



Installation Guideline

Product: Antikor v2 - Next Generation Firewall
Guides

Installation Guideline

Online Review

[Click](#) to review Antikor online.

Username: demo_en

Password: demo_en

Steps That Must Be Made Before Installation

Product Verification Producers

Verification procedure by the receiving party is performed by comparing md5sum of the received media.

- Customer ensures that the security seal is not broken upon receiving.
- Customer verifies the product name and version.
- Customer generates an md5sum of the medium and compares it to the md5sum of the ISO at the official web page.
- Installation process can begin if the computed md5sum and the md5sum available at the webpage are the same.

Physical and Logical Security

1. The Antikor installed hardware must be located in the secured system room Entry and exit to the room should only be done by authorized persons.
2. Backups of the Antikor should be kept regularly.
3. If the Antikor installed has USB ports on the hardware, it must be disabled.
4. The hardware which the Antikor is installed the power supply and ethernet cables, etc. must be checked.
5. The password information of people who will access the Antikor should not be the same as the admin password and their authority should be restricted.
6. Users accessing the Antikor must change their password at specific time periods.
7. The security of the user name and password information of the system administrators who access the Antikor is their own responsibility. By using this software, the system administrator accepts that has taken the necessary measures to protect the security of the user name and password information. Epati Information Technologies accepts no cost or liability if there is a direct or indirect loss resulting from the security of the user name and password information.

Hardware Requirements

Computers work according to the slowest component. As can be seen from the following articles, each

component has many parameters. The most important components in any Firewall are CPU, Ram Speed, Ethernet, and a Hard-disc. These components determine the Internet traffic that passes through the device. Throughput on Firewalls is affected by all peripheral components, from input (Ethernet), where packets are processed (CPU-Ram), to self-connected switches and Internet Bandwidth.

Components required for Antikor, an Integrated Cyber Security System are as follows:

1. Minimum 8 Core Xeon (excluding logical cores)
2. Minimum 32 GB DDR4 2133 Mhz Ram
3. Minimum 4 port multi queue Ethernet adapter
4. Minimum 256 GB SSD

CPU (Processor)

Applications that require intensive computing, games and physical calculations are the areas where CPUs becomes important.

Antikor software supports multithreading. Therefore, there must be at least 8 cores as Processor.

RAM (Memory)

The RAM on the Firewalls is the unit where all operations and package checks are performed. For this reason, RAM speed is very important. Latency is the time difference (delay) between packets entering and leaving a system. AntiKor's RAM speed should be minimum DDR4-2133 Mhz. Today, the emergence of DDR5 memory and doubling of data paths is a major development for Firewalls.

Ethernet (Network) Adapter

In any Firewall the Ethernet Adapter must be a multi-queue Ethernet Adapter. This will allow Ethernet drivers to disperse onto multiple core.

Recommended Ethernet adapters are as follows:

- Intel i210 Ethernet adapter 2 port 1 GBit/s (for SMEs)

<https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/i210-ethernet-controller-datasheet.pdf>

- Intel 4 port 1GBit/s i350 Ethernet adapter, with each port has 8 TX/RX paths, meaning that Ethernet drivers can be dispersed on total 32 cores (for medium size SMEs)

<http://www.intel.com/content/www/us/en/ethernet-controllers/ethernet-i350-server-adapter-brief.html>

- The other 2-port Intel x540 models also running 10 GBit /s, and each port can be distributed to 128 queues (For larger enterprises)

<http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-x540-datasheet.pdf>

- Again another 4-port Intel x710T models running at 10 GBit/s (For larger enterprises)

<http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/intel-10-gigabit-server-adapters/intel-ethernet-converged-network-adapter-x710-series/intel-ethernet-converged-network-adapter-x710-t4.html>

Hard Disk (Storage)

If the program to be used has a heavy hard disk usage rate, requiring constant writing onto and reading from disk, the hard disc become more important. Hard disks vary in size and speed. Types of disk include SATA Disks, SAS Disks, SSS Disks, and recently SSD NVMe Disks are introduced to market. When the system administrators commission a service or system, they consider only the capacity with respect to disk

requirement. Naturally, when load becomes heavier in the medium and long term bottlenecks occur thereby resulting in losses in performance. The only reason for this is that total IOPS and Throughput have not been correctly estimated, or been taken into account at all. So, what are these values and what functions do they have? As name suggests, IOPS (Input/output operations per second) is the maximum number of writing or reading operation per second while Throughput represent the task carried out at a certain interval. Generally, this is the value indicating how much data is written or read in MB per second.

For example, in the case of camera software size more important. Software's writing speed is constant. We may think that total workload of this particular server shall be comprised of 10% reading and 90% writing. Reading occurs only when we browse the images we have taken.

Let's take FTP file servers as another example. Total workload of this serves shall be comprised of 80% reading and 20% writing. Generally, downloading from file serve entails reading from the disk while uploading a file entails writing on a disk.

Functional IOPS = ((Total IOPS *writing %*)/(Raid penalty))+(Total IOPS*reading %*)

Note: In this formula RAID 0 shall be calculated as Raid Penalty 1, RAID 1 as Raid Penalty 2, RAID 5 s Raid Penalty 4, and RAID 6 as Raid Penalty 6.

As can be seen, the same discs give completely different results with different raid structures and reading and writing rates. Because Antikor entails database operations and Logging, at least 256GB SSD Disk type is preferred as disk type and size.

Note: After you perform the Antikor setup any hardware other than RAM should not be mount (ethernert card, harddisk etc.). Because, the Antikor will switch to "safe mode" for security purposes and will not perform its function.

1. For the device to be installed, Ethernet cards must be connected in accordance with the network structure or Ethernet cards must be opened if the virtual installation is to be performed. For example, if WAN, LAN, and DMZ are to be used, 3-port Ethernet card or 3 separate Ethernet cards must be connected. If installing via virtualization, 3 Ethernet ports should be opened. The Ethernet card should not be added or removed after the installation is complete.

2. For the device that has been set up, the "Last State" setting must be on continuously. For this the BIOS settings must be checked.

Note: If there is a firewall in the network environment where Antikor is to be installed, the server IP address where Antikor is installed, the ports 7001 and 7002 must be open for communication with the license server. These ports can only be opened for access to the IP address of the Antikor license server. You can contact the Technical Team for the license server IP address.

For testing;

```
telnet lisans.epati.com.tr 7001
telnet lisans.epati.com.tr 7002
```

Installation Phase

[Click.](#)

to GET ISO File

```
CD Loader 1.2

Building the boot loader arguments
Looking up /BOOT/LOADER... File not found
Looking up /boot/loader... Found
Relocating the loader and the BTX
Starting the BTX loader

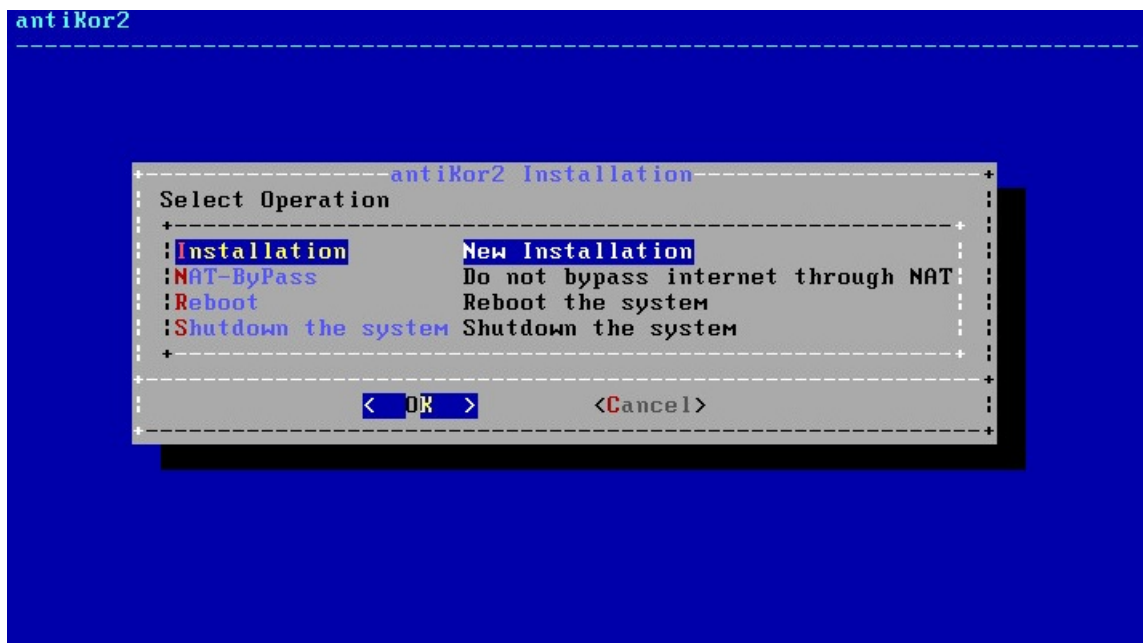
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive C: is disk0
BIOS 639kB/1047488kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
(root@antiKor2.epati.com.tr, Thu Sep  7 11:01:07 EEST 2017)
Loading /boot/defaults/loader.conf
/boot/kernel/kernel text=0x1034450 _
```

When “CD Loader” is written on the first line on the screen above, it indicates that the installation has started.

Choose Language

If the CD successfully runs, Language Chooseion will appear first prior to installation. Choose the desired language and click OK.



In above screen; “Installation” is for a New Antikor version.

- Nat-Bypass

is for accessing Internet by bypassing Antikor, which is already installed.

