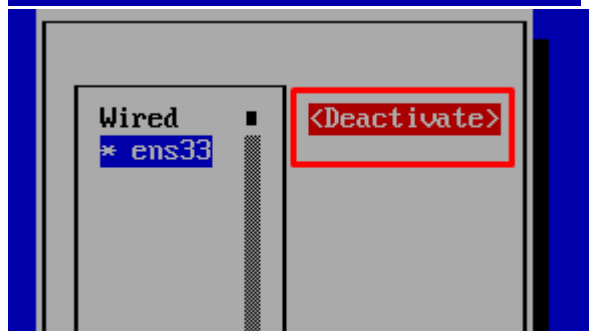
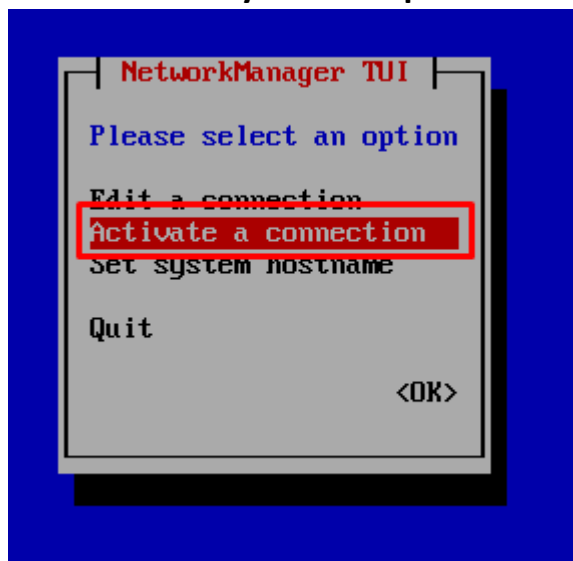
☒ Automatically connect

