



FastNAC



DEVICE PROFILING

Contents:

1. Beginning	3
2. Adding a Profile	4
3. Profile Details Page	5
4. Adding Profile Rules	6
5. Profile Rule Types	7
5.1. MAC Address	7
5.1.1. MAC Address	7
5.1.2. MAC Manufacturer Information	7
5.2. By IP Address	8
5.3. By Location	9
5.3.1. Location Information	9
5.3.2. Switch/Port Information	10
5.4. Domain Control	10
5.4.1. Domain Device Control	11
5.4.2. Domain User Control	11
5.5. Active Directory	12
5.6. HTTP/HTTPS	12
5.7. Telnet/SSH	14
5.7.1. Telnet	15
5.7.2. SSH	16
5.8. DHCP Fingerprint	17
5.8.1. Manufacturer Information	17
5.8.2. Device Name (Hostname)	17
5.8.3. Parameters	18
5.9. TCP/UDP Port	18
5.10. SNMP	19
5.11. Posture	19
5.11.1. Windows	20
5.11.1.1. Operating System Control	20
5.11.1.2. Program Control	21
5.11.1.2.1. Program Name	21
5.11.1.2.2. Program Version	22
5.11.1.3. Service Inspection	22
5.11.2. Linux	23
5.11.2.1. Operating System Control	23
5.11.2.2. Program Control	24
5.11.2.2.1. Program Name	24
5.11.2.2.2. Program Version	25
5.11.2.3. Service Inspection	25

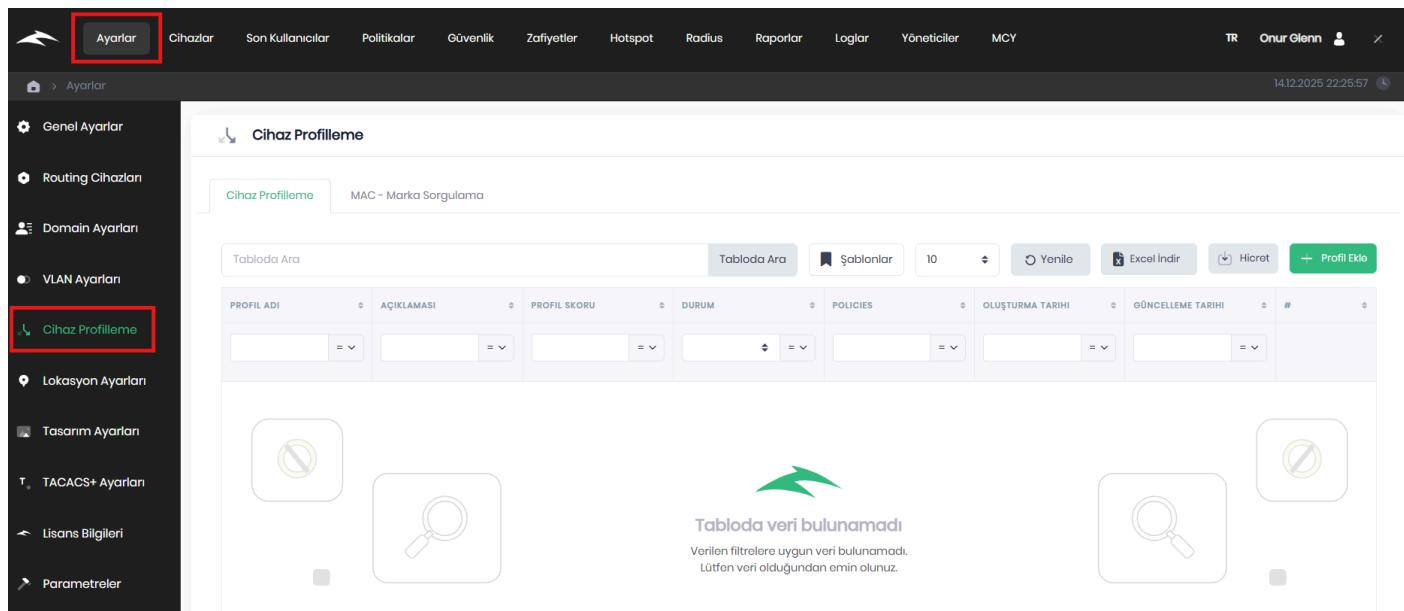
5.11.3. File Tracking	26
5.11.4. Session Monitoring	26
5.12. NMAP	27
6. Profile and Scoring System and Examples	27
6.1. Example IP_Camera Profile	28
6.2. Sample Printer Profile	30
6.3. Example IoT Device Profile	33

1. Beginning

FastNAC allows you to classify IoT or similar devices on your network using multiple profiling methods simultaneously. The devices can be categorized as follows:

- Based on MAC addresses or MAC manufacturer information,
- Based on IP addresses or IP blocks,
- Depending on its location or Switch/Port information,
- According to Active Directory attributes,
- We scan the content using the HTTP/HTTPS method,
- By running a command via Telnet/SSH and analyzing the output,
- DHCP Fingerprint;
 - According to the manufacturer's information,
 - Based on the hostname,
 - According to fingerprint parameters
- Depending on TCP/UDP port status (open/closed/filtered),
- By sending an SNMP request and depending on the response received,
- For Windows operating system;
 - According to the operating system control,
 - Depending on whether the program is installed or not in Windows,
 - According to the version information of the program installed in Windows,
 - Depending on the situation, you can see which services are running/not running within Windows.
- For the Linux operating system;
 - According to the operating system control,
 - Depending on whether the program is installed or not in Linux,
 - According to the version information of the program installed in Linux,
 - In Linux, the services that are running/not running depend on the situation.
- Depending on the path of a file within the operating system,
- Based on login time,
- According to the results of the NMAP scan (you can use custom parameters),

