



FastNAC



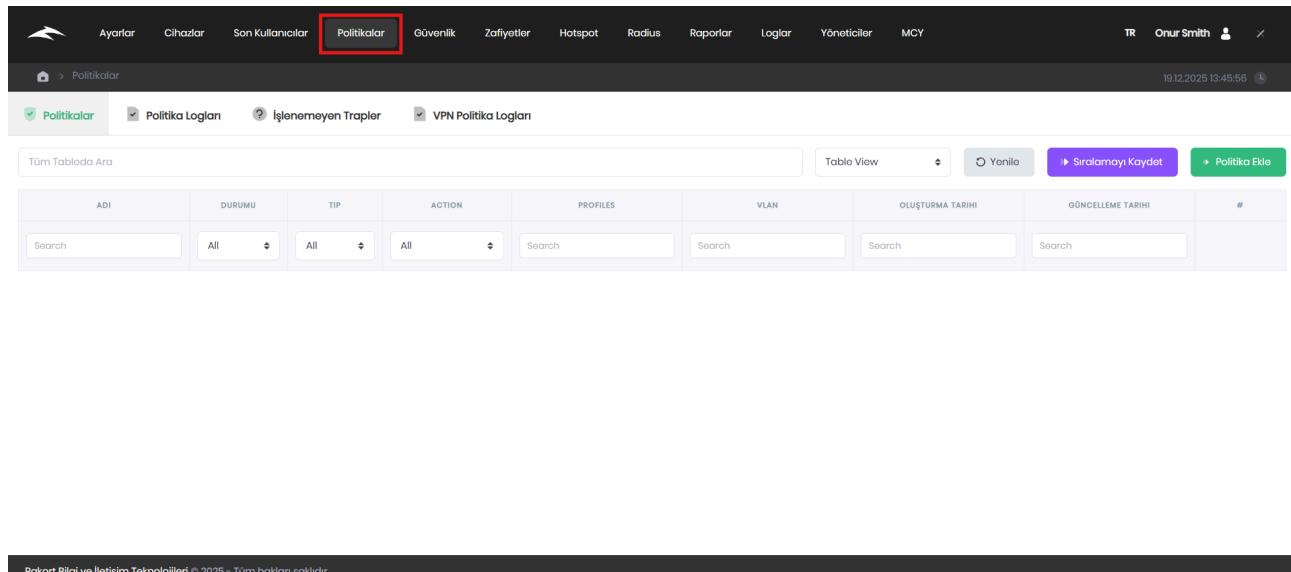
POLICIES

Contents;

1.1) Getting Started	3
1.2) Adding Policies	3
1.3) Policy Details Page	4
1.3.1) Adding a Profile	4
1.3.2) Basic Information	5
1.3.3) Types of Actions	5
1.3.3.1) VLAN Modification	6
1.3.3.1.1) VLAN Assignment	6
1.3.3.1.2) Interface VLAN Assignment	6
1.3.3.1.3) Dynamic VLAN Assignment	7
1.3.3.1.3.1) Assignment by Domain Groups	8
1.3.3.1.3.2) Assignment according to Domain OUs	9
1.3.3.1.3.3) Using Dynamic VLANs and Profiles	10
1.3.3.2) Disable Port	11
1.3.3.3) IP Phone Type	11
1.3.3.4) Quarantine VLAN	12
1.3.3.4.1) Port Closing	12
1.3.3.4.2) VLAN Change	12
1.3.3.4.3) Quarantine and Profile Usage	13
1.3.3.4.4) General Use Regarding Quarantine	13
1.3.3.5) Location VLAN	14
1.3.3.5.1) General Usage Regarding Location VLANs	15
1.3.3.6) No Action	18
1.3.4) Radius	18
1.3.5) VPN	18
1.3.5.1) Auth Type	19
1.3.5.2) Deauth Type	19
1.3.6) Situation	19
1.3.7) Notifications	20
1.3.8) Icon (Port Visualization)	20