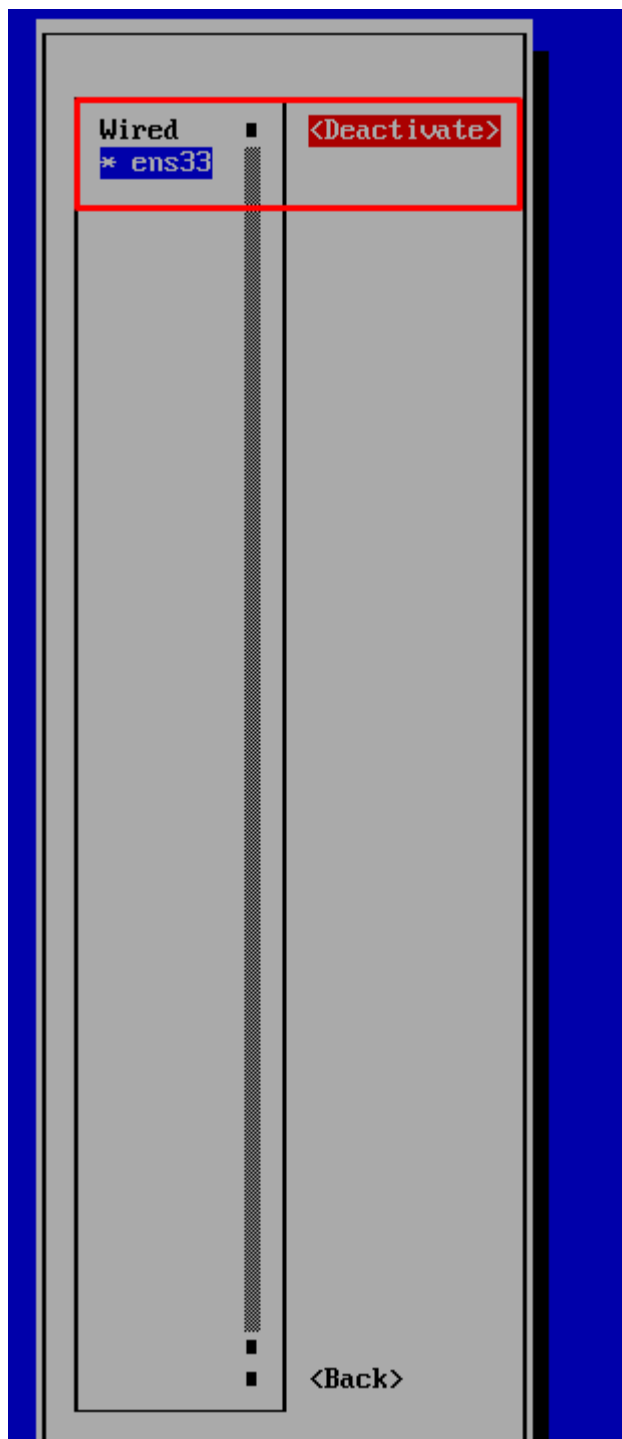
☒ Available to all users

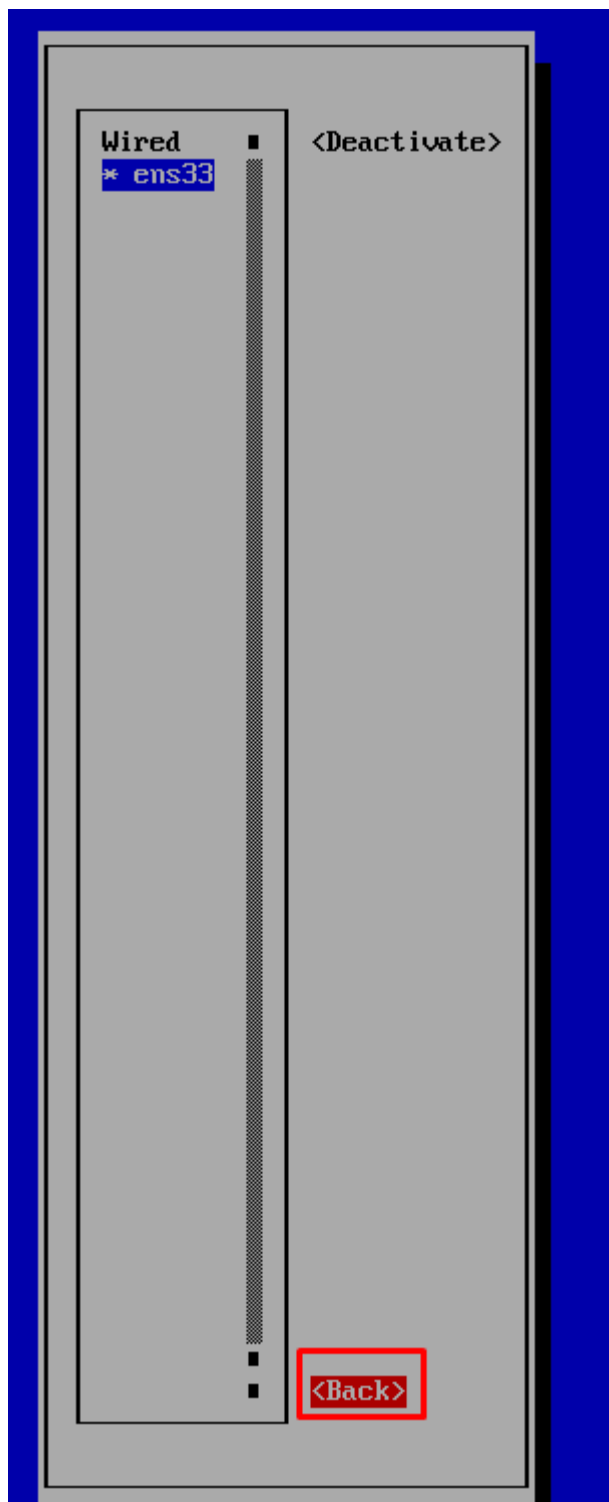
<Cancel>

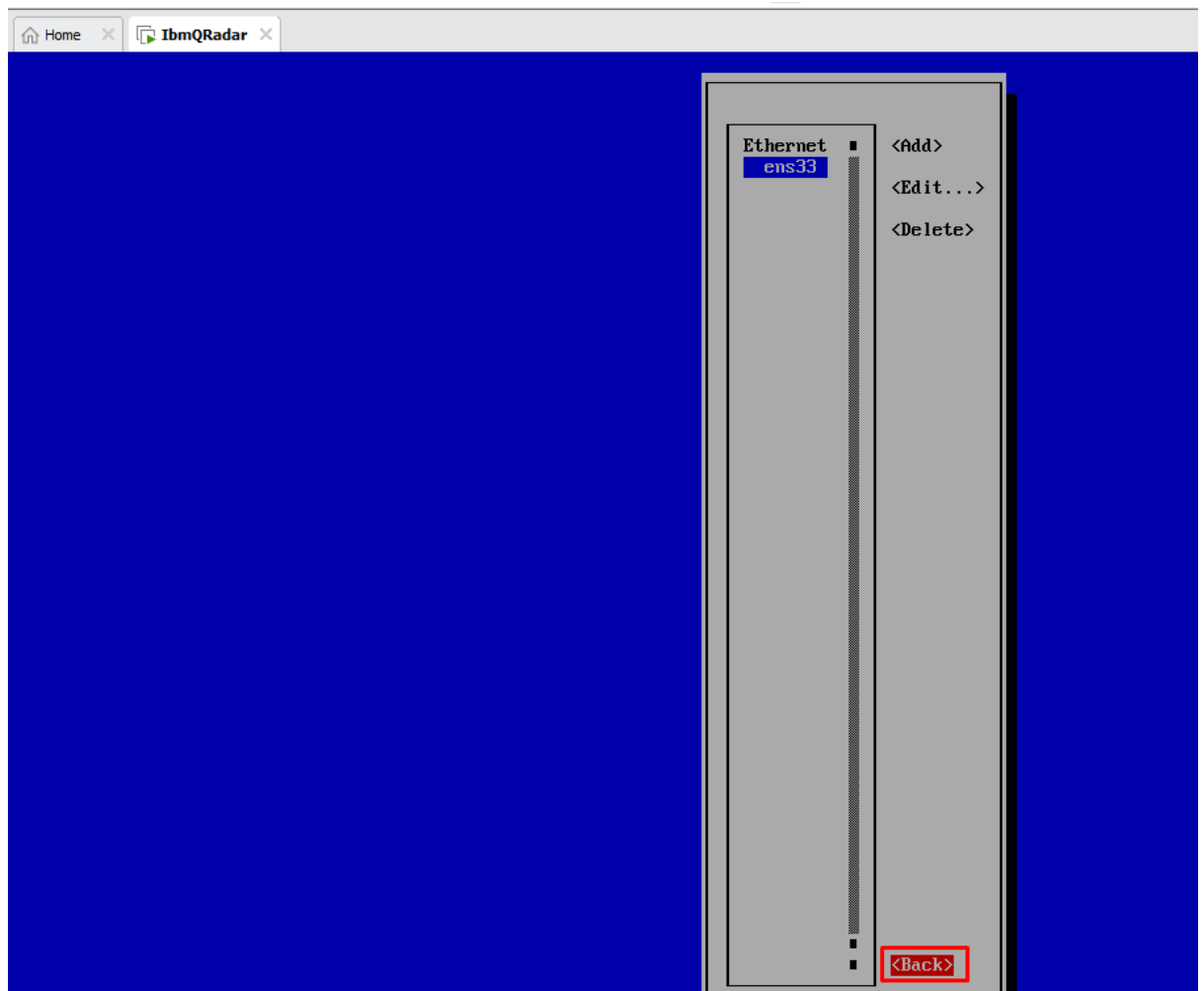
<OK>

15-      Activate your new Ip Address

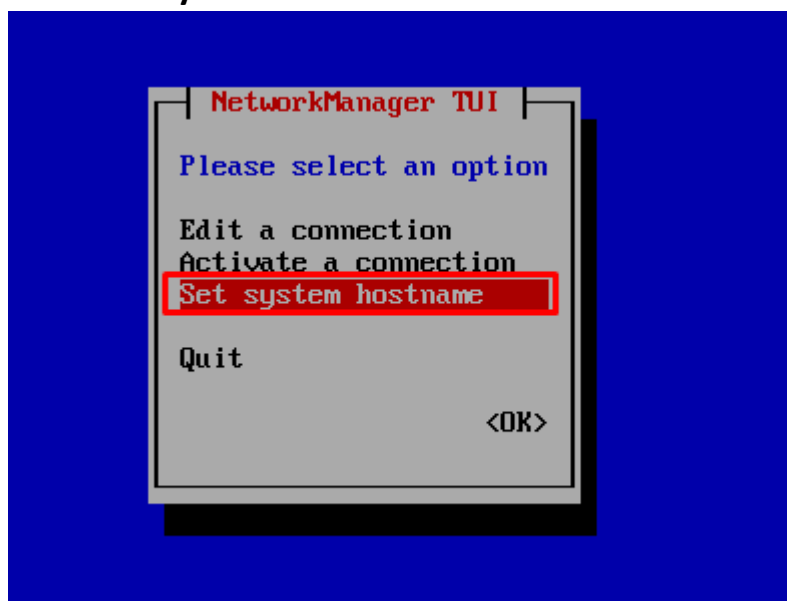


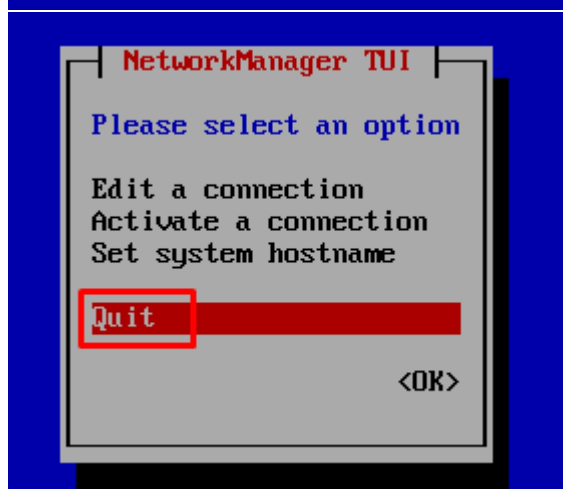