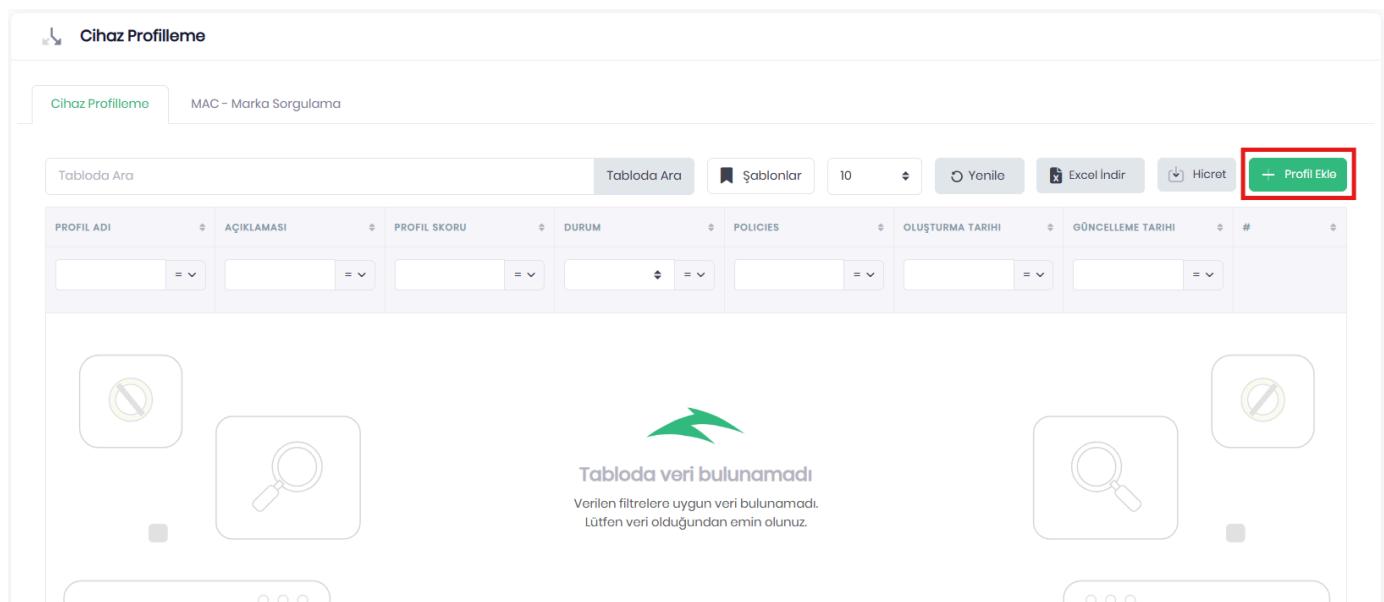
You can classify them using methods such as these. You can access Device Profiling settings under **the Settings -> Device Profiling** menu.



The screenshot shows the 'Cihaz Profilreme' (Device Profiling) screen. The top navigation bar includes links for Ayarlar, Cihazlar, Son Kullanıcılar, Politikalar, Güvenlik, Zayıfyetler, Hotspot, Radius, Raporlar, Loglar, Yöneticiler, and MCY. The top right corner shows the user 'Onur Glenn' and the date '14.12.2025 22:25:57'. The left sidebar lists configuration categories: Genel Ayarlar, Routing Cihazları, Domain Ayarları, VLAN Ayarları, Cihaz Profilreme (highlighted with a red box), Lokasyon Ayarları, Tasarım Ayarları, TACACS+ Ayarları, Lisans Bilgileri, and Parametreler. The main content area is titled 'Cihaz Profilreme' and includes tabs for 'Cihaz Profilreme' and 'MAC - Marka Sorulama'. It features a search bar, a table header with columns for PROFIL ADI, AÇIKLAMASI, PROFIL SKORU, DURUM, POLICIES, OLUŞTURMA TARİHİ, and GÜNCELLEME TARİHİ, and a 'Profil Ekle' (Add Profile) button. A message in the center states 'Tabloda veri bulunamadı' (Data not found in the table) with a note: 'Verilen filtrelerle uygun veri bulunamadı. Lütfen veri olduğundan emin olunuz.' (No data found matching the filters. Please make sure the data exists.)

2. Adding a Profile

You can create a new profile by clicking the "Add Profile" button on the Device Profiling screen.



This screenshot is identical to the one above, showing the 'Cihaz Profilreme' screen. The 'Profil Ekle' button in the top right corner of the table header is highlighted with a red box.

In the window that opens;



Profil Ekle

Adı: * IoT_Enerji

Açıklama:

Toplam Eşik Değeri: * 10

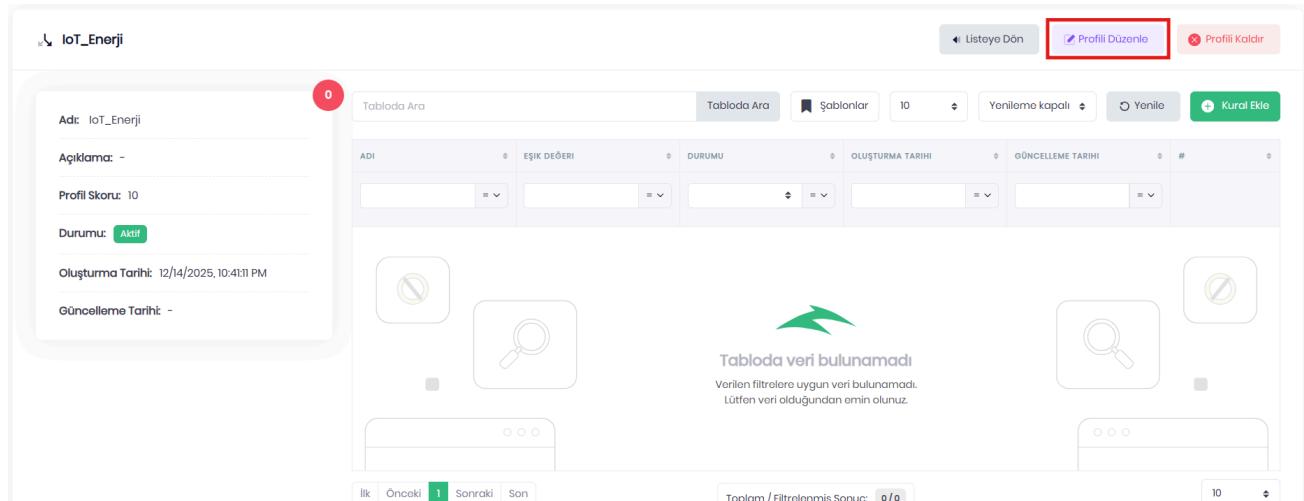
İptal Et Ekle

You must specify the Name, Description (optional), and Total Threshold Score for the profile you wish to create. Once you create the profile, you will be automatically redirected to the details page.

Important: The Total Threshold Score represents the total score of the rules added to the profile. The score you provide here should be the sum of the scores you give to the rules added to the profile. This section is explained in more detail in "1.6) Profile Score System and Examples".

3. Profile Details Page

You can edit your profile by using the "Edit Profile" button located in the upper right corner of the profile details page.