1.1) Getting Started

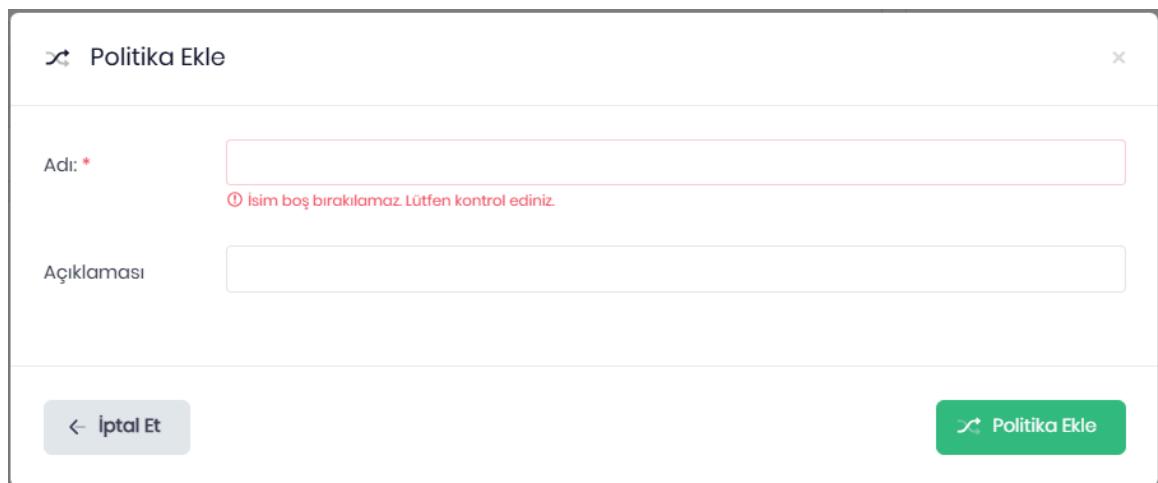
Actions to be taken regarding devices connected to the network are decided through the " **Policies** " section in the main menu.



On FastNAC, policies are checked starting from the top, just like a firewall rule, and when a device hits a policy, other policies under that policy are not checked. You can change the policy order by dragging and dropping within the table on the " **Policies** " page.

1.2) Adding Policies

Add Policy " button located in the " **Policies** " list . In the window that opens;



Name: A name to be given to politics

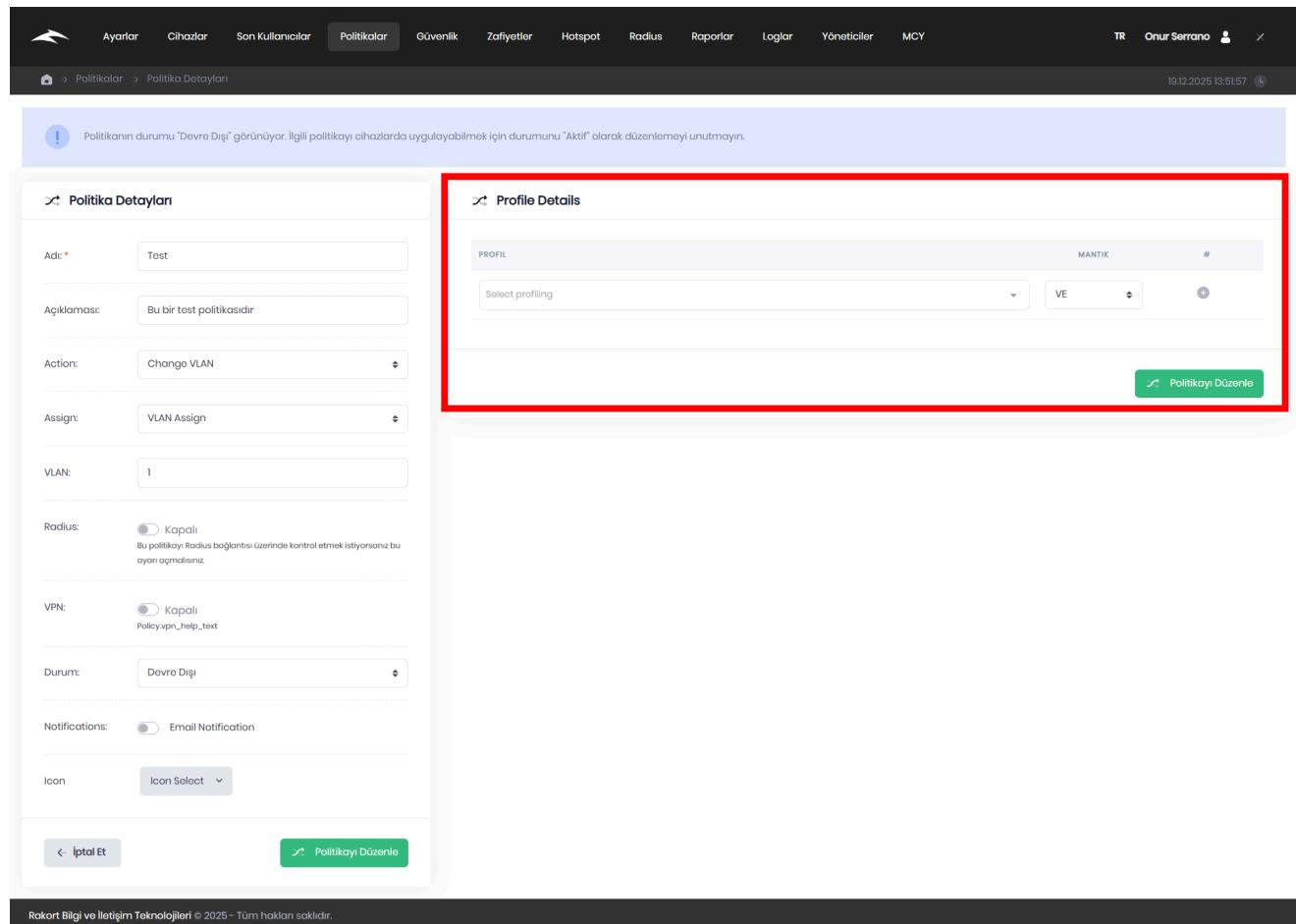
Explanation: A statement to be given regarding policy (Optional)