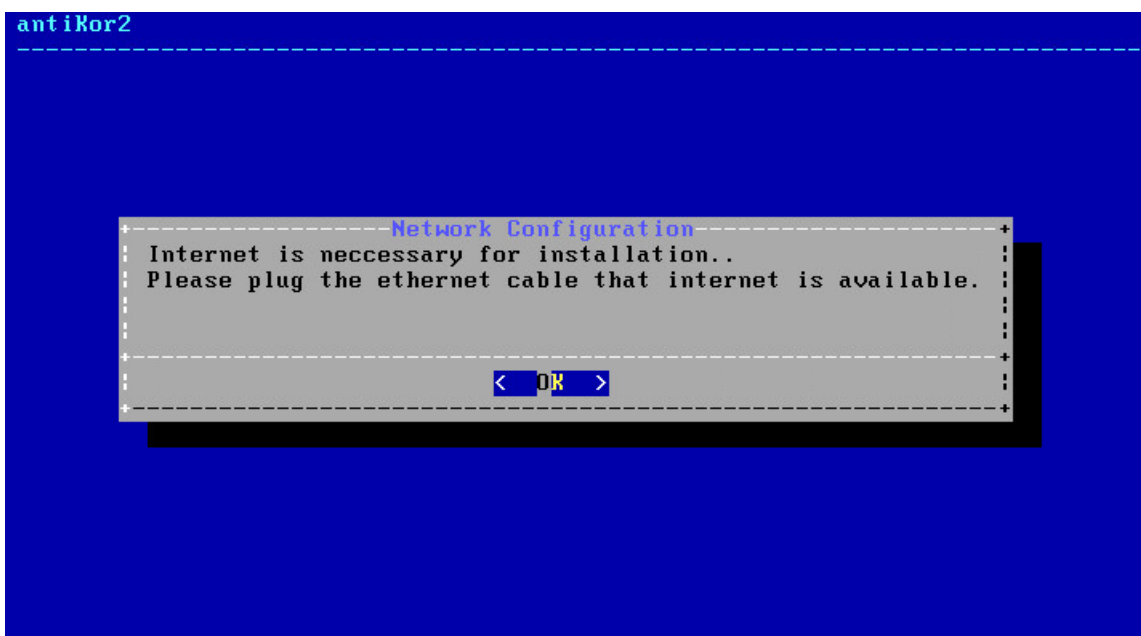
- Re-start

is for restarting the installation.

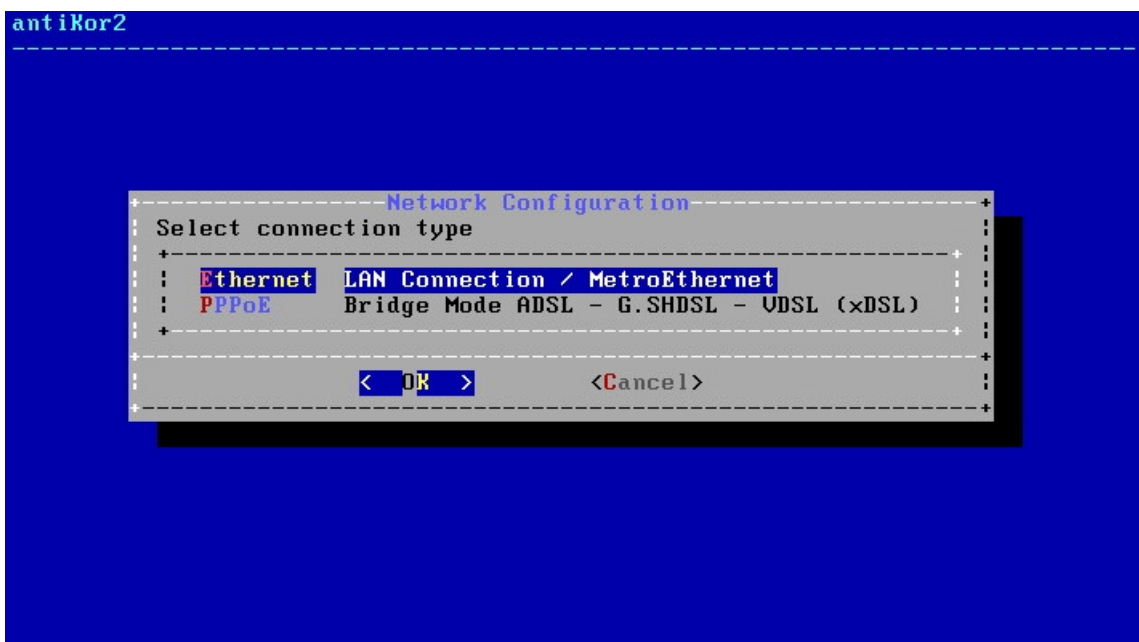
- Shut Down System

is for powering of the system.

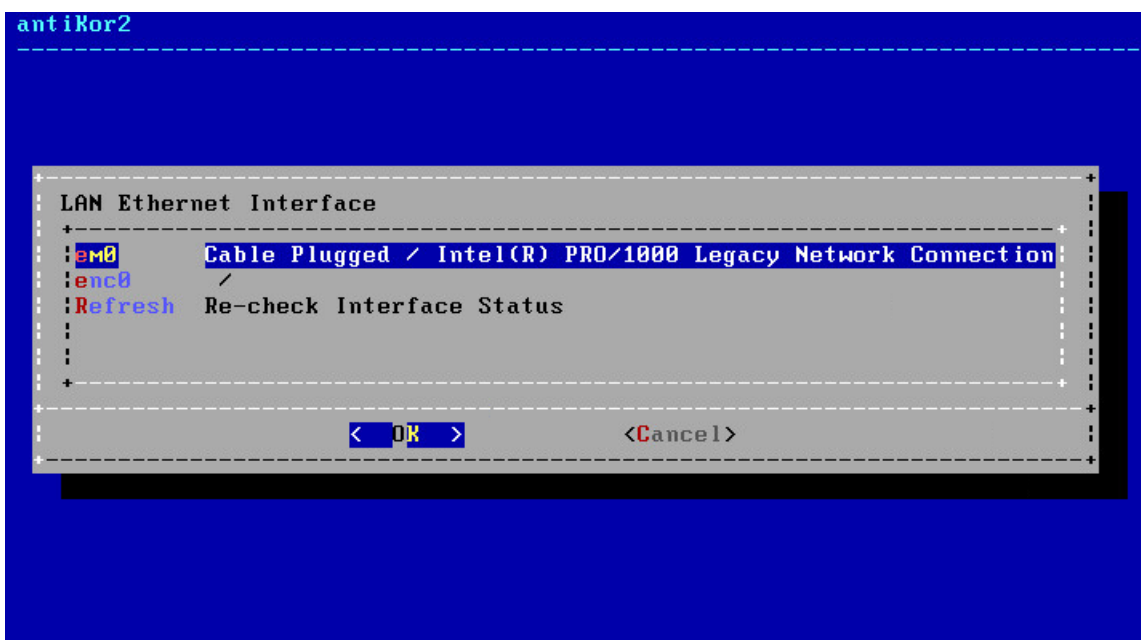
Since you are going to perform a new installation we choose “Installation” and proceed.



Ethernet connection is needed for installation.

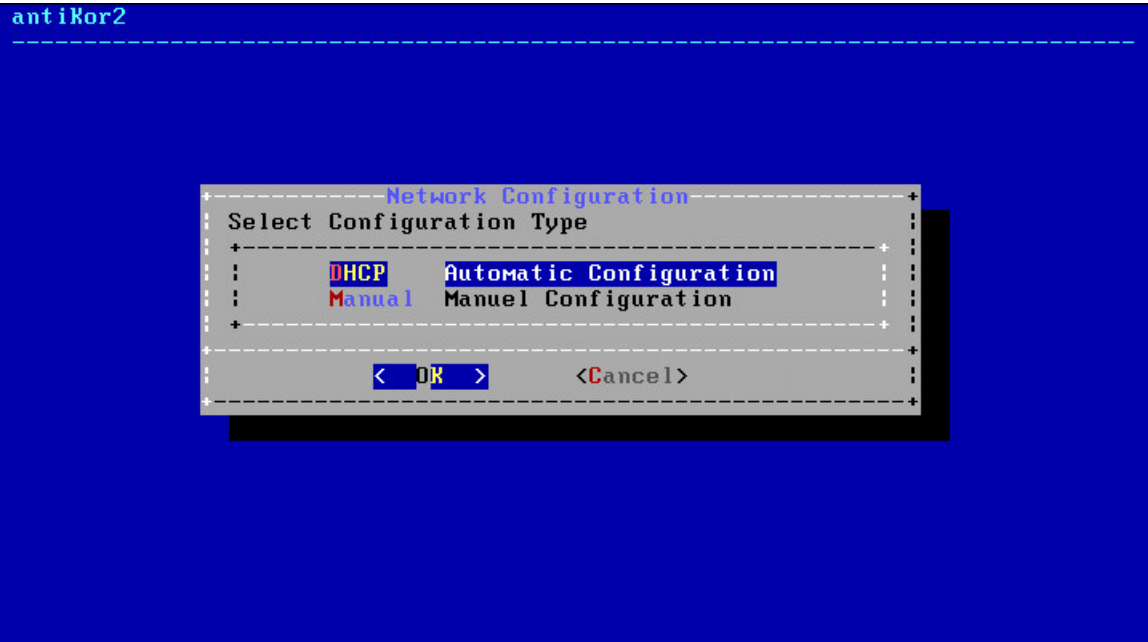


Choose Internet connection type.