IoT_Enerji

Profil Düzenle Profili Kaldır

Tabloda Ara Tabloda Ara Şablonlar 10 Yenileme Kapalı Yenile Kural Ekle

ADI EŞIK DEĞERİ DURUMU OLUŞTURMA TARIHI GÜNCELLEME TARIHI #

0

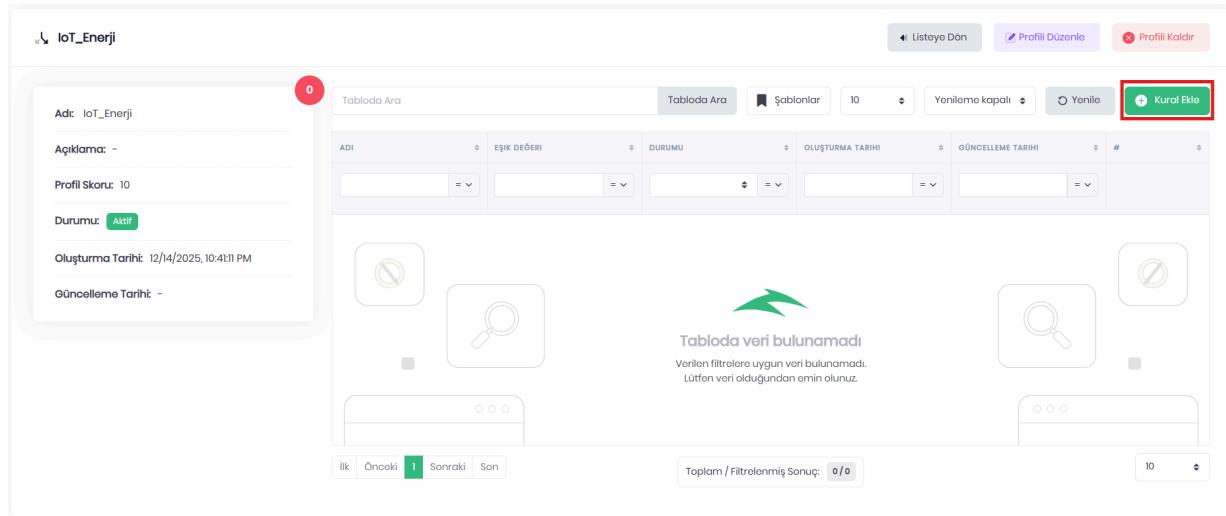
Tabloda veri bulunamadı
Varılan filtrelerle uygun veri bulunamadı.
Lütfen veri olduğundan emin olunuz.

İlk Öncəki 1 Sonraki Son Toplam / Filtrlenmiş Sonuç: 0/0 10

On the editing screen, you can change the Profile Name, Description, or Total Threshold Score.

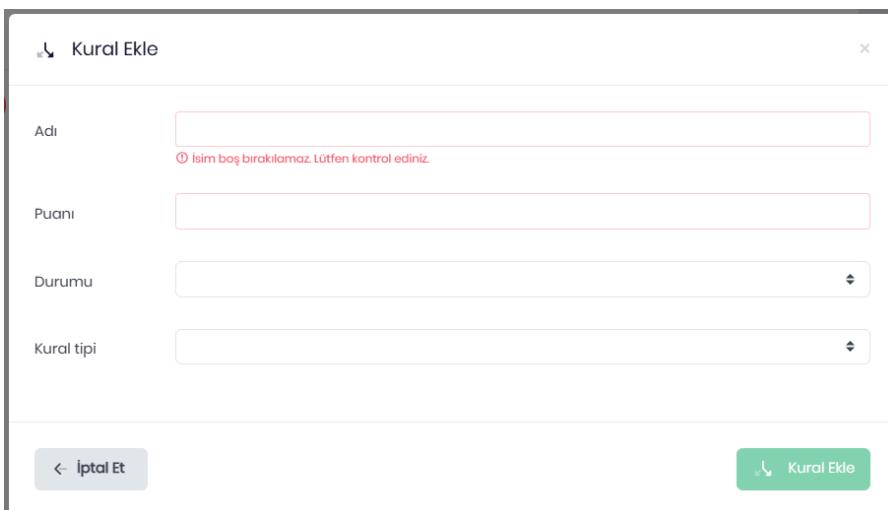
4. Adding a Profile Rule

You can add a new rule by clicking the "Add Rule" button located on the right side of the profile details page;



The screenshot shows the profile details for 'IoT_Enerji'. On the right side, there is a 'Kural Ekle' (Add Rule) button highlighted with a red box. The main content area displays a table with columns: ADI, EŞİK DEĞERİ, DURUMU, OLUŞTURMA TARİHİ, and GÖNCELLEME TARİHİ. Below the table, a message says 'Tabloda veri bulunamadı' (No data found in the table) with a green arrow pointing to it. At the bottom, there are navigation buttons for 'İlk', 'Önceki', 'Sonraki', 'Son', and a search bar with 'Toplam / Filtrlenmiş Sonuç: 0/0'.

When adding a rule;



The dialog box has fields for 'Adı' (Name), 'Puani' (Score), 'Durumu' (Status), and 'Kural tipi' (Rule Type). The 'Adı' field is required, as indicated by a red border and the message 'İsim boş bırakılamaz. Lütfen kontrol ediniz.' (Name cannot be left empty. Please check). At the bottom, there are 'İptal Et' (Cancel) and 'Kural Ekle' (Add Rule) buttons.

Name: A specific name you can give to the rule.

Score: Points for the relevant rule (affects profile score)

Status: Rule active/passive status.

Rule Type: Profiling class

You can create a new rule set by entering the information.

Note: When you select a rule type, extra input fields for that rule type will appear on the relevant screen. These are explained in the Rule Types section.

5. Profile Rule Types

5.1. According to MAC address information

The rule type is "**MAC**". When "**Address**" is selected;

Kural tipi	MAC Adresi
Tipi	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">MAC Adresi Üretici</div>

You can create profile rules based on the MAC address itself or the manufacturer information .

5.1.1. MAC Address

When MAC address is selected as the rule type;

Tipi	MAC Adresi
MAC Adresi	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"><div style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px; margin-right: 10px;">?</div>Kullanım Biçimleri 0:aa:02:bb:03:cc - 01:aa:02:*</div>

You can create a rule using the full MAC address or if it starts with `*:` regex. For example;

- If the MAC address of the device trying to access the network is 01:aa:02:bb:03:cc
- If the MAC address of the device trying to access the network starts with 01:aa:02:*

You can define the rule in this way.

5.1.2. MAC Manufacturer Information

In MAC manufacturer information type;

Kural tipi	MAC Adresi
Tipi	Üretici
Üretici	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"><input type="text"/></div>
Kelime içeriği	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">İçeriyorsa</div>