You can create a new policy by filling in the fields. Once the policy is created, you will be redirected directly to the policy details page.

1.3) Policy Details Page

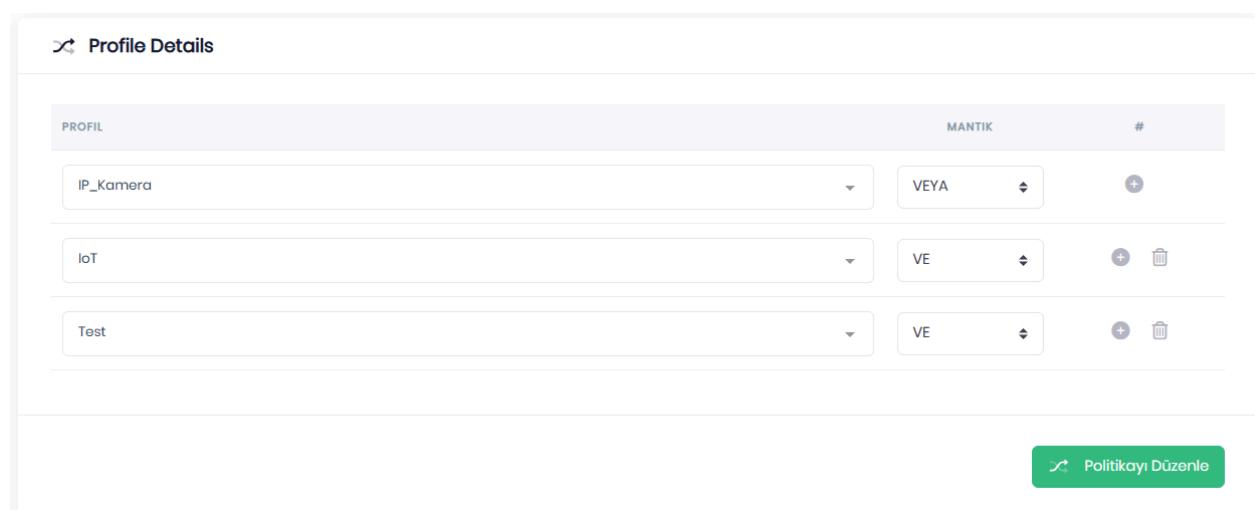
1.3.1) Adding a Profile

On the right side of the policy details page, you can find the "**Profile**" section. The profiles created can be linked to the relevant policy from the "**Details**" section.



The screenshot shows the 'Politika Detayları' (Policy Details) page. On the left, there are several configuration fields: 'Adı:' (Name: Test), 'Açıklaması:' (Description: Bu bir test politikasıdır), 'Action:' (Action: Change VLAN), 'Assign:' (Assign: VLAN Assign), 'VLAN:' (VLAN: 1), 'Radius:' (Radius: Kapalı), 'VPN:' (VPN: Kapalı), 'Durum:' (Status: Devre Dışı), 'Notifications:' (Notifications: Email Notification), and 'Icon' (Icon: Icon Select). On the right, the 'Profile Details' section is highlighted with a red box. It contains a table with two rows. The first row has 'PROFİL' (Profile) set to 'Select profiling' and 'MANTIK' (Logic) set to 'VE'. The second row has 'PROFİL' set to 'Select profiling' and 'MANTIK' set to 'VE'. A green button at the bottom right of this section says 'Politikayı Düzenle' (Edit Policy).