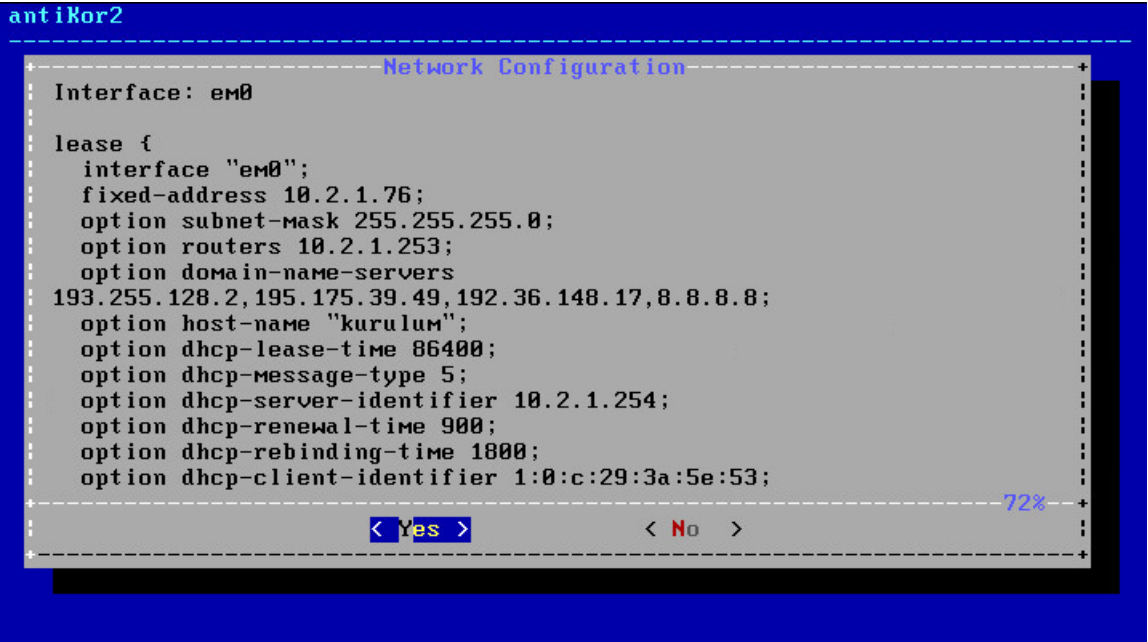


In this screen there are 4 Intel Ethernet connections. Choose desired Ethernet connection for installation and proceed with installation.

Note: In the event no Ethernet adapter is showed, check connections and choose “Refresh Recheck Status” option.



By choosing DHCP, the system will connect to the Internet by chooseing an IP from the list of IPs that are being distributed. If there is no system to distribute IP, a manual IP is taken thereby connecting to Internet.



If the internet access is available as stated above, the authorized IP block to access the Antikor shall be specified.

antiKor2

Network Configuration

Allowed network address 0.0.0.0/0

< OK > <Cancel>

Enter License number in next screen.

antiKor2

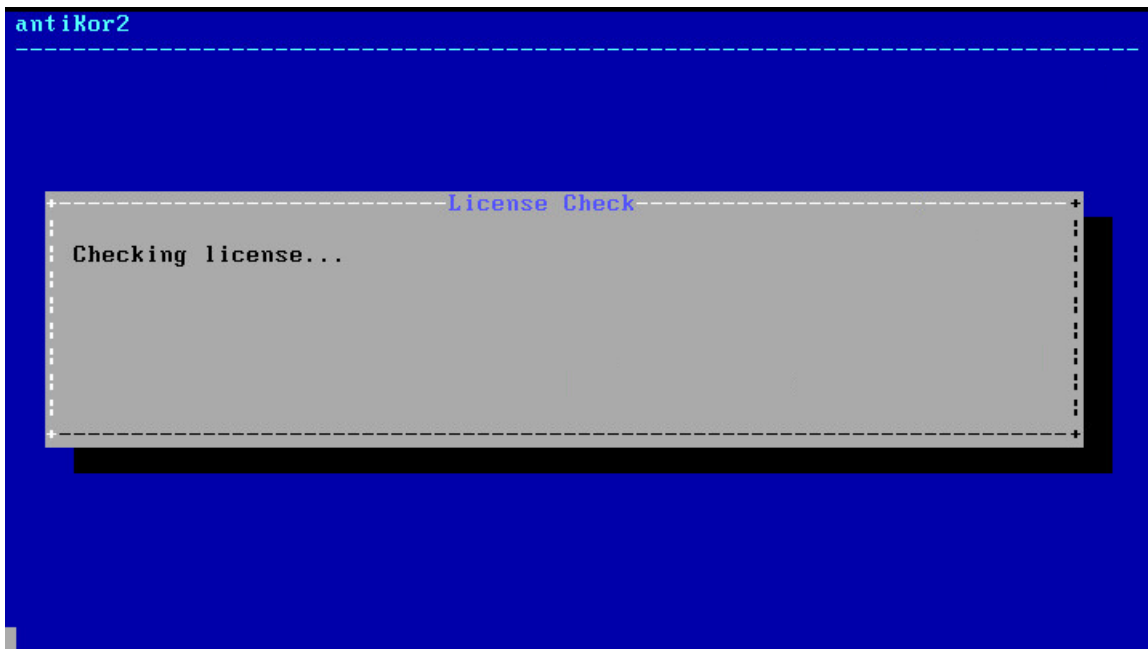
License Check

Please type license key.

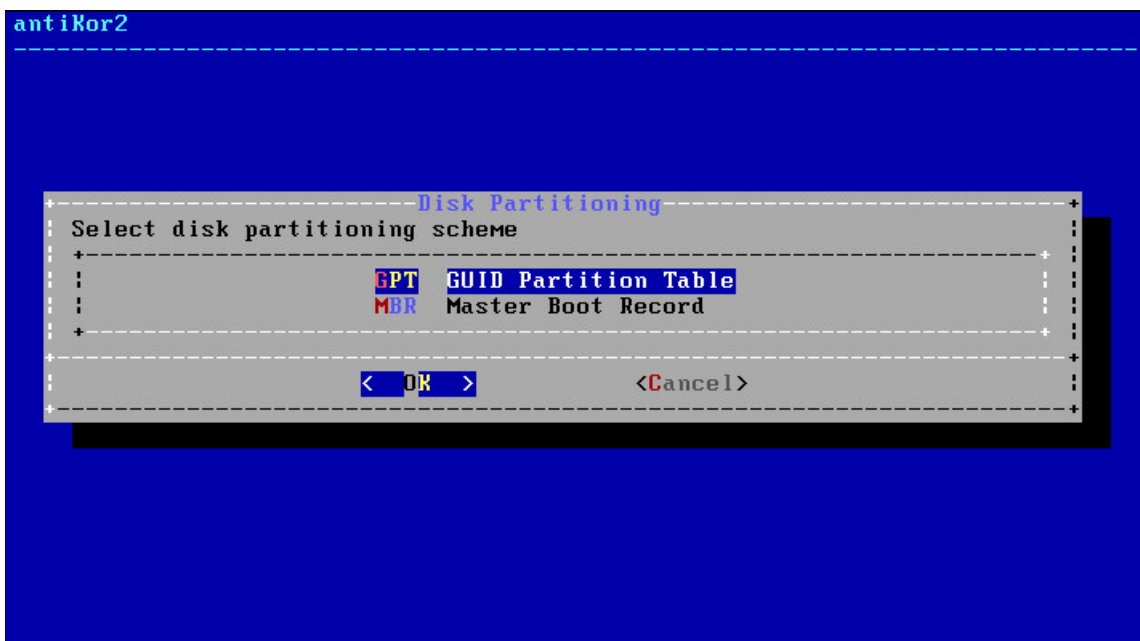
:

< OK > <Cancel>

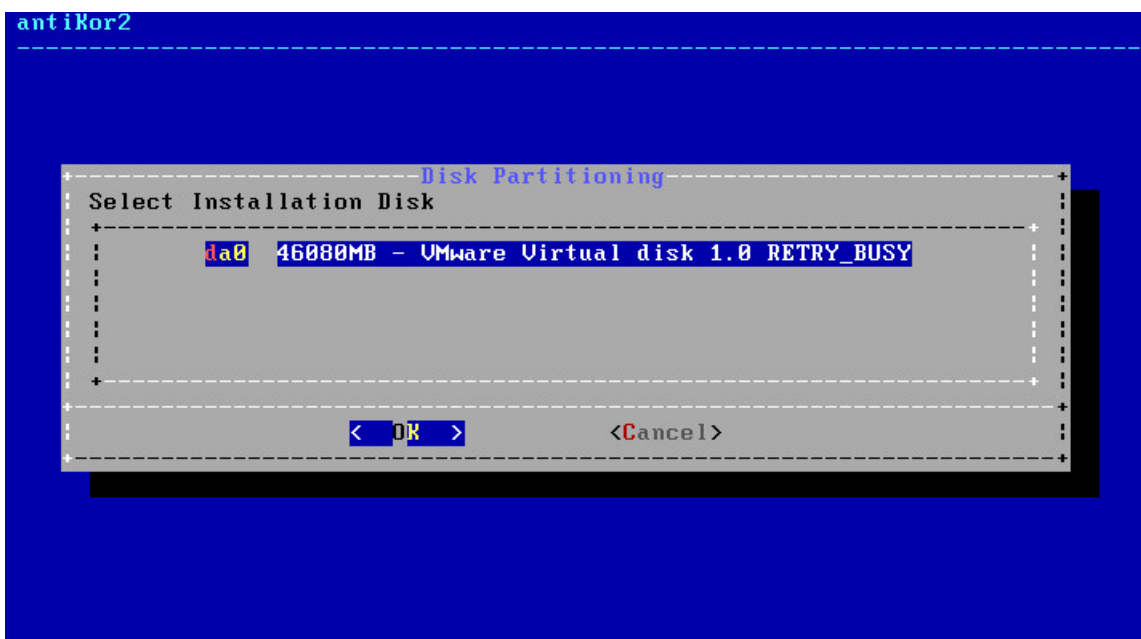
Package shall begin to be downloaded if License is verified.