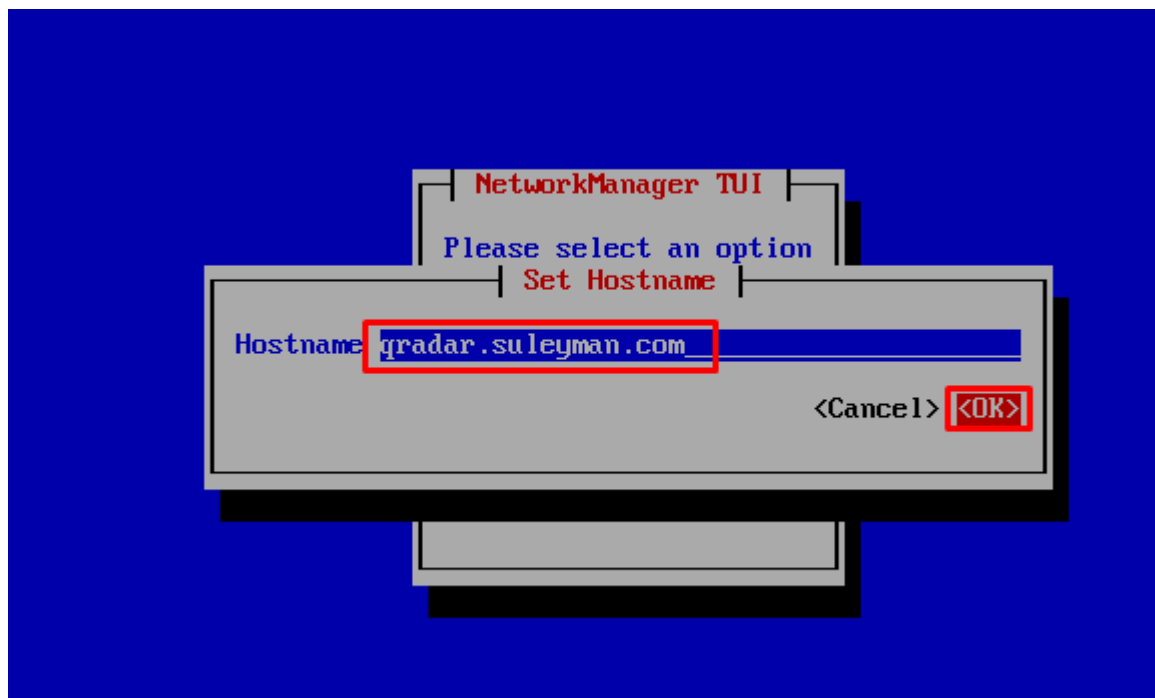






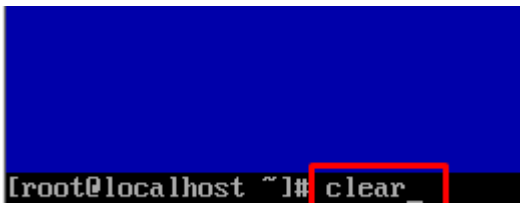
## 16- Set system Hostname







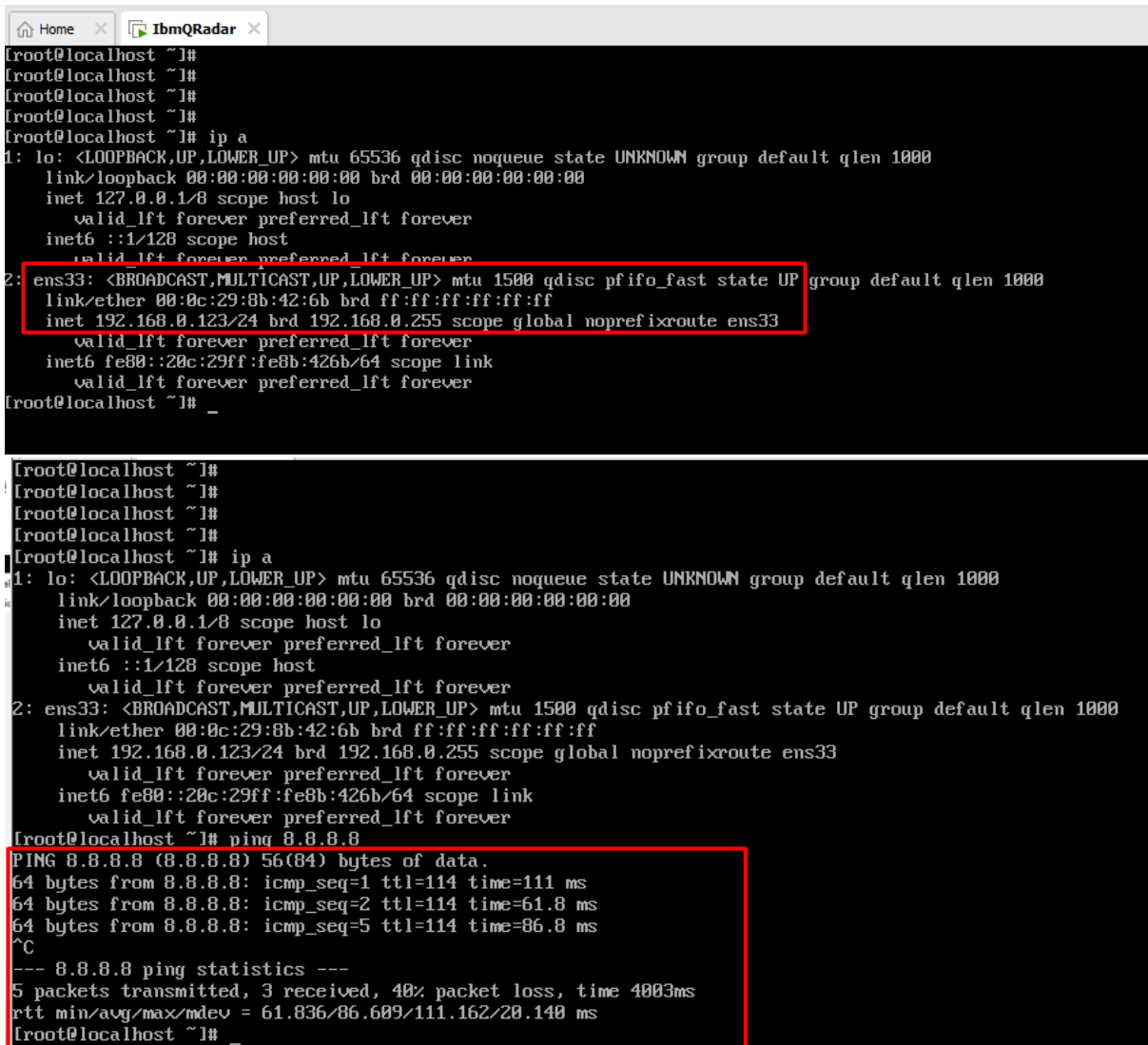
## 17- Clear the Console Screen



```
[root@localhost ~]# clear
```

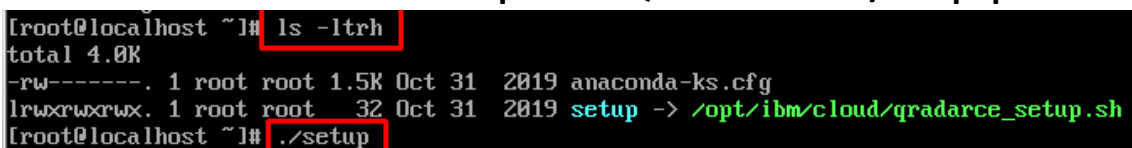
To direct input to this VM, click inside or press Ct