Here, you can link the created profiles using "AND - OR" logic, and use as many profiles as you want in a single policy. By clicking on the icon in the profiles table  you can add a second profile to the policy and define the logical connection (AND - OR) between the two profiles.



The screenshot shows the 'Profile Details' section with three profiles listed: 'IP_Kamera', 'IoT', and 'Test'. Each profile is linked with the logic 'VEYA' (OR). The 'IP_Kamera' profile is linked with 'VE'. The 'IoT' and 'Test' profiles are also linked with 'VE'. A green button at the bottom right says 'Politikayı Düzenle' (Edit Policy).

, we stated that the device must match the “ **IP_Camera** ” or “ **IoT** ” and “ **Test** ” **profiles. Logically, this can be interpreted as: [IP_Camera or IoT (if it matches one of them)] and [Test] profiles.**

Note: The profile area changes in some action types. The changing parts will be shown when describing the action types.

1.3.2) Basic Information

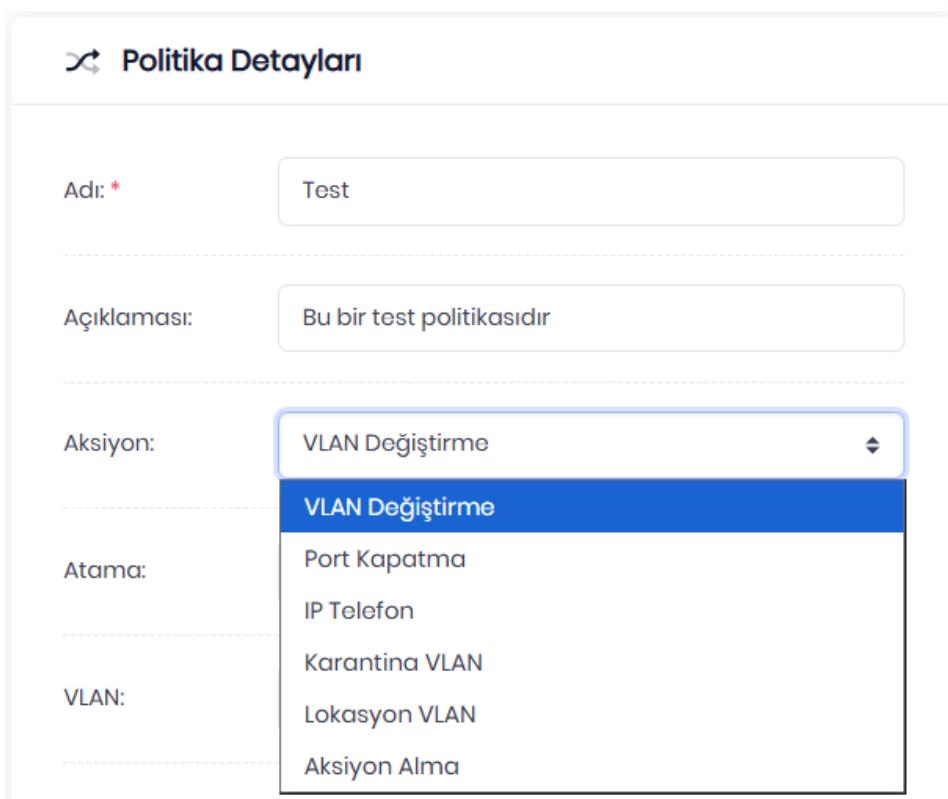
You can edit the policy name and description in the upper left corner of the policy details page;



The screenshot shows the 'Politika Detayları' (Policy Details) page. It has two main input fields: 'Adı:' with the value 'Test' and 'Açıklaması:' with the value 'Bu bir test politikasıdır'.

1.3.3) Types of Actions

From the Actions section on the left side of the policy details page, you can select which action to take for devices connected to the selected profiles;



The screenshot shows the 'Politika Detayları' (Policy Details) page with an expanded 'Actions' section. The 'Aksiyon:' field is set to 'VLAN Değiştirme'. A dropdown menu is open, showing the following options: 'VLAN Değiştirme' (which is highlighted in blue), 'Port Kapatma', 'IP Telefon', 'Karantina VLAN', 'Lokasyon VLAN', and 'Aksiyon Alma'.