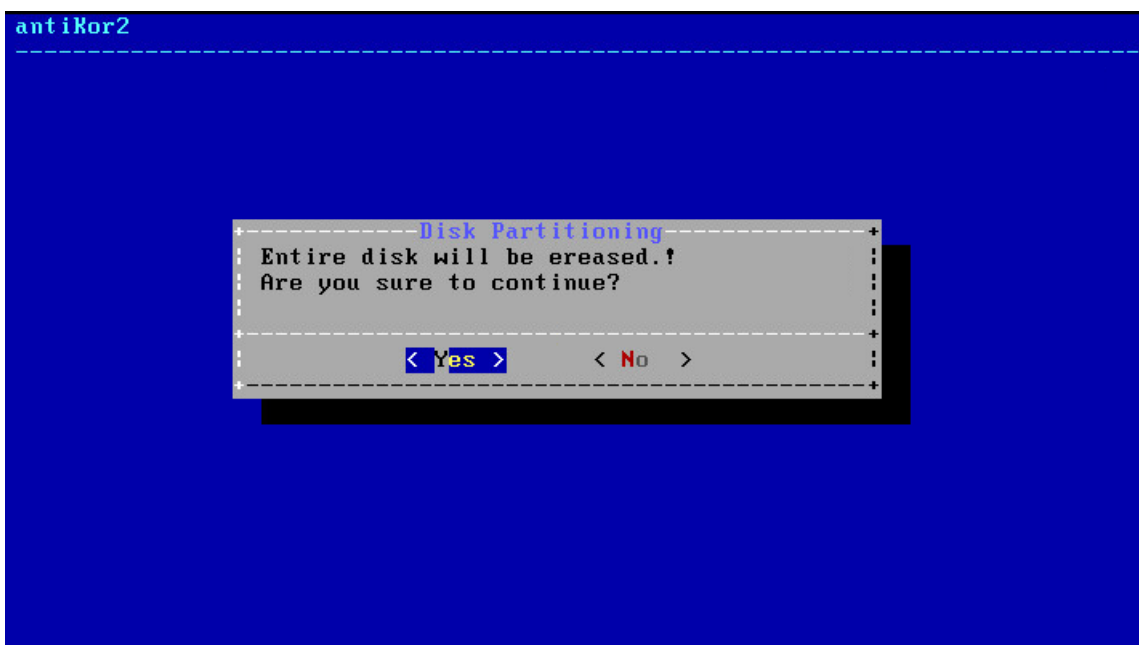
System installation will start after the package download is finished. The next screen is the fdisk process. We should choose GPT in the Disk Partitioning diagram. GPT supports larger disk volumes. MBR does not support disks with capacity more than 2TB.



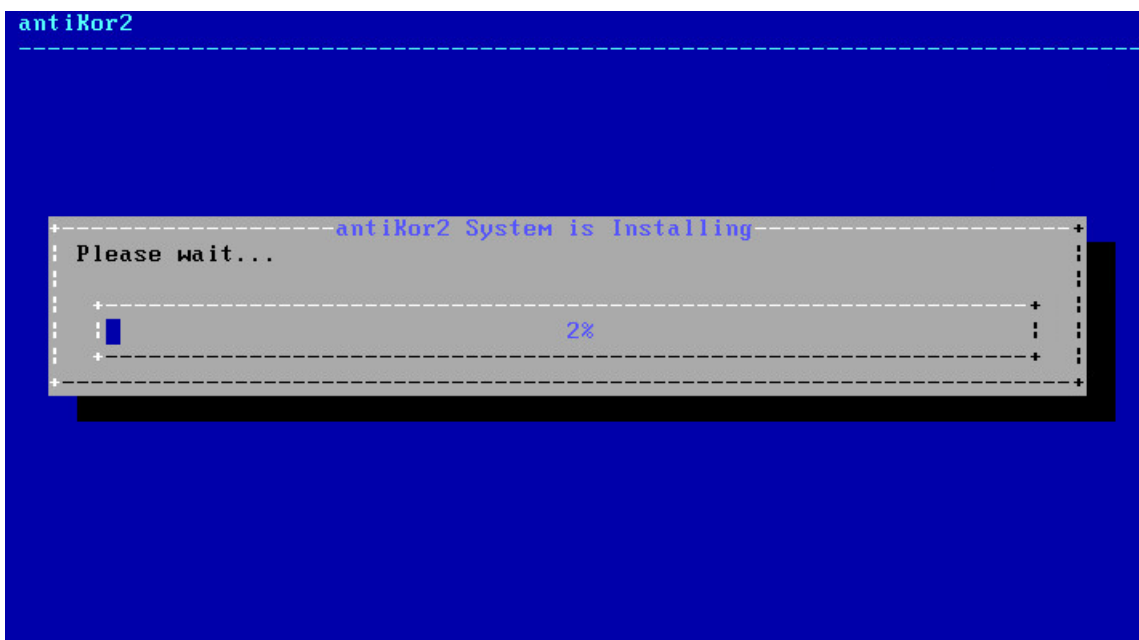
In Disk Configuration screen, choose disk where the installation shall take place.



The system informs you that all data in the disk will be erased.

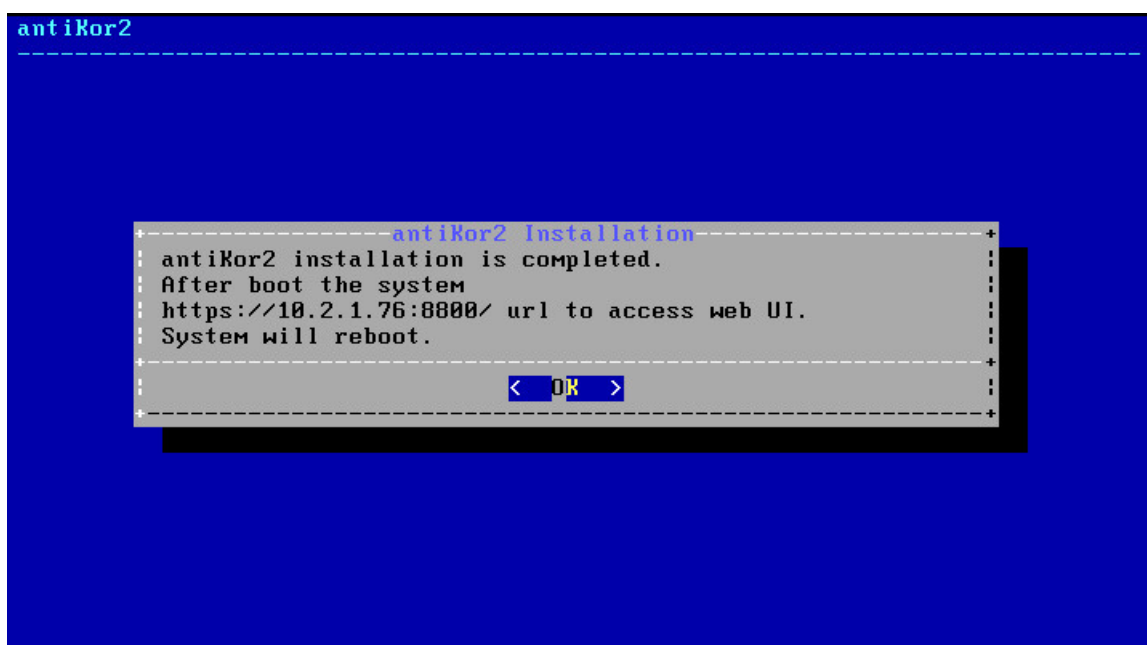


Antikor2 installation begins.