## 18- Run ip a command & send ping 8.8.8.8



```
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:8b:42:6b brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.123/24 brd 192.168.0.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe8b:426b/64 scope link
        valid_lft forever preferred_lft forever
[root@localhost ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=111 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=61.8 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=86.8 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 3 received, 40% packet loss, time 4003ms
rtt min/avg/max/mdev = 61.836/86.609/111.162/20.140 ms
[root@localhost ~]#
```

## 19- Run ls -ltrh & see the setup file of Qradar Siem & ./setup qradar



```
[root@localhost ~]# ls -ltrh
total 4.0K
-rw-----. 1 root root 1.5K Oct 31 2019 anaconda-ks.cfg
lrwxrwxrwx. 1 root root 32 Oct 31 2019 setup -> /opt/ibm/cloud/qradarce_setup.sh
[root@localhost ~]# ./setup
```

## 20- Accept the License Agreement so press enter

```
Found /tmp/.accepted_gradar_eula - answer yes to accept eula
About to install QRadar Community Edition 7.3.3 (Build 20191031163225)
Do you wish to continue (Y/[N])? Y
```

IBM QRadar - VMware Workstation

File Edit View VM Tabs Help

Home x IBMQRadar x

Starting QRadar 7.3.3 Community Edition setup

CentOS 7 Linux EULA

CentOS 7 Linux comes with no guarantees or warranties of any sorts,  
either written or implied.

The Distribution is released as GPLv2. Individual packages in the  
distribution come with their own licences. A copy of the GPLv2 license  
is included with the distribution media.

Use of this product is subject to the license agreement above.

Press enter to accept these terms or press CTRL+C to quit.

This Program may contain cryptography. Transfer to, or use by, users of  
the Program may be prohibited or subject to export or import laws,  
regulations or policies, including those of the United States Export  
Administration Regulations. Licensee assumes all responsibility for  
complying with all applicable laws, regulations, and policies regarding  
the export, import, or use of this Program, including but not limited to,  
U.S. restrictions on exports or reexports. To obtain the export  
classification of this Program refer to:  
<https://www.ibm.com/products/exporting/>.

Third Party Beneficiaries

Each of the following suppliers is a third-party beneficiary of this  
Agreement:  
Oracle America, Inc.

In addition to the above, the following terms apply to Licensee's use of  
the Program.

Lawful Use of Program:  
This Program is designed to help Licensee improve its security environment  
and data. Use of this Program may implicate various laws or regulations,  
including those related to privacy, data protection, employment, and  
electronic communications and storage. The Program may be used only for  
lawful purposes and in a lawful manner. Licensee agrees to use the Program  
pursuant to, and assumes all responsibility for complying with, applicable  
laws, regulations and policies. Licensee represents that it will obtain or  
has obtained any consents, permission's, or licenses required to enable  
its lawful use of the Program.

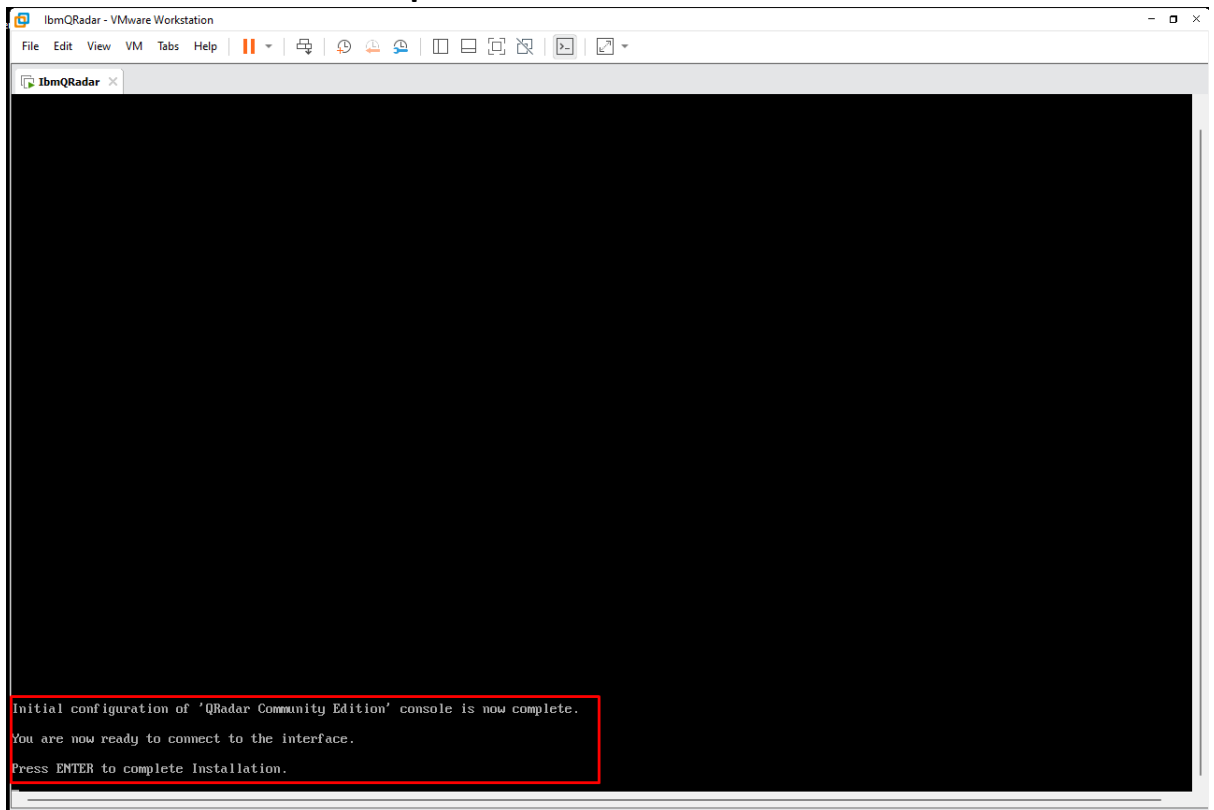
Cloud Service Provider:  
Licensee may install the Program at a third party environment identified  
in the Program's installation guide that provides Licensee with  
infrastructure services, networking, storage and data center space for  
hosting software applications ("Cloud Service Provider"). This  
authorization does not modify or supersede any of Licensee's obligations  
in the applicable license agreement, including requirements for use in a  
virtualized environment. Licensee acknowledges that the verification terms  
in the applicable license agreement extend to the Cloud Service Provider  
environment on which the Programs are installed, and Licensee agrees to  
collect any required usage data. Licensee will not provide the Cloud  
Service Provider with any unauthorized use or access to the Program.