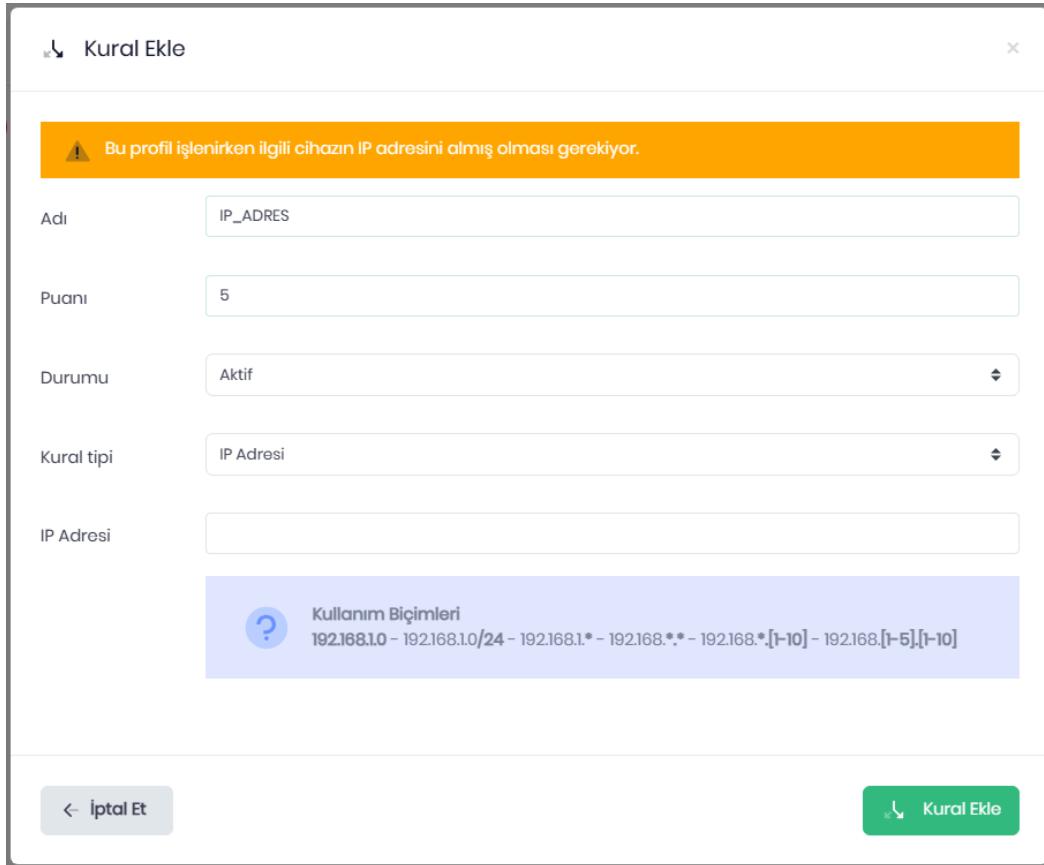
After entering the " **Producer** " information, the " **Word**" you entered will be processed. The content is selected using the sub-rule " **If Equal to** , **Contains** , **Begins with** , **Ends with** ". For example, when " **Samsung** " is selected as the manufacturer information and " **Contains** " is selected as the word content;

- the MAC address of the device trying to access the network contains " **Samsung** "

You can define the rule in this way.

5.2. Based on IP Address

The rule type is " **IP**". When " **address** " is selected;



Kural Ekle

Adı: IP_Adres

Puanı: 5

Durumu: Aktif

Kural tipi: IP Adresi

IP Adresi:

Kullanım Biçimleri
192.168.1.0 – 192.168.1.0/24 – 192.168.1.* – 192.168.*.* – 192.168.*.[1-10] – 192.168.[1-5].[1-10]

← İptal Et Kural Ekle

Rules can be defined for devices connecting to the network based on their full IP address, IP block, the last octet of the IP address, the last two octets of the IP address, or IP address ranges. For example;

- If the IP address of the device trying to access the network is 192.168.1.10,
- If the IP address of the device trying to access the network is within the 192.168.1.0/24 IP block,
- If the IP address of the device trying to access the network starts with 192.168.1 and its 4th octet is any digit (maximum 254) (192.168.1.*),
- If the IP address of the device trying to access the network starts with 192.168 and the last 3rd and 4th octets contain any digit (maximum 254) (192.168.*.*),
- If the device trying to access the network gets an IP address that starts with 192.168 and its 3rd octet starts with any number (Maximum 254) and is between [1-10], then (192.168.*.[1-10])

- If the device trying to access the network has an IP address that starts with 192.168 and its 3rd octet is a number between [1-5] and its 4th octet is an IP address between [1-10] (192.168.[1-5].[1-10])

You can define rules in this way.

Note: For a rule to match the IP address type, the device connected to the network must have received an IP address.

5.3. Depending on location

"Location" is selected as the rule type ;

Kural Ekle

Adı	<input type="text"/>
① İsim boş bırakılamaz. Lütfen kontrol ediniz.	
Puanı	0
Durumu	<input type="text"/>
Kural tipi	Lokasyon
Tipi	<input type="text"/> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Lokasyon Bilgisi Switch/Port Bilgisi </div>

5.3.1. Location Information

In terms of location type;

Kural tipi: Lokasyon

Tipi: Lokasyon Bilgisi

Lokasyon:

You can define rules by selecting the locations created on FastNAC.

5.3.2. Switch/Port Information

In the Switch/Port Information Type;

Kural tipi	Lokasyon
Tipi	Switch/Port Bilgisi
Switch	Switch bilgisi Ip adresi olmalıdır. Örneğin: 192.168.1.10
Port	Port bilgisi interface description olarak girmeniz gerekmektedir. Örneğin: GigabitEthernet1/0/1

You can define rules based on the Switch/Port information written to the inputs.

5.4. Domain Control

Domain Control " is selected as the rule type ;

Kural Ekle

⚠ Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	<input type="text"/>
① İsim boş bırakılamaz. Lütfen kontrol ediniz.	
Puanı	0
Durumu	<input type="text"/>
Kural tipi	Domain Kontrolü
Durumu	Domaindeki Cihazlar

[← İptal Et](#) [Kural Ekle](#)

5.4.1. Domain Device Control

This is the default profile type.

Kural tipi: Domain Kontrolü

Durumu: Domaindeki Cihazlar

Tipi: Domain Cihaz Kontrolü

Domain Kullanıcı Kontrolü

This profile enables domain control of devices according to parameter settings.

5.4.2. Domain User Control

In the Domain User Control type;

Kural tipi: Domain Kontrolü

Durumu: Domaindeki Cihazlar

Tipi: Domain Kullanıcı Kontrolü

Kullanıcı Adı:

Oturum Kontrolü: Açık

Kaç Cihazda Oturum Açıbilir:

You can create custom profiles for users on the domain. You can also control how many devices a user can log in from using the **"Login" option**. You can enable **the "Control"** setting. For example;

- **onur** "is logged in" on the device attempting to access the network , and if session control is enabled and a second session is opened on any device (the number 3 must be entered in the input field to comply with the rule definition.)

You can define the rule in this way.

5.5. Active Directory

Active Directory " is selected as the rule type ;

Kural tipi	Active Directory
Attribute Adı	
Değer	
Kelime İçeriği	<ul style="list-style-type: none">EşitseEşitseİçeriyorsaİle Başlıyorsaİle Bitiyorsa
← İptal Et	

You can define profiles for Active Directory users based on their attributes (custom attributes). The attribute name must match the attribute name in Active Directory. You can define rules based on the corresponding value. For example;

Attribute Name: **department**

Value: **Information Processing**

Word Content: **Equal**

- **onur** " is logged in on the device attempting to access the network , and the department attribute of the user " **onur** " is " **Information**" If **the operation** is equal to the text "Operation"

You can define the rule in this way.