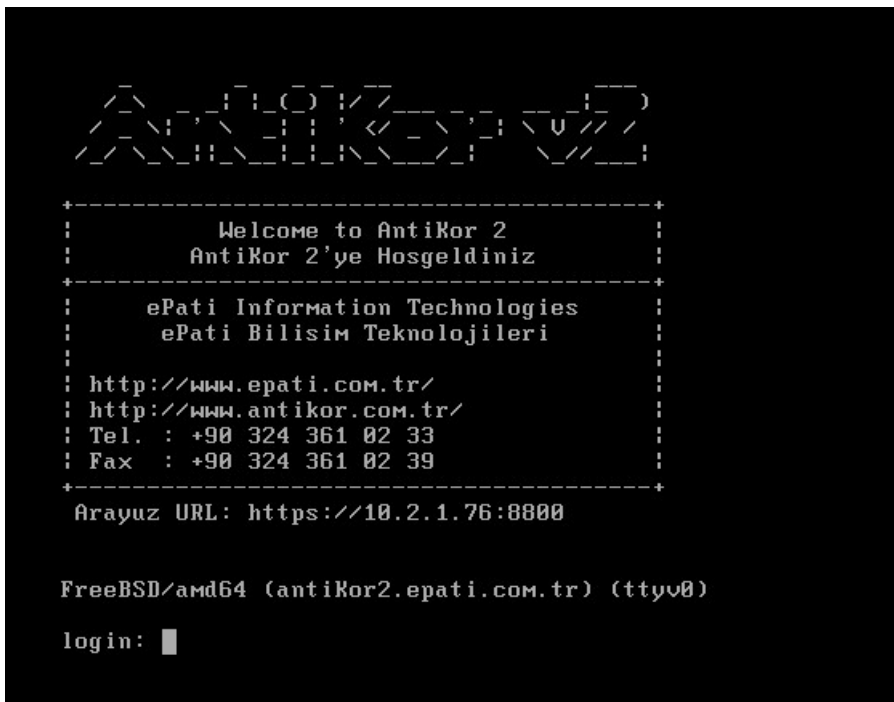


antiKor2		
INSTALLING PACKAGES		
Arayuz Modulu	2.0.682	Downloading
Arac Kutusu	2.0.11	Pending (Download)
Yonetimsel Araclar	2.0.11	Pending (Download)
Yapilandirma Yoneticisi	2.0.254	Pending (Download)
Haberlesme Modulu	2.0.371	Up-to-date
Haberlesme Aracisi	2.0.15	Pending (Download)
URL Kategori Veritabani	2.0.28	Pending (Download)
Uygulama Imza Veritabani	2.0.8908	Pending (Download)
Web Erisim Loglari	2.0.10	Pending (Download)
Proxy Kimlik Dogrulama	2.0.4	Pending (Download)
Balkupu Modulu	2.0.18	Pending (Download)
Layer2 Anormallik	RC-2.0.7	Pending (Download)
Modul Yoneticisi	2.0.15	Up-to-date
Yoneticici Konsolu	2.0.18	Pending (Download)
Epati Network Isletim	RC-2.0.9	Up-to-date
Bant Genisligi Monitoru	2.0.0	Pending (Download)
Kamu SM - Zamane	2.0.5	Pending (Download)
Arayuz Modulu (Halka	2.0.4	Pending (Download)
Acik)		

The following message is showed when installation is completed.



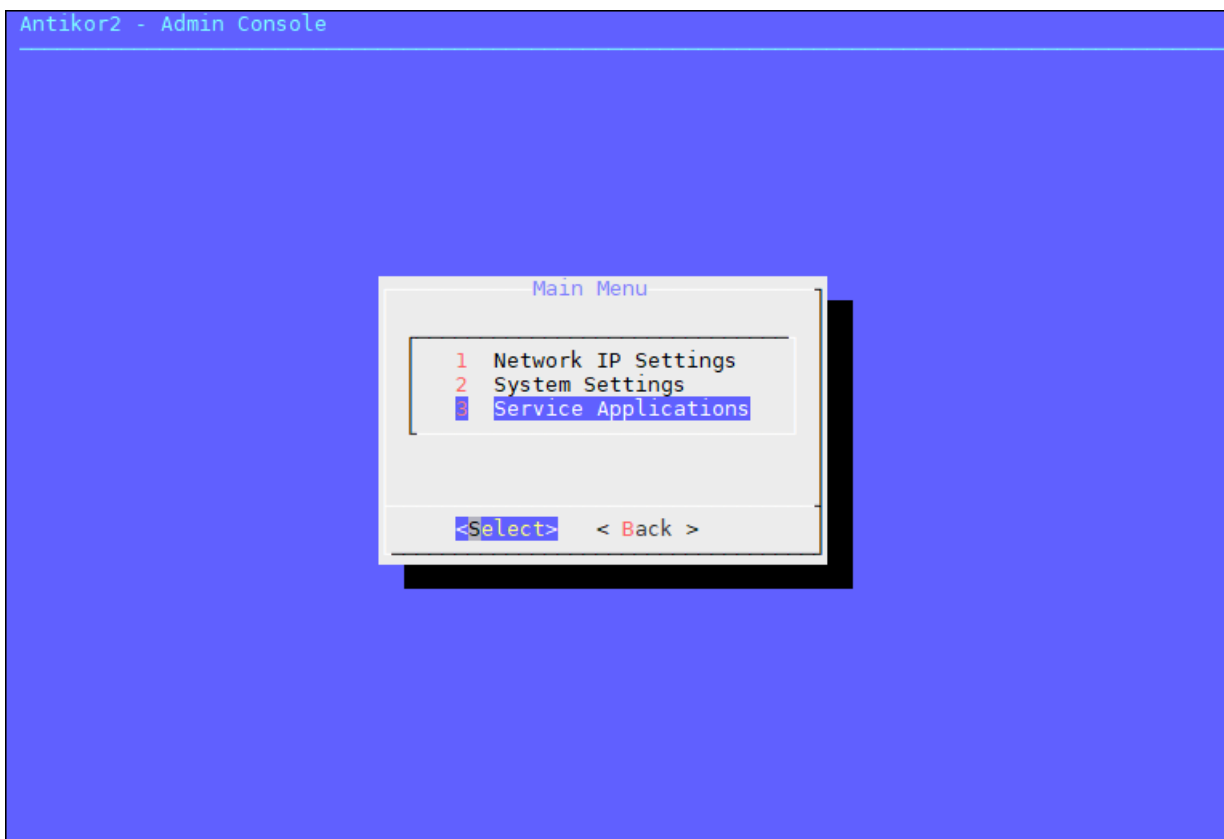
The system restarts and following screen appears. The system is ready. The above is typed in the address bar to log into web interface. During initial login type antikor for username (admin) and password.



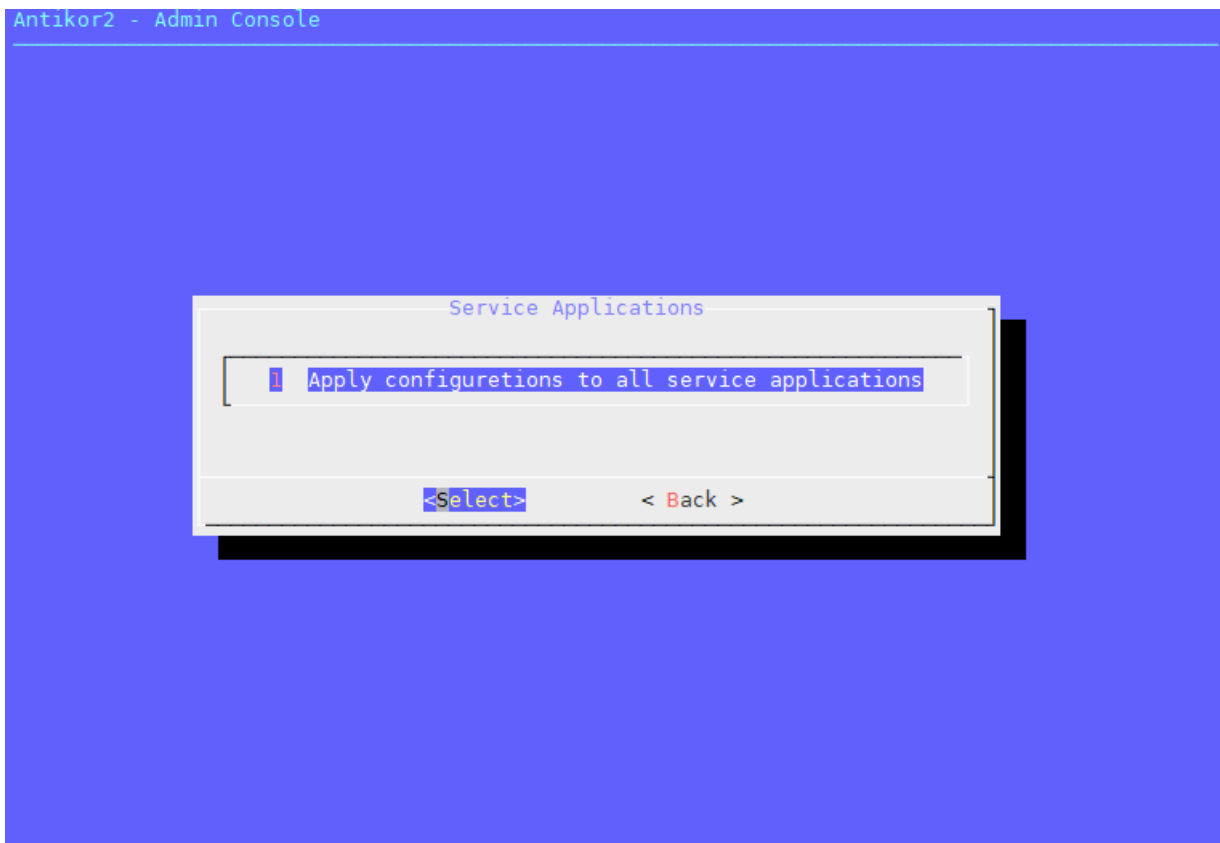
In both console and web interface type antikor for username (admin) and password.

Steps That Must Be Made After Installation

1. Enter The Service Applications menu.



Click the “ Apply configurations to all service applications” Button and wait for the configurations to finish.