L/N: L-KFRN-BH7JG3  
D/N: L-KFRN-BH7JG3  
P/N: L-KFRN-BH7JG3  
(END)

- 21- Write Y and Finally begin the Installation 😊  
It takes time about 49 minutes

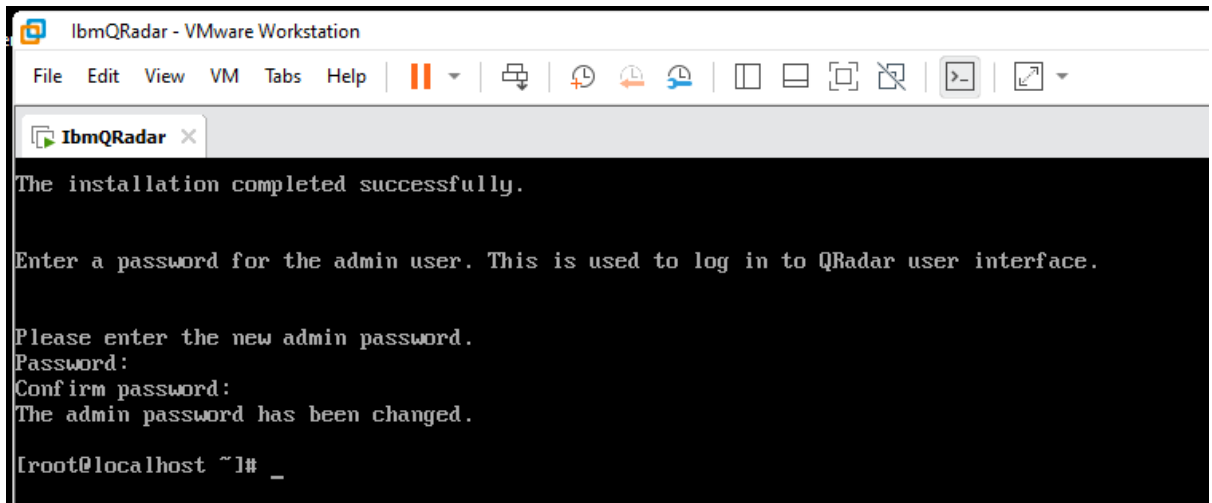
```
Found /tmp/.accepted_gradar_eula - answer yes to accept eula
About to install QRadar Community Edition 7.3.3 (Build 20191031163225)
Do you wish to continue (Y/[N])? Y
```

- 22- Press enter the complete installation



```
Initial configuration of 'QRadar Community Edition' console is now complete.
You are now ready to connect to the interface.
Press ENTER to complete Installation.
```

## 23- Peress enter the Qradar password for interface



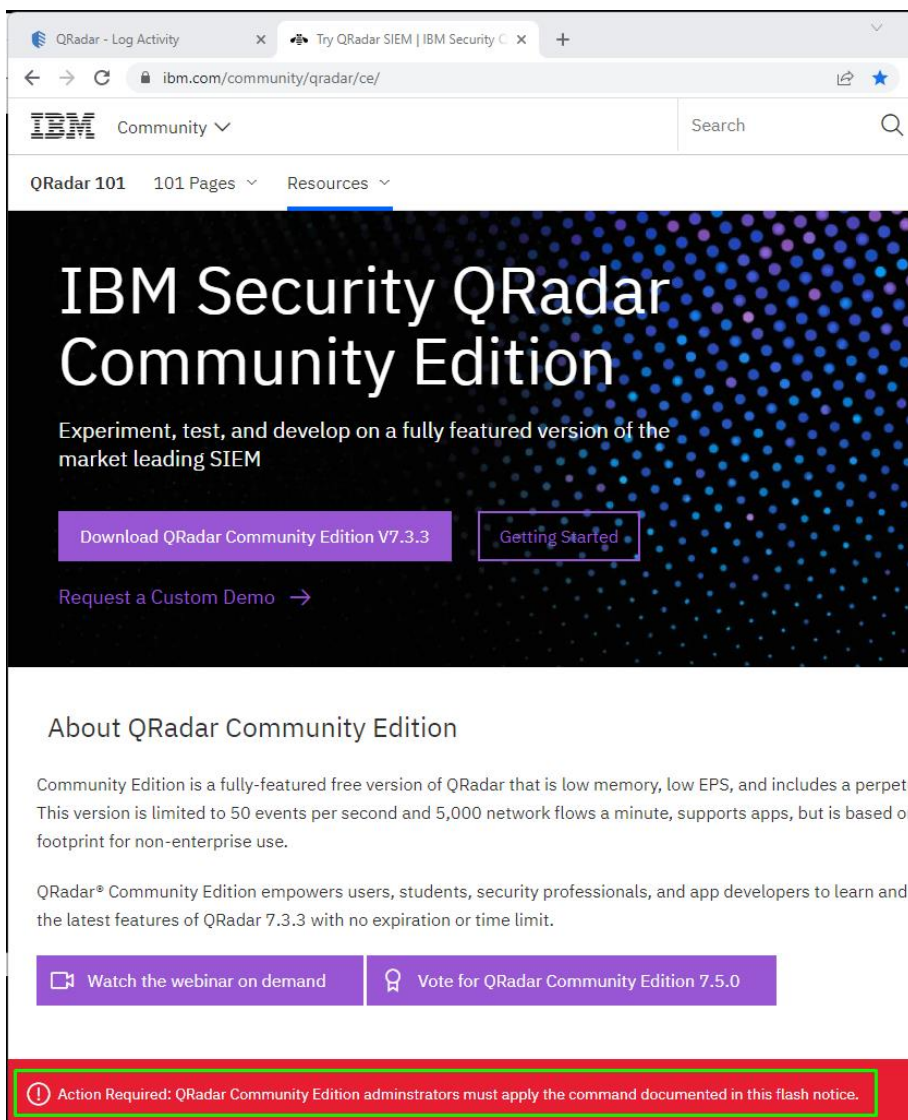
```
IbmQRadar - VMware Workstation
File Edit View VM Tabs Help
The installation completed successfully.

Enter a password for the admin user. This is used to log in to QRadar user interface.

Please enter the new admin password.
Password:
Confirm password:
The admin password has been changed.

[root@localhost ~]# _
```

## 24- Set command documented so go to community webpage at the bottom enter the command documented



QRadar - Log Activity x Try QRadar SIEM | IBM Security C x +

ibm.com/community/qradar/ce/

IBM Community Search

QRadar 101 101 Pages Resources

# IBM Security QRadar Community Edition

Experiment, test, and develop on a fully featured version of the market leading SIEM

[Download QRadar Community Edition V7.3.3](#) [Getting Started](#)