5.6. HTTP/HTTPS

HTTP/HTTPS " is selected as the rule type, if the device has a web interface (80/443), you can scan the interface and define a profile based on the words it contains.

Kural tipi	HTTP/HTTPS
URL	<input type="text"/> Port URL Üzerinden belirtebilirsiniz. Örneğin: https://192.168.1.10:6000
Değer	<input type="text"/>
Kelime İçeriği	<input type="text"/>
Giriş Ekranı	<input checked="" type="checkbox"/>

URL: If the device you wish to profile has a specific URL address, you can enter it here. Otherwise, simply enter "/".

Value: After scanning the web interface, the value you wish to search for is entered here.

Word Content: If it is equal to, contains, begins with, or ends with, a sub-rule should be selected.

Login Screen: On/Off

After logging in to the desired web interface with your Username and Password, if you need to continue with the process, you can open the "Login Screen" section and make the following settings;

Giriş Ekranı	<input checked="" type="checkbox"/>
Giriş URL	<input type="text"/>
Kullanıcı Adı	<input type="text"/>
Şifre	<input type="text"/> 
Basic Auth	<input checked="" type="checkbox"/>
Payload Kullanıcı	<input type="text"/>
Payload Şifresi	<input type="text"/> 

Login URL: The URL where the user will log in (for example: login.php)

Username: The username that will be used to log in to the page.

Password: The password to log in to the page.

Basic Auth: On/Off

Basic Authentication is one of the simplest authentication methods used in the HTTP protocol. If the web interface you wish to scan uses Basic Authentication, enabling this setting will attempt Basic Authentication using the Username and Password provided on the form.

If Basic Authentication is not enabled, the relevant setting is set to Off. The user information for logging in must be entered in the Payload Username and Payload Password sections.

5.7. Telnet/SSH

Telnet/SSH " is selected as the rule type ;

! Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	<input type="text"/>
	<small>① İsim boş bırakılamaz. Lütfen kontrol ediniz.</small>
Puanı	<input type="text"/>
Durumu	Aktif
Kural tipi	Telnet/SSH
Tipi	<input type="button" value="TELNET"/> <input type="button" value="SSH"/>

[← İptal Et](#) [Kural Ekle](#)

5.7.1. Telnet

Tipi	TELNET	▼
Port		
Timeout		
Kullanıcı Adı		
Şifre		◎
Komut	Komutu belirtiniz. Örneğin: show version	
Kelime	Komut çıktısında aranacak kelimeyi belirtiniz. Örneğin: Cisco	
Kelime İçeriği	İçeriyorsa	▼

Port: Telnet port information (Default port is 23.)

Timeout: Connection timeout period (30 seconds if not specified)

Username: The username required for Telnet connection.

Password: The password required for Telnet connection.

Command: The command to be executed after establishing a Telnet connection.

Word: The output sought after the execution of the command.

Word Content: If it's equal to, contains, starts with, or ends with, then a sub-rule should be selected.

The working principle is as follows: you can access the relevant device via telnet using the given information and write a rule based on the output of the specified command that matches the searched word.

5.7.2. SSH

Kural tipi	Telnet/SSH
Tipi	SSH
Port	
Kullanıcı Adı	
Şifre	
Komut	<small>Komutu belirtiniz. Örneğin: show version</small>
Kelime	<small>Komut çıktısında aranacak kelimeyi belirtiniz. Örneğin: Cisco</small>
Kelime İçeriği	İçeriyorsa

Port: Telnet port information (Default port is 22)

Timeout: Connection timeout period (30 seconds if not specified)

Username: The username required for Telnet connection.

Password: The password required for Telnet connection.

Command: The command to be executed after establishing a Telnet connection.

Word: The output sought after the executed command.

Word Content: If it equals, contains, starts with, or ends with, then a sub-rule should be selected.

The working principle is as follows: you can access the relevant device via SSH using the given information and write a rule based on the searched word resulting from the output of the specified command.

5.8. DHCP Fingerprint

“DHCP Fingerprint” is selected as the rule type ;

 Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	<input type="text"/>
① İsim boş bırakılamaz. Lütfen kontrol ediniz.	
Puanı	<input type="text"/>
Durumu	Aktif
Kural tipi	DHCP Fingerprint
Tipi	<input type="button" value="Üretici Bilgisi"/> <input type="button" value="Hostname"/> <input type="button" value="Parametreler"/>
<input type="button" value="← İptal Et"/> <input type="button" value="Kural Ekle"/>	

5.8.1. Manufacturer Information

Kural tipi	DHCP Fingerprint
Tipi	Üretici Bilgisi
Üretici Bilgisi	<input type="text"/>

You can define rules based on the manufacturer information in the DHCP Fingerprint output.

5.8.2. Device Name (Hostname)

Kural tipi	DHCP Fingerprint
Tipi	Hostname
Hostname	<input type="text"/>

You can define rules based on the device name (hostname) in the DHCP Fingerprint output.

5.8.3. Parameters

Kural tipi	DHCP Fingerprint										
Tipi	Parametreler										
Parametreler	<button>Önekler</button>										
<table><thead><tr><th>İŞLETİM SİSTEMİ</th><th>PARAMETRELER</th></tr></thead><tbody><tr><td>Windows</td><td>1,3,6,15,31,33,43,44,46,47,119,121,249,252</td></tr><tr><td>Pardus</td><td>1,2,6,12,15,26,28,121,3,33,40,41,42,119,249,252,17</td></tr><tr><td>Android 11</td><td>1,3,6,15,26,28,51,58,59,43,114,108</td></tr><tr><td>Apple iOS</td><td>1,121,3,6,15,108,114,119,252</td></tr></tbody></table>		İŞLETİM SİSTEMİ	PARAMETRELER	Windows	1,3,6,15,31,33,43,44,46,47,119,121,249,252	Pardus	1,2,6,12,15,26,28,121,3,33,40,41,42,119,249,252,17	Android 11	1,3,6,15,26,28,51,58,59,43,114,108	Apple iOS	1,121,3,6,15,108,114,119,252
İŞLETİM SİSTEMİ	PARAMETRELER										
Windows	1,3,6,15,31,33,43,44,46,47,119,121,249,252										
Pardus	1,2,6,12,15,26,28,121,3,33,40,41,42,119,249,252,17										
Android 11	1,3,6,15,26,28,51,58,59,43,114,108										
Apple iOS	1,121,3,6,15,108,114,119,252										

You can define rules based on the parameters in the DHCP Fingerprint output.

5.9. TCP/UDP Port

TCP/UDP Port " is selected as the rule type ;

Kural tipi	TCP/UDP
TCP Portları	
UDP Portları	
Port Durumu	

 **Kullanım Bİçimleri**
80 - 80,8080 - 90,50,8081-9000

You can define a profile based on the status of the TCP/UDP ports of the relevant device as specified above. Port Statuses:

- Open
- Closed
- Open Filtered

When defining ports, you can use a single port number (e.g., 80), multiple ports separated by commas (e.g., 80,8080), and a range of ports (e.g., 80-8080) to define the rule.