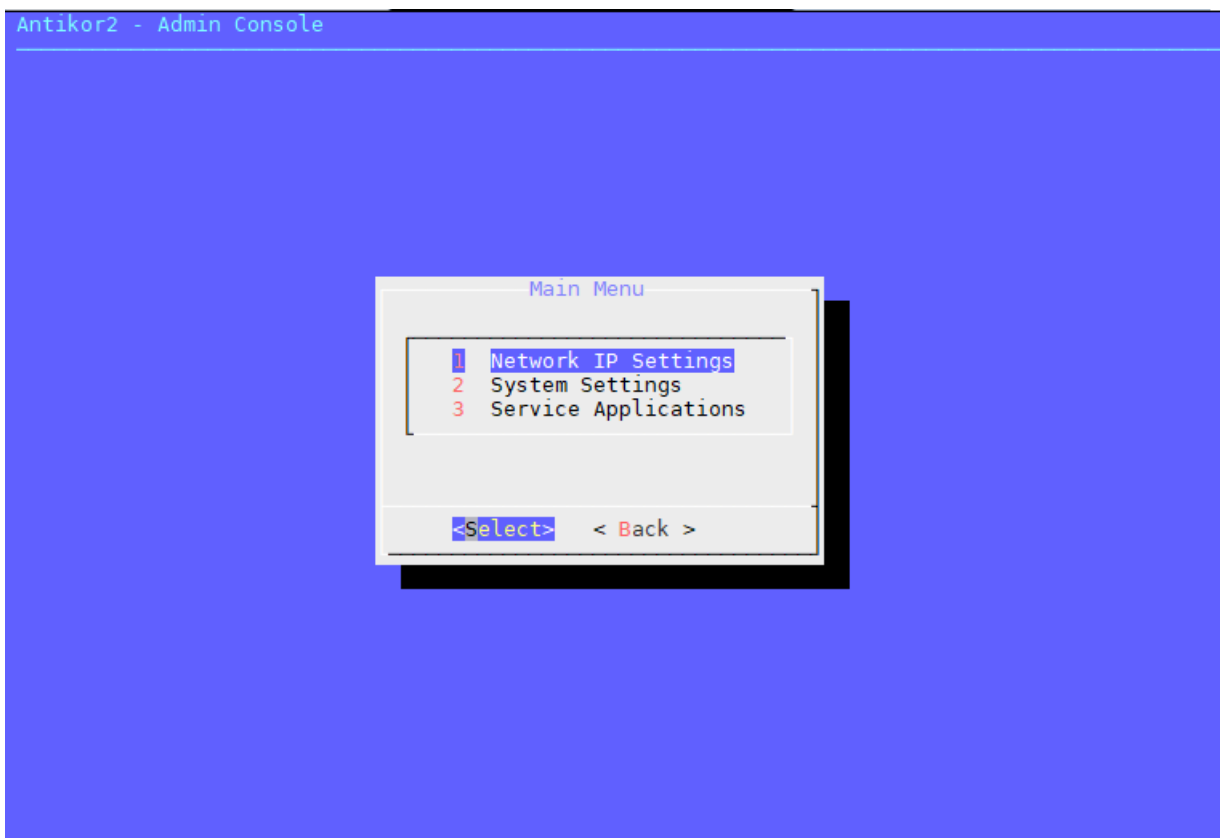


Once the process is complete, the Antikor must be restarted.

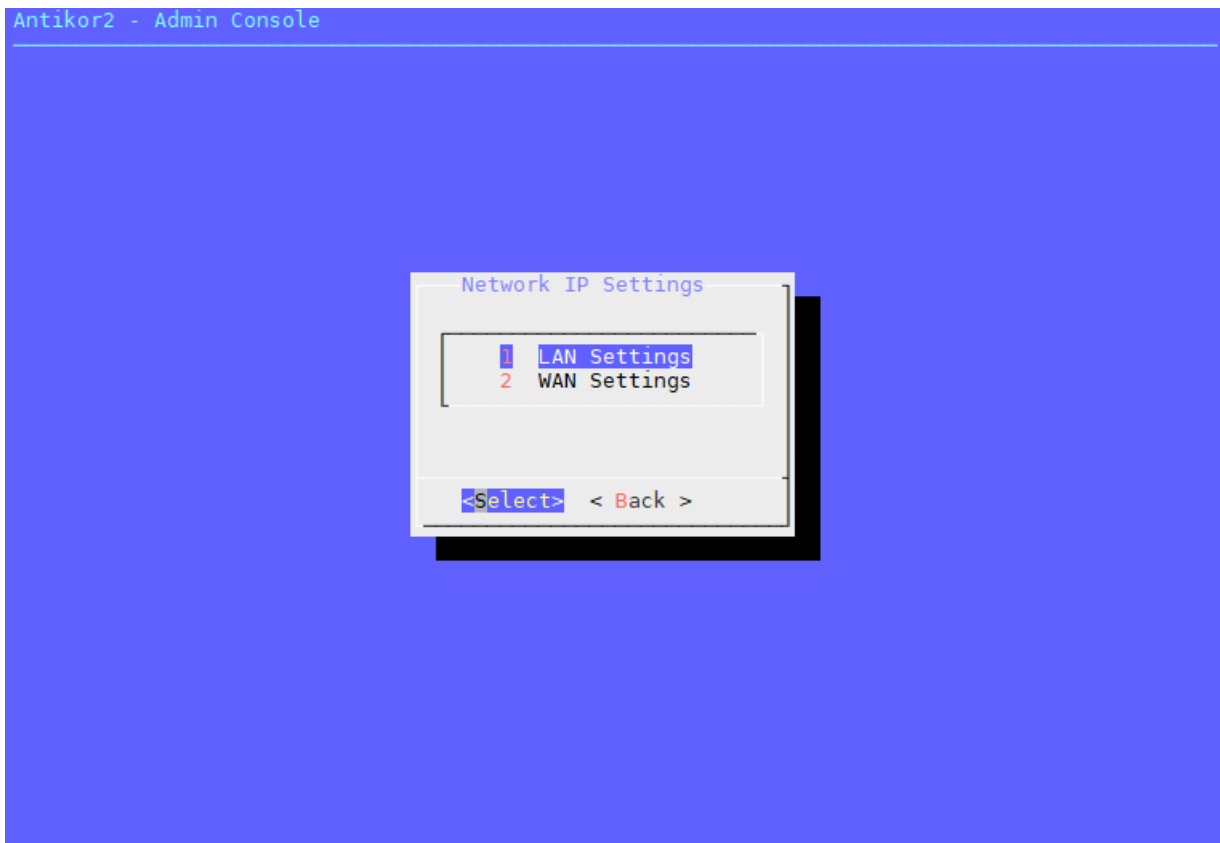
2. IP assignment must be done from on the Admin Console.

```
Username: admin
Password: antikor
```

The first thing to do is to open the Network&IP settings menu.

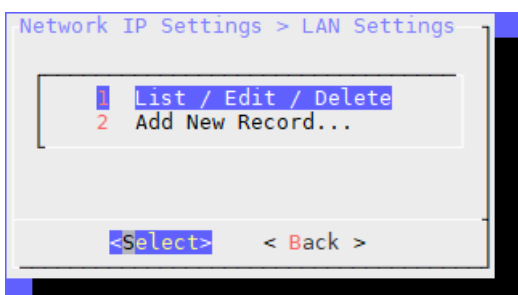


Select the Ethernet port to edit.

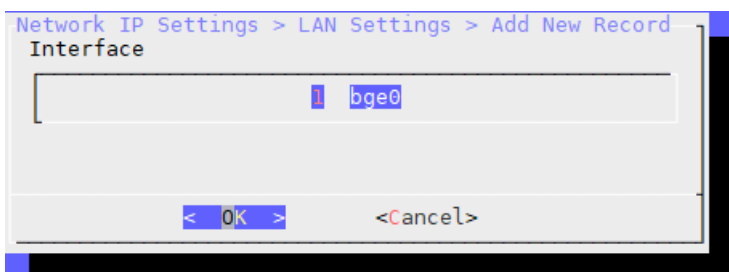


When you open the LAN Settings menu;

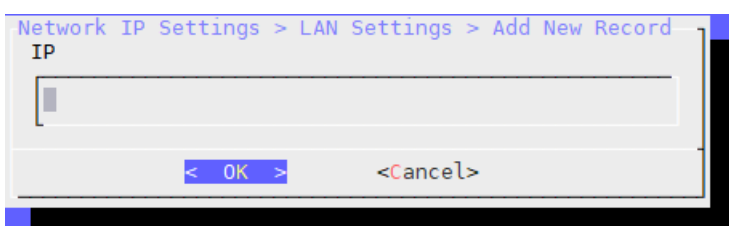
Two submenus will appear. If there is no record, the “Add New Record...” is selected.

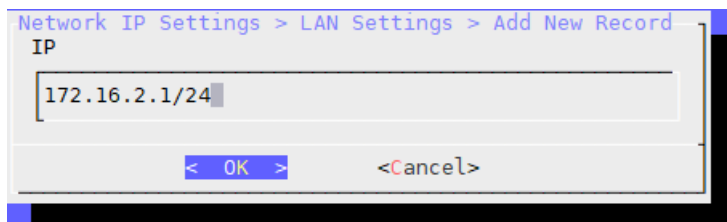


When the Add New Record is selected, the Ethernet ports on the device will be displayed. Select the Ethernet port to use for the LAN.

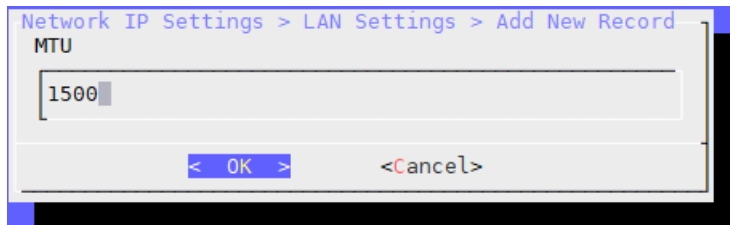


In the IP field, type the IP and subnet mask to use in the LAN IP block.