1.3.3.1) VLAN Modification

, you must select the " **Change VLAN** " **action type** in this section .

Aksiyon: **VLAN Değiştirme**

Atama: **VLAN Ataması**

VLAN: **VLAN Ataması**

Interface VLAN Ataması

Dinamik VLAN Ataması

There are 3 different assignment types in the VLAN modification action. These are;

1.3.3.1.1) VLAN Assignment

When "VLAN Assignment" is selected as the assignment method;

Aksiyon: **VLAN Değiştirme**

Atama: **VLAN Ataması**

VLAN: **10**

In the "VLAN" input section located directly below the assignment section, you can enter the VLAN number to which the device connected to the relevant profiles will be assigned.

Profile We will use the profiles we created under the " **Adding** " heading as examples. If the device connected to the network;

[**IP_Camera** or **IoT** (if it fits either)] and [**Test**], we can interpret the action type above as assigning the device to **VLAN 10** .

1.3.3.1.2) Interface VLAN Assignment

When "Interface VLAN Assignment" is selected as the assignment method;

Aksiyon:

VLAN Değiştirme

Atama:

Interface VLAN Ataması

The "VLAN" input under the assignment section is disabled. This means that;

When the switch is added to FastNAC, the existing VLAN numbers of the ports are recorded in the database (Interface VLAN). If "Interface VLAN Assignment" is selected as the assignment, the switch will remain assigned to the current VLAN number of the port (i.e., whatever the Interface VLAN is).

Let's explain with an example;

First, let's assume the VLAN number of port 5 of the switch with IP address 192.168.1.10 is 20. When we add this switch to FastNAC, we register the Interface VLAN of port 5 as 20 in the database. Then, in the "**Profile**" section ... We will use the profiles we created under the "**Adding**" heading as examples. If the device connected to the network;

[**IP_Camera** or **IoT** (if it matches either)] and [**Test**], the action type "Interface VLAN Assignment" can be interpreted as leaving the device in VLAN 20.

Note: Interface VLAN definitions can be changed from the switch details page. You can find the details in the switch_details.docx documentation.

1.3.3.1.3) Dynamic VLAN Assignment

Dynamic VLAN assignment is used to assign VLANs based on Organizational Units (OUs) within a domain or groups of domain users (members).

Aksiyon:

VLAN Değiştirme

Atama:

Dinamik VLAN Ataması

VLAN:

10

When this assignment type is selected, the "**Profile**" icon on the right side can be found. The "**Details**" section is changing. The assigned OU or domain group is selected from this section.

Profil Detayları

Tip:	<input type="text"/>
Profil Kullan	<input type="text"/> Domain Grupları Domain OU'ları

1.3.3.1.3.1) Assignment by Domain Groups

When "Domain Groups" is selected as the type,

Profil Detayları

Tip:	<input type="text"/> Domain Grupları								
Grup Seç	<input type="text"/> Lütfen bir grup seçiniz								
Profil Kullan	<input type="text"/> Domain Admins Guests Domain Users Selected <table><tr><td>Users</td><td>Press enter to select</td></tr><tr><td>Test1</td><td></td></tr><tr><td>Test2</td><td></td></tr><tr><td>Test3</td><td></td></tr></table>	Users	Press enter to select	Test1		Test2		Test3	
Users	Press enter to select								
Test1									
Test2									
Test3									

When the "Select Group" input is opened, a list of user groups available on the domain is displayed. The user must select the desired group from the relevant screen.

For illustrative purposes, we'll select the "**Test1**" user group;

Profil Detayları

Tip:	<input type="text"/> Domain Grupları
Grup Seç	<input type="text"/> Test1
Profil Kullan	<input type="checkbox"/> Kapalı

In the assignment section on the left side of the screen, the VLAN input located under the "Dynamic VLAN Assignment" option represents the VLAN to which the users in the Test1 group will be assigned.

Aksiyon:	VLAN Değiştirme
Atama:	Dinamik VLAN Ataması
VLAN:	10

In summary, users within the Test1 domain user group will be moved to VLAN 10 when they try to connect through any switch on the network.