5.10. SNMP

SNMP " is selected as the rule type ;

Kural tipi	SNMP
SNMP Tipi	
Port	
SNMP OID	
Değer	
Kelime İçeriği	İçeriyorsa

You can define a profile based on the content of the value received in the output of the specified SNMP OID. It offers support for SNMPv1, SNMPv2c, and SNMPv3. Accepted options for SNMPv3 are:

The supported formats are noAuthNoPriv, authNoPriv, and authPriv.

As for authentication types, it supports No Auth Protocol, MD5, SHA128, SHA256, SHA384, and SHA512.

Priv type support includes: No Priv Protocol, DES, AES 128, AES 192, and AES 256.

For example, based on the entered SNMP information, you can define a rule that responds to a request sent to the OID 1.3.6.1.2.1.1.1 (SNMP sysdesrc OID) if the request contains the word "Cisco".

Note: You can find SNMP OIDs by searching online.

5.11. Posture

Posture " is selected as the rule type ;

Kural tipi	Posture
Tipi	<ul style="list-style-type: none">WindowsLinuxDosya TakibiOturum Takibi

You can define rules using features such as Windows, Linux, File Tracking, and Session Tracking.

5.11.1. Windows

Windows " is selected as the rule type ;

The screenshot shows a configuration interface with the following fields:

- Kural tipi: Posture
- Tipi: Windows
- Posture Tipi: A dropdown menu is open, showing three options: İşletim Sistemi Kontrolü, Program Kontrolü, and Servis Kontrolü. The first option, İşletim Sistemi Kontrolü, is highlighted with a blue border.
- Buttons at the bottom: 'İptal Et' (Cancel) and 'Kural Ekle' (Add Rule) in a green button.

5.11.1.1. Operating System Control

Posture type as " **Operating** " When "System Control" is selected;

The screenshot shows a configuration interface with the following fields:

- Kural tipi: Posture
- Tipi: Windows
- Posture Tipi: İşletim Sistemi Kontrolü
- OS Versiyonu: An empty input field.
- Tipi: A dropdown menu is open, showing three options: Küçük, Eşit, and Büyük. The first option, Küçük, is highlighted with a blue border.
- Buttons at the bottom: 'İptal Et' (Cancel) and 'Kural Ekle' (Add Rule) in a green button.

Operating system version " **OS** " You can define a rule that is " **Less than** , **Equal to** , or **Greater than** " the version you enter in the "Version" input field.

5.11.1.2. Program Control

As a posture type, " **Program** " When "Control" is selected;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Program Adı Program Versiyonu </div>

5.11.1.2.1. Program Name

Sub-rule type " **Program** " When the **name** "" is selected;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Adı
Durumu	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Yüklü Yüklü Değil </div>

" **Program** " The program you typed in the "**Name** " input field will be marked as "**Installed**" or "**Not Installed**" on the controlled device. You can define a rule as "**No**".

5.11.1.2.2. Program Version

Sub-rule type " **Program** " When the "**Version**" is selected;

Kural tipi	Posture	▼
Tipi	Windows	▼
Posture Tipi	Program Kontrolü	▼
Program Adı		
Tipi	Program Versiyonu	▼
Versiyon		
Tipi	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Küçük Eşit Büyük </div>	▼
← İptal Et Kural Ekle		

"Program" You can define rules such as "**Less than** , **Equal to** , **Greater than**" for the program version entered in the "**Version**" input, where the name of the program is entered in the "**Name**" input.

5.11.1.3. Service Check

Posture type as "**Serving**" When "**Control**" is selected;

Kural tipi	Posture	▼
Tipi	Windows	▼
Posture Tipi	Servis Kontrolü	▼
Servis Adı		
Durumu	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Çalışıyor Çalışmıyor </div>	▼

You can define rules based on whether the service you enter in the "Service Name" input field is "Running" or "Not Running".

5.11.2. Linux

Linux " is selected as the rule type ;



Kural tipi: Posture

Tipi: Linux

Posture Tipi:

- İşletim Sistemi Kontrolü
- Program Kontrolü
- Servis Kontrolü

İptal Et **Kural Ekle**

5.11.2.1. Operating System Control

Posture type as " **Operating** " When "System Control" is selected;



Kural tipi: Posture

Tipi: Linux

Posture Tipi: İşletim Sistemi Kontrolü

OS Versiyonu:

Tipi:

- Küçük
- Eşit
- Büyük

İptal Et **Kural Ekle**

Operating system version " **OS** " You can define a rule that is " **Less than** , **Equal to** , or **Greater than**" the version you enter in the "Version" input field.

5.11.2.2. Program Control

As a posture type, " **Program** " When "Control" is selected;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	<div style="border: 1px solid #ccc; padding: 5px;"> Program Adı Program Versiyonu </div>

5.11.2.2.1. Program Name

Sub-rule type " **Program** " When **the name** "" is selected;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	<div style="border: 1px solid #ccc; padding: 5px;"> Program Adı </div>
Durumu	<div style="border: 1px solid #ccc; padding: 5px;"> Yükü Yükü Doğıl </div>

" **Program** " The program you typed in the " **Name** " input field will be marked as " **Installed** " or " **Not Installed** " on the controlled device. You can define a rule as " **No** ".

5.11.2.2.2. Program Version

Sub-rule type " **Program** " When **the "Version"** is selected;

Kural tipi	Posture	◆
Tipi	Linux	◆
Posture Tipi	Program Kontrolü	◆
Program Adı		
Tipi	Program Versiyonu	◆
Versiyon		
Tipi	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Küçük Eşit Büyük </div>	◆
<input style="width: 150px; height: 30px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;" type="button" value="← İptal Et"/> <input style="width: 150px; height: 30px; background-color: #28a745; color: white; border: 1px solid #28a745; border-radius: 5px; padding: 5px;" type="button" value="Kural Ekle"/>		

"Program" You can define rules such as " **Less than** , **Equal to** , **Greater than** " for the program version entered in the " **Version** " input, where the name of the program is entered in the " **Name** " input.

5.11.2.3. Service Check

Posture type as " **Serving**" When " **Control** " is selected;

Kural tipi	Posture	◆
Tipi	Linux	◆
Posture Tipi	Servis Kontrolü	◆
Servis Adı		
Durumu	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Running Dead Exited Failed </div>	◆
<input style="width: 150px; height: 30px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;" type="button" value="← İptal Et"/> <input style="width: 150px; height: 30px; background-color: #28a745; color: white; border: 1px solid #28a745; border-radius: 5px; padding: 5px;" type="button" value="Kural Ekle"/>		

"Service" The service you enter in the input field labeled " **Name** " will have the following status: " **Running** " , " **Dead** " , " **Exit** " . You can define rules based on " **Exited** " and " **Failed** " status .