The MTU value is 1500.

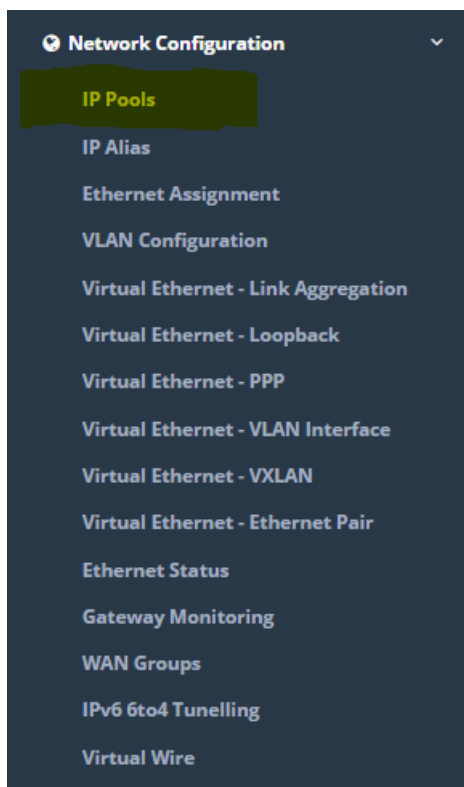


After this process, we have defined the IP for the LAN port.
For other ethernet ports, IP addresses can be given in the same way.

3. To enter the WEB interface, we can manually add an IP address that is covered by the LAN IP block to our computer.

We can access the WEB interface with <http://172.16.2.1:8800> IP address.

4. Click the IP Pool under the Network Configuration menu.



Click when "Add" button, the IP pool the for LAN will be determined.

IP Pools - New Record ✕

Ethernet

LAN1 ▼

Address Family

☒ IPv4 ☐ IPv6

IP Block

IPv4

172.16.2.0/24

Description

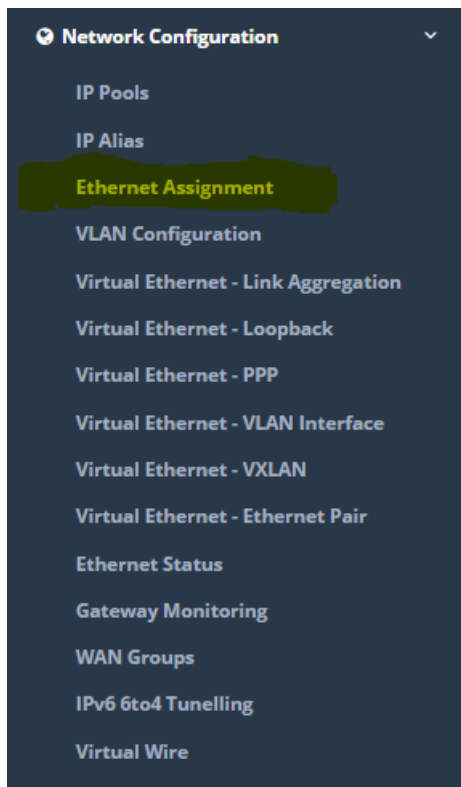
for LAN

Cancel

Save

Click when Save button, the IP pool the for LAN port was be determined. For other ethernet ports, IP addresses can be given in the same way.

5. Click the Ethernet Assignment under the Network Configuration.



Click when LAN Add button, LAN Ethernet Assignment are performed.

Reload

Add WAN

Add LAN

Add DMZ

Add PPPoE

The corresponding settings for the LAN port have been entered. For other ethernet ports, Ethernet Assignment can be make in the same way.

Ethernet States

Status Active

Security Zone Select...

Interface

Ethernet Name le1 - Advanced Micro I

Speed 10base5/AUI mediaop

MTU 1500

Web Interface Access Active

Cluster Membership Positive

Cluster Ethernet Name

Description

IPv4 Settings

☐ Obtain IPv4 Automatically

IPv4 Address IPv4 10.10.10.10/24

DHCPv4 Pool Mode Distribute IP to All Clients x

DHCPv4 Start IPv4

DHCPv4 End IPv4

DHCPv4 Gateway IPv4

DHCPv4 Relay Address IPv4

Lease Time 1 Day(s)

Options

☐ MAC-IP Pairing

☒ Anti-Spoof

☐ Registration

☐ Make announcement

☐ DHCPv6 Server

☒ DHCPv4 Server

☐ DHCPv6 Relay

☐ DHCPv4 Relay

☐ Managed Flag

☐ Other Flag

IPv6 Settings

☐ Obtain IPv6 Automatically

EUI64 Positive

IPv6 Address IPv6 ffff::1/8

DHCPv6 Start IPv6

DHCPv6 End IPv6

DHCPv6 Relay Address IPv6

Cancel

Save

If “DHCPv4 Server” is checked in the options section while performing the Ethernet assignment; The DHCPv4 Service, which is located under the service statuses on the dashboard, should be started.

Note: After installation, no ethernet card should be not mount and dismantl.

6. The default password (antibody) of the admin user needs to be changed.

- Go to User Settings page.

antikor

antikor v2 NGFW - EPA-NGFW-G1-TR

antikor v2 NGFW

admin

Antikor Admin

User Settings

Logout

Dashboard

System Utilization

CPU 42%

Memory 66%

Disk 4%

Service Status

Honeypot Service Running

Blackhole Service Not Configured

Anti-Spoof Service Closed

Apply Changes 1

Click the **Change User Password** button on the User Settings page.

antikor

antikor v2 NGFW - EPA-NGFW-G1-TR

antikor v2 NGFW

admin

Antikor Admin

Dashboard

Definitions

System Settings

Network Configuration

Announcement & Form Management

Reports

Authentication Rules

Hotspot Management

Instant Observation

Security Settings


Security Profiles

User Settings

Apply Changes 1

User Settings

Profile picture



Username : admin

User Informations

Name : Antikor

Surname : admin

Identification number : 11111111111


Phone : 3243610233

Email : bilgi@epati.com.tr

Birthday : 2008-06-08

First Login Date : 2023-03-16 11:20:41.626987+03

Upload Profile Photo

Profile Photo :  Upload

Language setting

☐ tr ☒ en

Navbar Position

☒ Fixed ☐ Static

Change Password

Change User Password


Two Factor Authentication

Two Factor Authentication Settings


- The password is changed.

Update Your Password


Old Password



New Password




New Again




Save

Update Your Password


Old Password



New Password



New Again



Save

- After changing the password, the new password assigned to the admin user is logged in.

antikor

antikor v2 NGFW

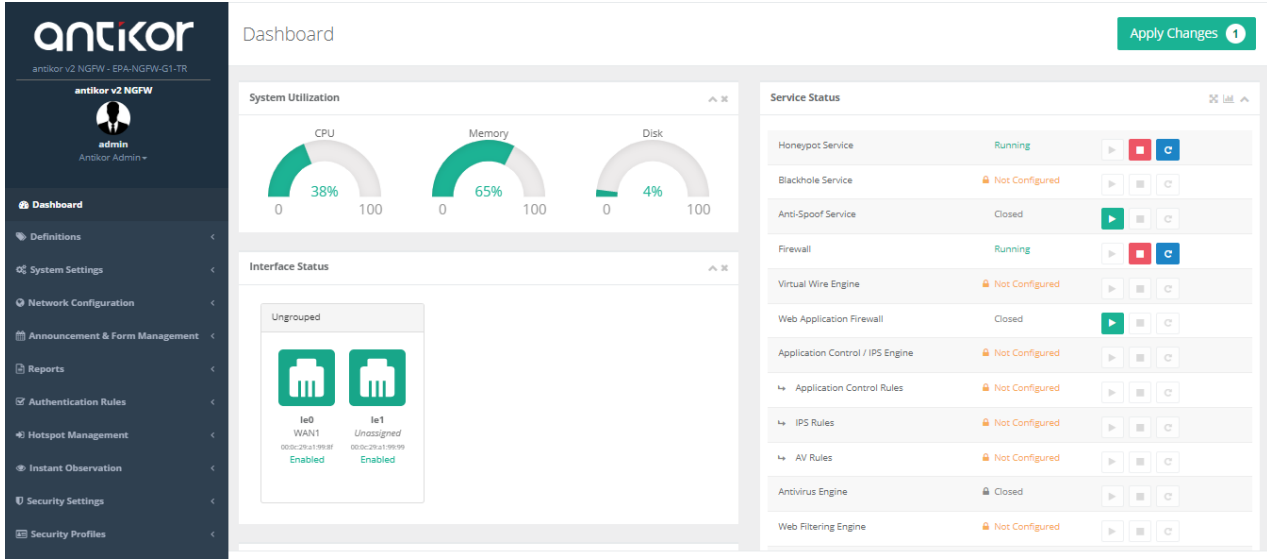
Giriş yapmak için bilgileri giriniz.