[Request a Custom Demo](#) →

## About QRadar Community Edition

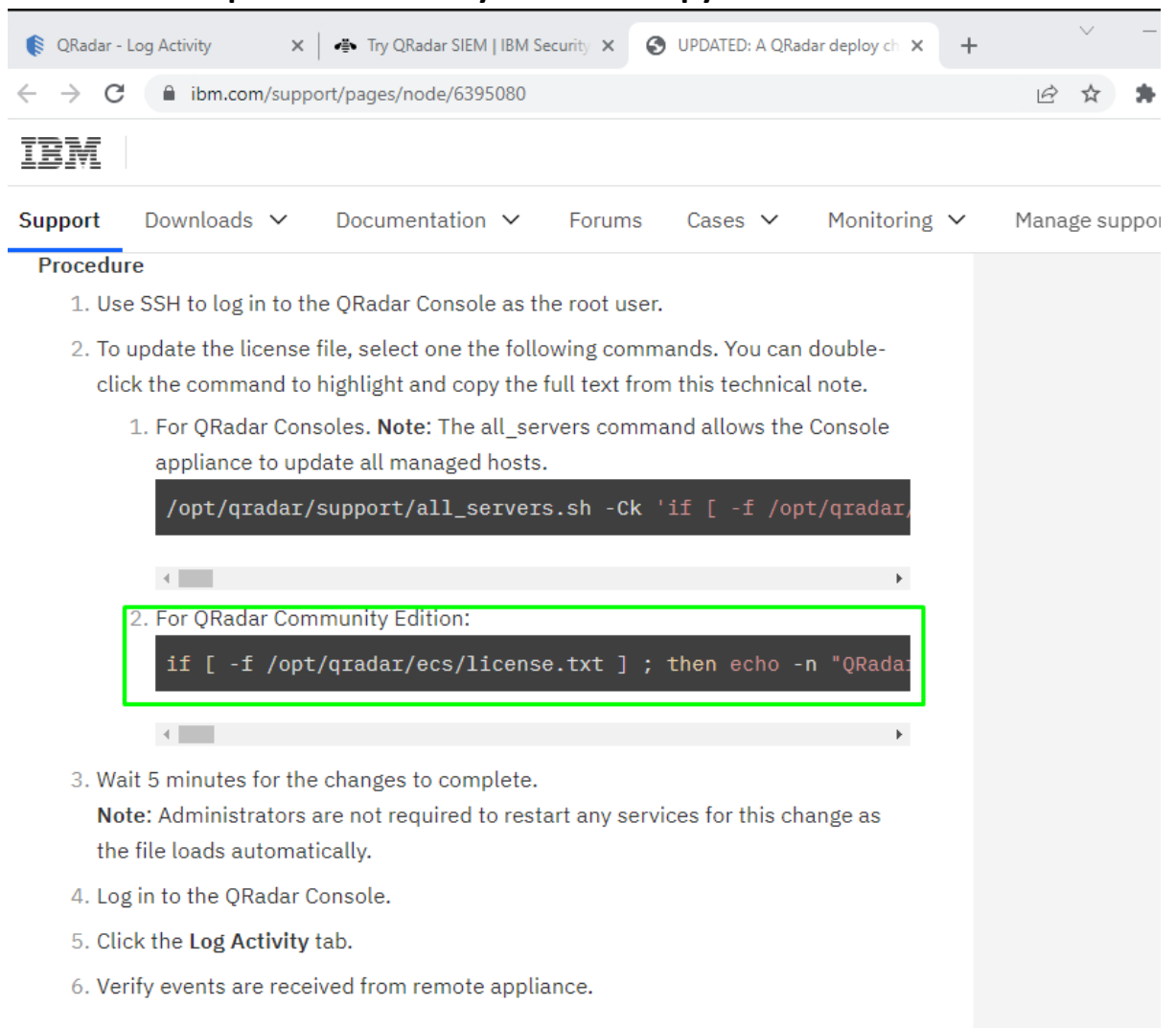
Community Edition is a fully-featured free version of QRadar that is low memory, low EPS, and includes a perpetual license. This version is limited to 50 events per second and 5,000 network flows a minute, supports apps, but is based on footprint for non-enterprise use.

QRadar® Community Edition empowers users, students, security professionals, and app developers to learn and explore the latest features of QRadar 7.3.3 with no expiration or time limit.

[Watch the webinar on demand](#) [Vote for QRadar Community Edition 7.5.0](#)

**Action Required: QRadar Community Edition administrators must apply the command documented in this flash notice.**

## 25- Choose qradar community Edition & copy the command



Support Downloads Documentation Forums Cases Monitoring Manage support

### Procedure

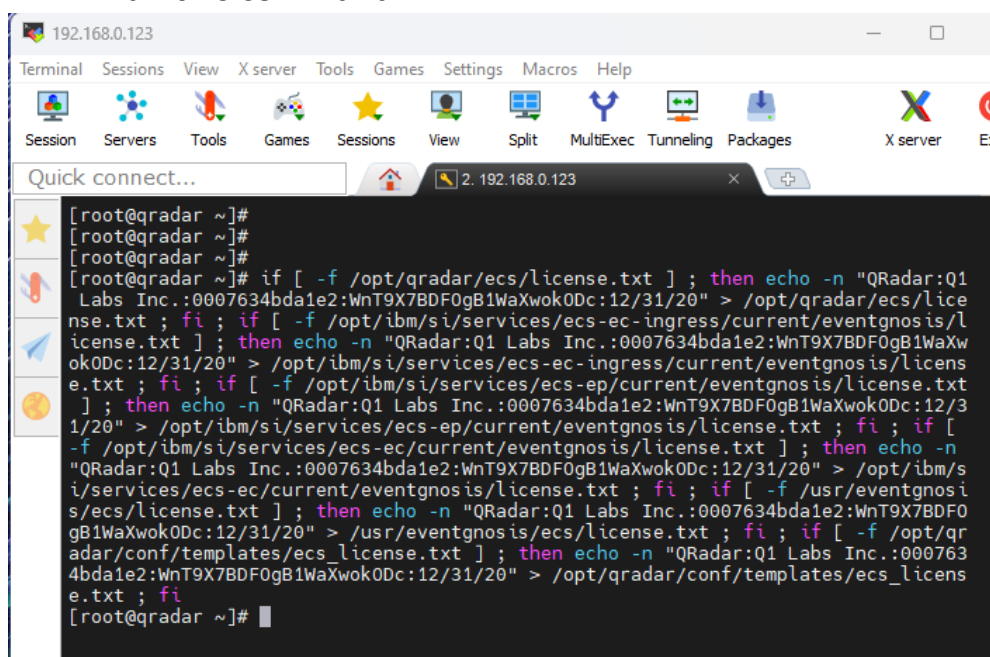
1. Use SSH to log in to the QRadar Console as the root user.
2. To update the license file, select one the following commands. You can double-click the command to highlight and copy the full text from this technical note.
  1. For QRadar Consoles. **Note:** The `all_servers` command allows the Console appliance to update all managed hosts.

```
/opt/qradar/support/all_servers.sh -Ck 'if [ -f /opt/qradar,
```
  2. For QRadar Community Edition:

```
if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar
```
3. Wait 5 minutes for the changes to complete.

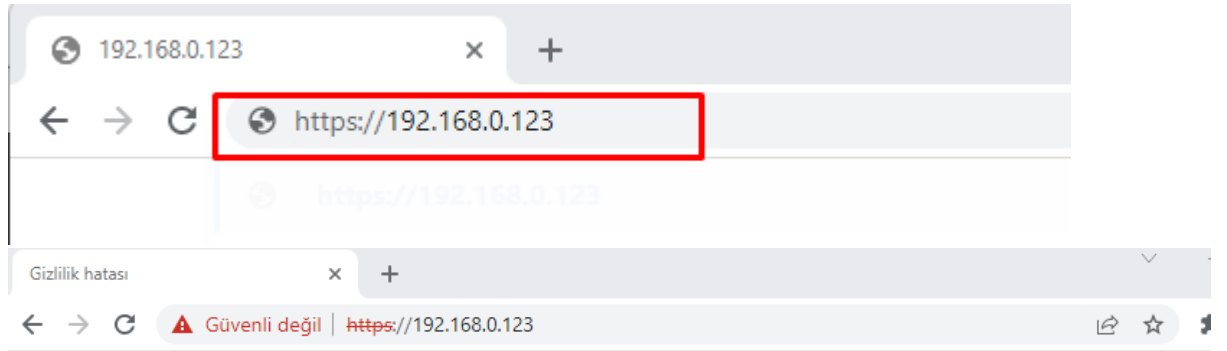
**Note:** Administrators are not required to restart any services for this change as the file loads automatically.
4. Log in to the QRadar Console.
5. Click the **Log Activity** tab.
6. Verify events are received from remote appliance.