5.11.3. File Tracking

The rule type is "**File**". When "**Tracking**" is selected;

Kural tipi	Posture
Tipi	Dosya Takibi
Dosya Yolu	<input type="text"/> Dosya yolunun tam halini girmelisiniz. Örneğin: C:\Program Files\Notepad++\notepad++.exe

" **File** You can define a rule to check the device for the existence of the file specified in the " **Path** " **input**.

5.11.4. Session Tracking

Rule type: "**Session**" When "**Tracking**" is selected;

Kural tipi	Posture
Tipi	Oturum Takibi
Süre	<input type="text"/> X gündür giriş yapmamış

You can define a rule on the device to prevent login based on the number of days specified in the " **Duration** " **input**.

5.12. NMAP

NMAP " is selected as the rule type ;

Kural tipi	NMAP
Parametre	<input type="text"/>
Kelime	<input type="text"/>

Parametreler

starts a scan using the NMAP parameters entered in the "**Parameters**" section and searches for the output entered in the "**Word**" input. For example, I entered "**-Pn -O**" in the Parameters input and "**Windows**" in the Word input;

- Start an NMAP scan on the device with the specified parameters, and if the output shows "**Windows**"...

You can define the rule in this way.

6. Profile and Score System and Examples

When a new profile is created, you are asked for a Total Threshold Value (Profile Score);

Profil Ekle X

Adı: *	<input type="text"/>
① İsim boş bırakılamaz. Lütfen kontrol ediniz.	
Açıklama:	<input type="text"/>
Toplam Eşik Degeri: *	<input type="text"/>
② Eşik değeri 1'den küçük olamaz.	

Iptal Et

▶ Ekle

This Profile Score should be set to equal or greater than the total points of the profile rules added to the profile details. The details of the example rules given below are explained in detail under the heading "**1.5 Profile Rule Types**".

6.1. Example IP_Camera Profile

To understand the Profile Score system in more detail, let's create a profile.

"**IP_Camera**" and setting its Total Threshold score to **10**;

Profil Ekle

Adı: *	IP_Kamera
Açıklama:	IP Kamera Profili
Toplam Eşik Değeri: *	10

[İptal Et](#) [▶ Ekle](#)

Now we need to add rule sets to the profile we've created in order to reach the Total Threshold Value score.

As a first rule, let's create a MAC address rule set using regex;

↳ Kural Ekle

Adı	MAC_Adres
Puanı	5
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	MAC Adresi
MAC Adresi	01:aa:02:*

Kullanım Bİçimleri
01:aa:02:bb:03:cc - 01:aa:02:*

[◀ İptal Et](#) [↳ Kural Ekle](#)

According to the example above, if the device's MAC address starts with "**01:aa:02:***", it will be interpreted as receiving 5 points from this rule set.

Next, let's create another set of rules and this time choose the Producer;

Kural Ekle

Adı	MAC_VENDOR
Puanı	5
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	Üretici
Üretici	samsung
Kelime İçeriği	İçeriyorsa

According to the example above, if the device's MAC manufacturer information contains "**Samsung**," it will be interpreted as receiving an additional 5 points from this rule set.

"**IP_Camera**" profile to **10**. If a device matches the two rule sets we wrote above, we can now say that the device complies with the "**IP_Camera**" profile. To explain further;

The device trying to access the network;

- 5 points if the MAC address starts with "**01:aa:02:*** ",
- MACs will receive 5 extra points if their manufacturer information includes "**Samsung** ".

So, in total, it will have **10** points from the rule sets and will be a device that matches the "**IP_Camera**" profile.

6.2. Sample Printer Profile

Let's create another example, this time a printer profile.

"**Printer**" and setting the Total Threshold score to **50 this time** ;

Profil Ekle

Adı: *	Yazıcı
Açıklama:	Yazıcı tipindeki cihazlar
Toplam Eşik Değeri: *	50

[İptal Et](#) [Ekle](#)

As a first rule, let's create a MAC address rule set using regex;

Kural Ekle

Adı	canon_mac_regex
Puanı	15
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	MAC Adresi
MAC Adresi	88:87:17:*

 **Kullanım Biçimleri**
01:aa:02:bb:03:cc - 01:aa:02:*

[İptal Et](#) [Kural Ekle](#)

If the device's MAC address starts with " **88:87:17:*** ", we can interpret this as it receiving **15** points from the rule set.

the Profile Score as **50**. If our rule applies, the device will receive **15** points, and to classify the device as a "**Printer**" profile device, we need an additional set of rules worth **50-15=35** points.

As a second rule, let's add the MAC manufacturer information;

Kural Ekle

X

Adı	canon_mac_vendor
Puanı	15
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	Üretici
Üretici	canon
Kelime İçeriği	İçeriyorsa

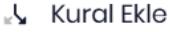
 İptal Et

 Kural Ekle

If the device's MAC manufacturer includes "**canon**," we can interpret this as it receiving 15 points from the rule set.

To reiterate, we specified the Profile Score as **50**. If our first rule works, the device will receive **15** points. If our second rule works, it will receive another **15** points, bringing the total to **30 points**. We need **50 points**, and therefore, we require an additional **20 points** from the rule sets ($50 - 30 = 20$ points).

Let's continue and add TCP/UDP port information as the third rule;

 Kural Ekle X

⚠ Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	tcp_9100
Puanı	20
Durumu	Aktif
Kural tipi	TCP/UDP
TCP Portları	9100
UDP Portları	
Port Durumu	Open

 **Kullanım Bİçimleri**
80 - 80,8080 - 90,50,8081-9000

[← İptal Et](#) [Kural Ekle](#)

We can interpret this as the device receiving **20 points from** the "**TCP 9100 port is open**" rule set .

In conclusion, the device attempting to access the network;

- 15 points if the MAC address starts with "**88:87:17:*** ",
- the MAC manufacturer information includes "**Canon**," it will receive 15 points.
- "**TCP port 9100 is open**," you will receive 20 points.

a total of **50** points and will be identified as a device that meets the Printer profile.

6.3. Sample IoT Device Profile

Let's create another example, this time making the profile more comprehensive and rigorous.

"IoT" and setting the Total Threshold score to **50 this time**;

Profil Ekle

Adı: *	IoT
Açıklama:	
Toplam Eşik Değeri: *	50

İptal Et → Ekle

As a first rule, let's create another MAC address rule set using regex and assign it 5 points;

Kural Ekle

Adı	mac_regex
Puanı	5
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	MAC Adresi
MAC Adresi	01:aa:02:*

? Kullanım Biçimleri
01:aa:02:bb:03:cc - 01:aa:02:*

← İptal Et → Kural Ekle

will receive 5 points if its MAC address starts with "**01:aa:02:***".