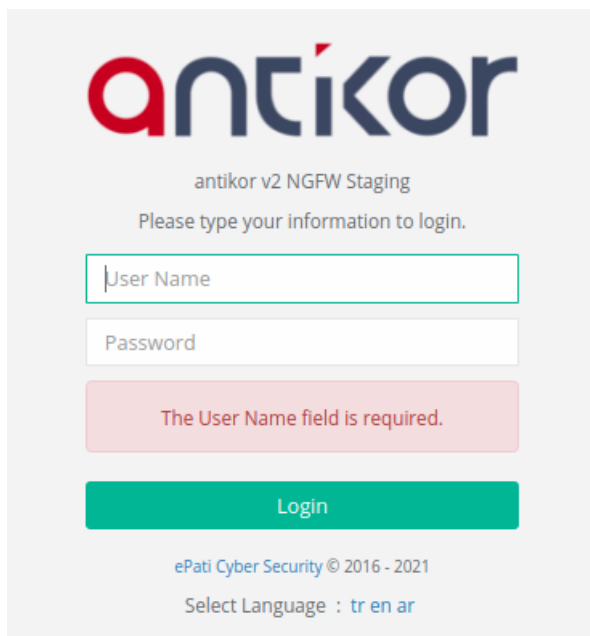
admin

Giriş

ePati Siber Güvenlik © 2016 -2023

Dil Seçiniz : tr en





antikor

antikor v2 NGFW Staging

Please type your information to login.

User Name

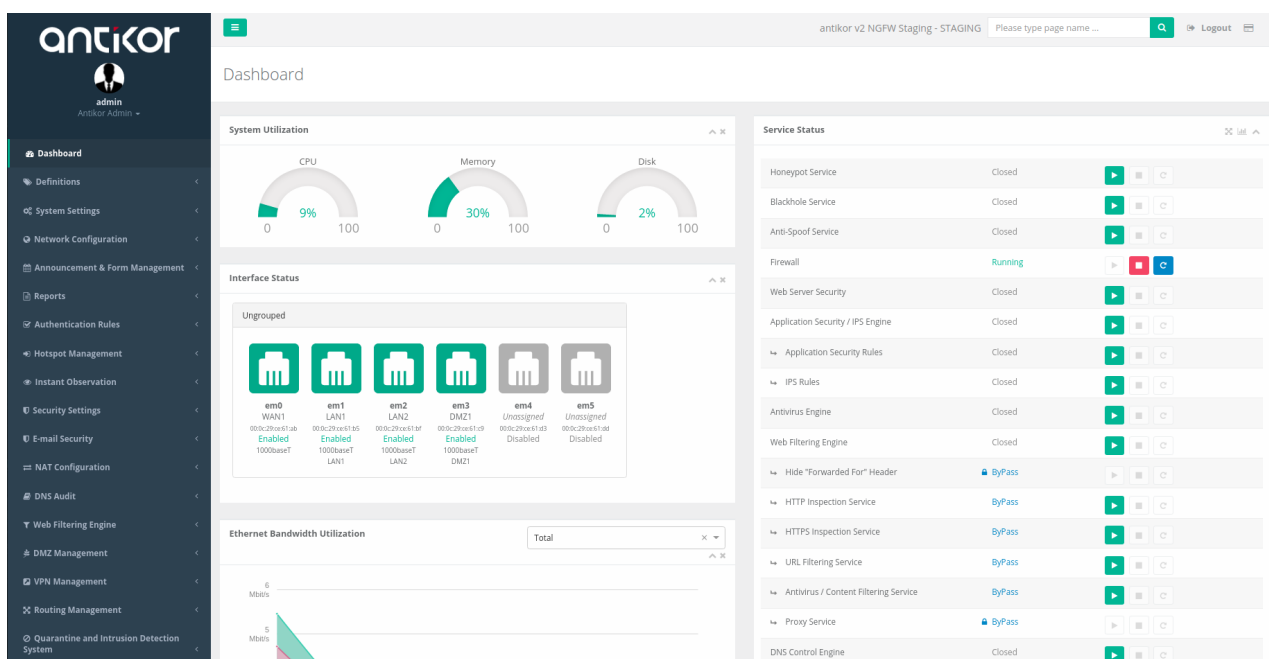
Password

The User Name field is required.

Login

ePati Cyber Security © 2016 - 2021

Select Language : tr en ar



antikor v2 NGFW Staging - STAGING

Please type page name ...

Logout

Dashboard

System Utilization

CPU: 9%

Memory: 30%

Disk: 2%

Interface Status

Un grouped

em0	em1	em2	em3	em4	em5
WAN1	LAN1	LAN2	DMZ1	Unassigned	Unassigned
00:0c:29:a6:51:a3	00:0c:29:a6:51:a5	00:0c:29:a6:51:a7	00:0c:29:a6:51:a9	00:0c:29:a6:51:a3	00:0c:29:a6:51:a5
Enabled	Enabled	Enabled	Enabled	Disabled	Disabled
1000baseT	1000baseT	1000baseT	1000baseT		

Ethernet Bandwidth Utilization

Total

6 MB/s

5 MB/s

Service Status

Service	Status	Actions
Honeypot Service	Closed	▶ ◻ ◻
Blackhole Service	Closed	▶ ◻ ◻
Anti-Spoof Service	Closed	▶ ◻ ◻
Firewall	Running	▶ ◻ ◻
Web Server Security	Closed	▶ ◻ ◻
Application Security / IPS Engine	Closed	▶ ◻ ◻
Application Security Rules	Closed	▶ ◻ ◻
IPS Rules	Closed	▶ ◻ ◻
Antivirus Engine	Closed	▶ ◻ ◻
Web Filtering Engine	Closed	▶ ◻ ◻
Hide "Forwarded For" Header	ByPass	▶ ◻ ◻
HTTP Inspection Service	ByPass	▶ ◻ ◻
HTTPS Inspection Service	ByPass	▶ ◻ ◻
URL Filtering Service	ByPass	▶ ◻ ◻
Antivirus / Content Filtering Service	ByPass	▶ ◻ ◻
Proxy Service	ByPass	▶ ◻ ◻
DNS Control Engine	Closed	▶ ◻ ◻

After login the interface, firstly for security must change password. Click Management Panel Users under the Management Panel Settings menu.

Management Panel Users

Reload Add

XLS CSV PDF

Show/Hide Records Per Page OK Filter Reset Filter

#	Status	Name	Surname	Username	Actions
1	Active	Antikor	Admin	admin	Edit Delete Group Members Authorities and Roles Details Certificate Management


After then click "Details" button.

On opened page the "Edit" button click.

Management Panel Users

[Switch User](#) [Edit](#) [Return](#)

Antikor Admin



Username : admin

User Informations

Name/Surname : Antikor Admin

Username : admin

eMail : bilgi@epati.com.tr

Creation Date :

Login IP Address : 172.16.33.1

Login Date : 2021-05-10 14:40:06+00

Last Login IP Address : 172.16.33.1

Last Login Date : 2021-05-10 14:33:57+00

Login Number : 7

Creator :


Copyright ePati © 2016 - 2021 antikor v2 NGFW Staging - STAGING

In the User Information section, click the **Change User Password** button.

Management Panel Users

[Switch User](#) [Edit](#) [Return](#)

Antikor Admin



Username : admin

User Informations

Name/Surname : Antikor Admin

Username : admin

eMail : bilgi@epati.com.tr

Creation Date :

Login IP Address : 172.16.33.1

Login Date : 2021-05-10 14:40:06+00

Last Login IP Address : 172.16.33.1

Last Login Date : 2021-05-10 14:33:57+00

Login Number : 7

Creator :

Upload Profile Photo

Profile Photo : [Upload](#)

ID Informations

Name

Antikor

Surname

Admin

Email

bilgi@epati.com.tr

User Informations

Username

admin

Change User Password

[Cancel](#) [Save](#)

In the Update Password page, enter the new password and click the **Save** button.

Update Your Password

Old Password

New Password

New Again

Save

Institutional Security Policy

Click, the Management Panel Settings under the Management Panel Settings menu.

For the WEB interface Limitless Access can be opened or that can Limited Access can be specified.

Management Panel Settings

Service Settings

Web Interface Access Protocol ☒ https ☐ http

Service Port Number

Cpu Rezervation For Management Panel

Independent Management Infrastructure

Session Settings

Log Traffic

Certificate Based Authentication

Authentication From External Source

Operation Mode

Service Cases

#	Ethernet Name	IP Address	Interface	Web Interface Access
1	em0	172.16.33.10/24	WAN1	<input type="button" value="Open"/>
2	em1	192.168.33.10/24	LAN1	<input type="button" value="Open"/>
3	em2	192.168.34.10/24	LAN2	<input type="button" value="Open"/>
4	em3	192.168.168.10/24	DMZ1	<input type="button" value="Open"/>

Accessible Networks

#	IP Address	Description	Actions
1	0.0.0.0/0		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Session Settings

Log Traffic

Closed

Certificate Based Authentication

Closed

Authentication From External Source

Closed

Operation Mode

Limited Access

Save

Accessible Networks

Reload

Add

XLS

CSV

PDF

#	IP Address	Description	Actions
1	0.0.0.0/0		<div>Edit</div> <div>Delete</div>

«

<

1

>

»

Go

Safe Mode

If any hardware other than Ram is added after the Antikor setup is made, the Antikor switches to Safe Mode for security purposes and does not perform its function. The hardware that has been added must be removed so that the Antikor can continue its function prior to Safe Mode. Re-installation is required to ensure that the hardware is work compatible with the Antikor.

Actions to be Performed after a Failure in the System

In the event of a failure in the system, please follow the steps below.

1. Regarding the failure, after post process which the malfunction occurred technical support should be requested with the details encountered and error output.
2. If the failure affects only certain services, the service should be closed.
3. If the fault has a negative effect on the whole system and the backup system is present, the backup system must be activated.

ePati Cyber Security Technologies Inc.
Mersin Universitesi Ciftlikkoy Kampusu
Teknopark Idari Binasi Kat: 4 No: 411
Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

www.epati.com.tr
info@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