## 26- Run this command



```
[root@qradar ~]#  
[root@qradar ~]#  
[root@qradar ~]#  
[root@qradar ~]# if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar:Q1  
Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/qradar/ecs/lice  
nse.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ingress/current/eventgnosis/l  
icense.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaX  
wok0Dc:12/31/20" > /opt/ibm/si/services/ecs-ingress/current/eventgnosis/licens  
e.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt  
 ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/3  
1/20" > /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ; fi ; if [  
-f /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt ] ; then echo -n  
"QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/ibm/s  
i/services/ecs-ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnos  
i/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0  
gB1WaXwok0Dc:12/31/20" > /usr/eventgnosis/ecs/license.txt ; fi ; if [ -f /opt/q  
radar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:000763  
4bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/qradar/conf/templates/ecs_licens  
e.txt ; fi  
[root@qradar ~]#
```

27- On the browser, write the Qradar Ip address & go to your Qradar Siem 😊



## Bağlantınız gizli değil

Saldırganlar **192.168.0.123** üzerinden bilgilerinizi çalmaya çalışıyor olabilir (örneğin, şifreler, mesajlar veya kredi kartları). [Daha fazla bilgi](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID



Chrome'un sağladığı en yüksek güvenlik düzeyinden faydalanmak için [gelişmiş korumayı açın](#)

Gelişmiş

Güvenliğe geri dön

Gizlilik hatası

x +



⚠ Güvenli değil | <https://192.168.0.123>



## Bağlantınız gizli değil

Saldırganlar **192.168.0.123** üzerinden bilgilerinizi çalmaya çalışıyor olabilir (örneğin, şifreler, mesajlar veya kredi kartları). [Daha fazla bilgi](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID



Chrome'un sağladığı en yüksek güvenlik düzeyinden faydalanmak için [gelişmiş korumayı açın](#)

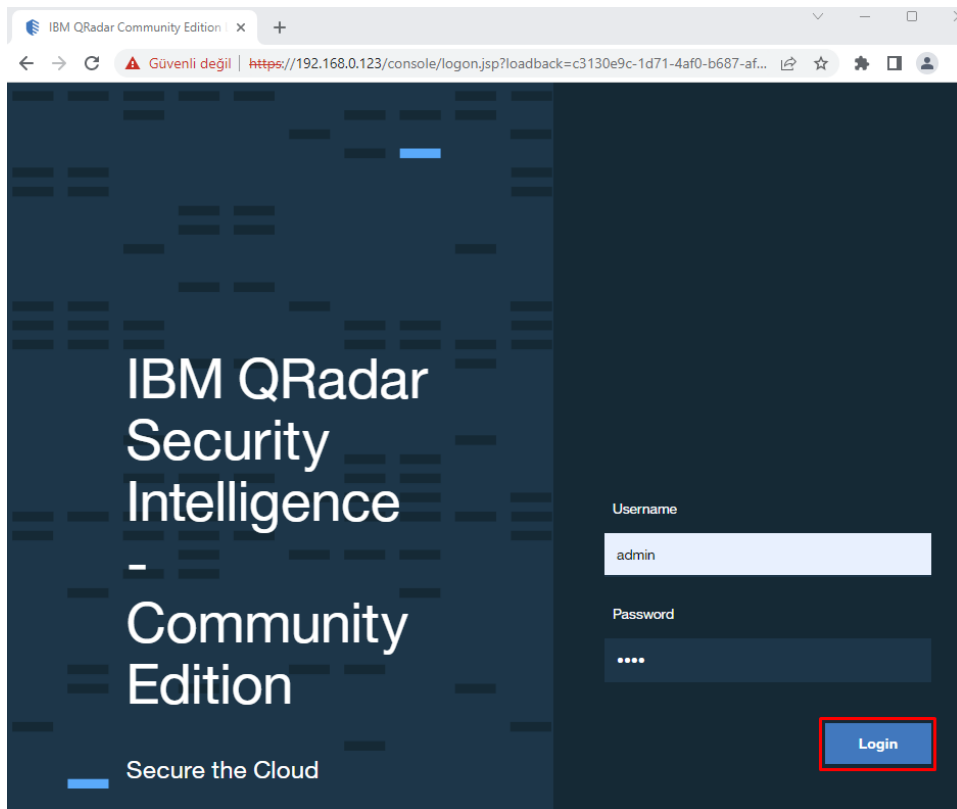
Gelişmiş bilgileri gizle

Güvenliğe geri dön

Bu sunucu **192.168.0.123** olduğunu kanıtlayamadı. Bilgisayarınızın işletim sistemi, sunucunun güvenlik sertifikasına güvenmiyor. Bu durum, bir yanlış yapılandırmadan veya bağlantıya müdahale eden bir saldırgandan kaynaklanıyor olabilir.

[192.168.0.123 sitesine ilerle \(güvenli değil\)](#)