Let's continue and add a second rule: this time, **the TCP port 1010** must be open, and we'll give that 10 points.

Kural Ekle

⚠ Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	tcp_1010
Puanı	10
Durumu	Aktif
Kural tipi	TCP/UDP
TCP Portları	1010
UDP Portları	
Port Durumu	Open

Kullanım Biçimleri
80 - 80,8080 - 90,50,8081-9000

← İptal Et Kural Ekle

If the device has TCP port **1010 open**, it will receive **10** points, bringing its total to **15** points.

As a third rule, let's create an SNMP rule and give it **10** points;

 Kural Ekle X

⚠ Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	snmp
Puanı	10
Durumu	Aktif
Kural tipi	SNMP
SNMP Tipi	SNMP v2c
Community	*****
Port	161
SNMP OID	1.3.6.1.2.1.1.1
Değer	IoT
Kelime İçeriği	İçeriyorsa

to the device using **the SNMPv2c** community with the code **1.3.6.1.2.1.1.1** (SNMP sysdescr OID), and if the response includes "**IoT**", **it will receive 10** points. This will bring the total to **25** points.

Remember, we gave **50** points when adding the profile. We're currently at **25** points. Let's continue and add the fourth rule as HTTP/HTTPS and give it **15** points;

Kural Ekle

⚠ Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

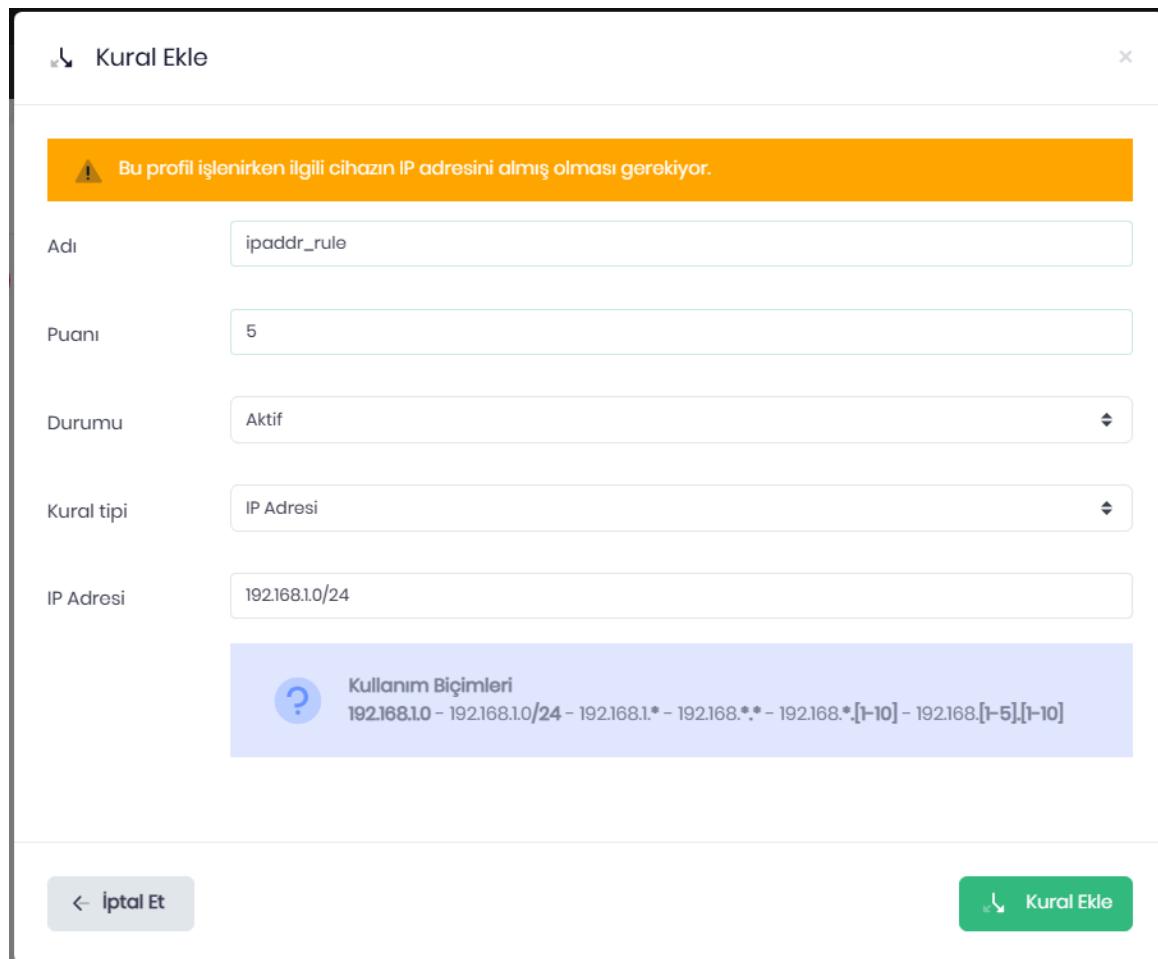
Adı	http_profil
Puanı	15
Durumu	Aktif
Kural tipi	HTTP/HTTPS
URL	/
Değer	Energy
Kelime İçeriği	İçeriyorsa
Giriş Ekranı	<input checked="" type="checkbox"/>

← İptal Et **Kural Ekle**

The device's web interface will be scanned, and if the word "**Energy**" **appears in its content, it will receive another 15** points for that rule . We've reached a total of **45** points.

To classify the device as having an IoT profile, we needed a 5-point rule set.

Let's add our fifth rule. Let's define its type as IP address and make it a rule that the device must be within an IP block;



Kural Ekle

Adı: ipaddr_rule

Puanı: 5

Durumu: Aktif

Kural tipi: IP Adresi

IP Adresi: 192.168.1.0/24

Kullanım Bİçimleri
192.168.1.0 - 192.168.1.0/24 - 192.168.1.* - 192.168.*.* - 192.168.*[1-10] - 192.168.[1-5].[1-10]

← İptal Et Kural Ekle

the device's IP address is within the **192.168.1.0/24 network block**, it will receive an additional **5** points from this rule . The total will be **50** .

Now all our rules are ready. We've created a strict set of rules for us to be able to categorize a device as having an "**IoT**" profile. In summary;

- the device's MAC address starts with "**01:aa:02:***" , you will receive **5** points.
- the device's "**TCP 1010 port**" is open, you will receive **10** points.
- When we send a request to the device's **SNMPv2c** community with the SNMP OID "**1.3.6.1.2.1.1.1 (sysDescr)**", if the response contains "**IoT**", we get **10** points.
- The device's web interface will be scanned, and if the word "**Energy**" appears in its content, **15** points will be awarded.
- **5** points if its IP address is within the "**192.168.1.0/24**" network block.

a total of **50** points, and we will then define this device as one that meets the "**IoT**" profile.

We've learned all the details about device profiling. Once devices are profiled, actions are taken through Policies. You can review the **policies.docx** document for this.