## 28- Enter your password & do not forget it default username: admin



IBM QRadar  
Security  
Intelligence  
—  
Community  
Edition

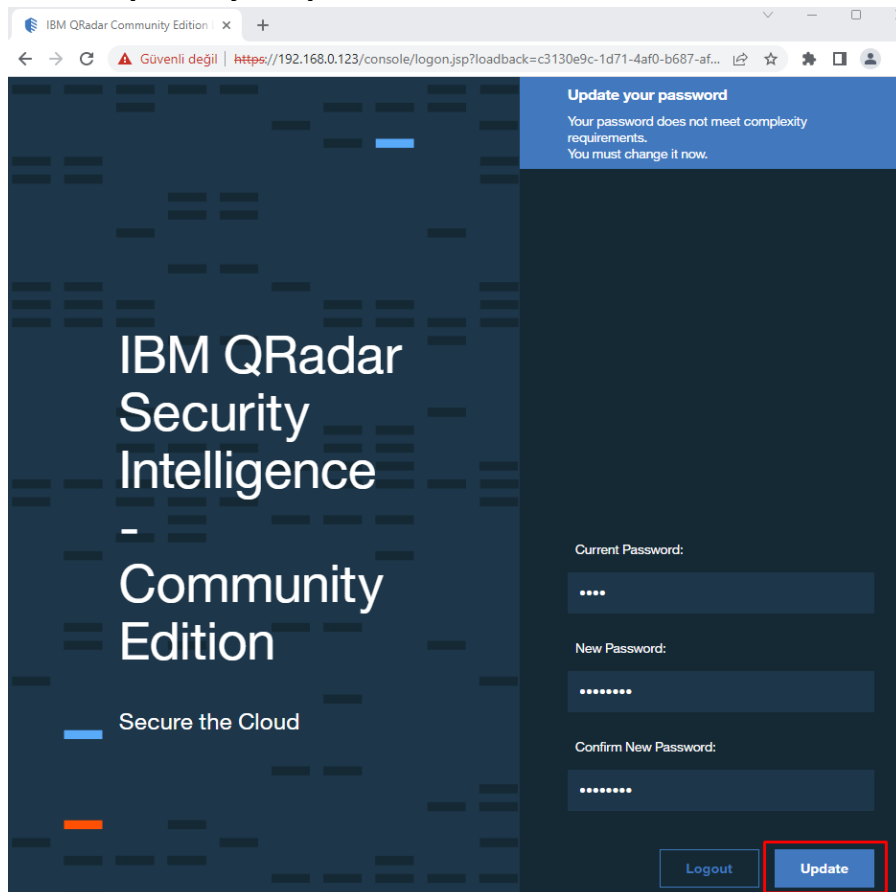
Secure the Cloud

Username  
admin

Password  
....

Login

## 29- Update your password



Update your password  
Your password does not meet complexity requirements.  
You must change it now.

IBM QRadar  
Security  
Intelligence  
—  
Community  
Edition

Secure the Cloud

Current Password:  
....

New Password:  
.....

Confirm New Password:  
.....

Logout Update



## 30- Accept the agreement license

QRadar CE - EULA

← → ↻ Güvenli değil | https://192.168.0.123/console/eula/eula.jsp

QRadar Community Edition - License Agreement

Review the license terms before logging in. Türkçe

Yönetimi Düzenlemeleri de dahil olmak üzere ithalat ya da ihracat yasalarına, düzenlemelerine veya ilkelere tabi olabilir. Lisans Alan Taraf, A.B.D.'deki ihracat veya yeniden ihracat sınırlamaları da dahil olmak, ancak tüm bunlarla sınırlı olmamak üzere bu Programın ihracatına, ithalatına veya kullanımına ilişkin tüm geçerli yasa, düzenleme ve ilkelere uygun davranmaktan tümüyle kendisinin sorumlu olduğunu kabul eder. Bu Programın ihracat sınıflandırmasını edinmek için aşağıdaki URL adresini ziyaret edin: <https://www.ibm.com/products/exporting/>.

Üçüncü Kişi Lehtarlar

Aşağıdaki sağlayıcılardan her biri bu Sözleşmenin bir üçüncü kişi lehtarıdır.  
Oracle America, Inc.

Yukarıdakilere ek olarak, aşağıdaki koşullar Lisans Alan Tarafın bu Programı kullanımı için geçerlidir.

**Programın Yasalara Uygun Kullanımı:**  
Bu Program, lisans Alan Tarafın güvenlik ortamını ve verilerini geliştirmesine yardımcı olmak için tasarlanmıştır. Bu Programın kullanılması çeşitli yasalara veya yasal düzenlemelere tabi olabilir; bunlara gizlilik, veri koruması, istihdam ve elektronik iletişim ve depolamayla ilgili olanlar dahildir. Bu Program yalnızca yasalara uygun amaçlarla ve yasalara uygun şekilde kullanılabilir. Lisans Alan Taraf Programı geçerli yasalara, yasal düzenlemelere ve ilkelere uygun olarak kullanmayı kabul eder ve bunlara uymakla ilgili tüm sorumluluğu üstlenir. Lisans Alan Taraf, Programın yasalara uygun kullanımı için gerekli tüm onay, izin ya da lisansları edineceğini ya da edinmiş olduğunu beyan eder.

**Bulut Hizmet Sağlayıcı:**  
Lisans Alan Taraf, Programın kuruluş kılavuzunda belirtilen ve yazılım uygulamalarının barındırılması için altyapı hizmetleri, ağ hizmeti, depolama ve veri merkezi alanı içeren lisans sağlayan bir üçüncü kişi ("Bulut Hizmet Sağlayıcı") ortamına Programı kurabilir. Bu yetki, Lisans Alan Tarafın geçerli olan lisans sözleşmesinde yer alan herhangi bir yükümlülüğünü değiştirmez veya herhangi bir yükümlülüğünün yerini almaz; bunlara sanallaştırılmış bir ortamda kullanıma dair gereksinimler de dahildir. Lisans Alan Taraf, geçerli olan lisans sözleşmesindeki doğrulama terimlerinin, Programın kurulu olduğu Bulut Hizmet Sağlayıcı ortamını kapsadığını ve gereken tüm kullanım verilerini toplamayı kabul eder. Lisans Alan Taraf Bulut Hizmet Sağlayıcıya hiçbir izinsiz kullanım veya Programa izinsiz erişim sağlamayacaktır.

L/N: L-KFRN-BH7JG3  
D/N: L-KFRN-BH7JG3  
P/N: L-KFRN-BH7JG3

Decline

Accept

## 31- That's It 😊

QRadar - Dashboard

← → ↻ Güvenli değil | https://192.168.0.123/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin System Time: 22:57

Show Dashboard: Threat and Security Monitoring

Next Refresh: 00:00:55

New Dashboard Rename Dashboard Delete Dashboard Add Item...

Default:IDS / IPS-All: Top Alarm Signatures (Event Count)

There was no Time Series data for the search performed.

[View in Log Activity](#)

Top Systems Attacked (IDS/IDP/IPS) (Event Count)

There was no Time Series data for the search performed.

[View in Log Activity](#)

Top Systems Sourcing Attacks (IDS/IDP/IPS) (Event Count)

My Offenses

No results were returned for this item.

Most Severe Offenses

No results were returned for this item.

Most Recent Offenses

No results were returned for this item.

Top Services Denied through Firewalls (Event Count)

There was no Time Series data for the search performed.

[View in Log Activity](#)

Flow Bias (Total Bytes)

There was no Time Series data for the search performed.

[View in Network Activity](#)

Top Category Types

No results were returned for this item.

Top Sources

No results were returned for this item.

Top Local Destinations

No results were returned for this item.

Qlradar - Log Activity

Try Qlradar SIEM | IBM Security C...IBMSec Community - YouTube

←→↻

Güvenli değil | https://192.168.0.123/console/qlradar/jsp/Qlradar.jsp

🔍🌟🔖📱👤⋮

☰

IBM Qlradar Security Intelligence - Community Edition

🔔👤

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Admin

System Time: 04:37

Search...

Quick Searches

Add Filter

Save Criteria

Save Results

Cancel

False Positive

Rules

Actions

⏸🔍

Quick Filter

Search

Viewing real time events

View: Select An Option:

Display: Default (Normalized)

	Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:46	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:46	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:46	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:45	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:44	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:43	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:39	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:29	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Warning Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Warning	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Warning Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Warning	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Warning Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Warning	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:30	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴
	API request successful	SIM Audit-2 : qlradar	1	21 May 2023 04:37:29	SIM User Action	192.168.0.35	0	192.168.0.123	0	admin	🔴🔴
	Information Message	System Notification-2 : qlradar	1	21 May 2023 04:37:29	Information	192.168.0.123	0	127.0.0.1	0	N/A	🟡🔴