1.3.3.1.3.2) Assignment according to Domain OUs

When "Domain OUs" is selected as the type,

Profil Detayları

Tip:	Domain OU'ları
OU Seç:	Lütfen OU seçiniz. (Birden Fazla OU seçimi yapılabılır.)
Profil Kullan	DC=rakort,DC=dev OU=Rakort,DC=rakort,DC=dev Press enter to select OU=Others,OU=Rakort,DC=rakort,DC=dev OU=Network,OU=Rakort,DC=rakort,DC=dev OU=Domain Controllers,DC=rakort,DC=dev OU=Software,OU=Rakort,DC=rakort,DC=dev

When you open the "Select OU" input, a list of OUs available on the domain is displayed. The OU to which you want to assign a OU must be selected from the relevant screen. Multiple OUs can be selected here.

For example, we select the OUs "**OU=Network,OU=Rakort,DC=rakort,DC=dev**" and "**OU=Software,OU=Rakort,DC=rakort,DC=dev**";

Profil Detayları

Tip:	Domain OU'ları
OU Seç:	OU=Network,OU=Rakort,DC=rakort,DC=dev x OU=Software,OU=Rakort,DC=rakort,DC=dev x
Profil Kullan	<input checked="" type="checkbox"/> Kapalı

In the assignment section on the left side of the screen, the VLAN input located under the "Dynamic VLAN Assignment" option represents the VLAN to which the selected OUs will be assigned.

Aksiyon:	VLAN Değiştirme
Atama:	Dinamik VLAN Ataması
VLAN:	10

In summary, if a domain user is within the OU "**OU=Network,OU=Rakort,DC=rakort,DC=dev**" or "**OU=Software,OU=Rakort,DC=rakort,DC=dev**", it can be interpreted that when they try to connect through any switch on the network, they will be moved to VLAN 10.

1.3.3.1.3.3) Using Dynamic VLANs and Profiles

If you want to control any profile in addition to dynamic VLAN assignment, you need to enable the "**Use Profile**" option. When you enable this setting, an area where you can select profiles will open directly below the relevant screen.

PROFIL	MANTIK	#
Profil Seç	VE	+

A scenario like the following could be used here;

First, let's add a profile to ensure the antivirus service is running. (Detailed information about profiling can be found in the device_profiling.docx documentation.) Then, let's check both the user group using Dynamic VLAN assignment and the antivirus profile simultaneously.

Let's write a policy that states the user requesting network access must be in the "Test" domain user group and the Antivirus service must be running.

Politika Detayları

Adı *	Test
Açıklaması:	Bu bir test politikasıdır
Aksiyon:	Change VLAN
Atama:	Dynamic VLAN Assign
VLAN:	10
Radius:	<input checked="" type="radio"/> Kapalı Bu politikayı Radius bağlantı üzerinde kontrol etmek istiyorsanız bu oyuna oynamalısınız.

Profil Detayları

Type:	Domain Grupları
Grup Seç:	Test1
Profil Kullan:	<input checked="" type="checkbox"/> Açık

Profil Detayları

PROFİL	MANTIK
Antivirüs_Servis	VE

In the example above, if a domain user is within the "Test1" domain group and has an antivirus service running on their computer, it can be interpreted that when they try to connect through any switch on the network, they will be moved to VLAN 10.

This way you can perform both dynamic VLAN assignment and comprehensive profile checks simultaneously.

1.3.3.2) Disable Port

When the action type is selected as "Port Closure",

Aksiyon:

Port Kapatma

Port Geri Açma Açık

Süre:*

Kapatılan portun geri açılma süresi. (Dakika cinsinden)

This action closes (shutdown or disabled) the port to which the connected device is attached, according to the selected profiles. By enabling the "**Port Reopen**" time and specifying the duration (in minutes), you can ensure that the closed port is automatically reopened. When the port is reopened, if the device is still connected, the policy is checked again, and if the conditions are still met, the port is closed again.

1.3.3.3) IP Phone Type

When the action type is selected as "IP Phone",

Aksiyon:

IP Telefon

No action is taken on the device connected to the selected profiles. This is a special profile. FastNAC does not interfere with the Voice VLANs in which IP phones operate. If IP phones are used

on the network and devices access the network from behind the IP phones, this action type must be selected for the IP phones themselves.

1.3.3.4) Quarantine VLAN

When "Quarantine VLAN" is selected as the action type;

Aksiyon:	Karantina VLAN
Atama:	Port Kapatma
	Port Kapatma
	VLAN Değiştirme
Radius:	

This action type is for devices that do not comply with any policy. Two different assignment types can be used;

1.3.3.4.1) Port Closing

When "Port Closing" is selected as the assignment;

Aksiyon:	Karantina VLAN
Atama:	Port Kapatma

This action shuts down the switch port to which the device is connected. (Shutdown or Disabled)

1.3.3.4.2) VLAN Change

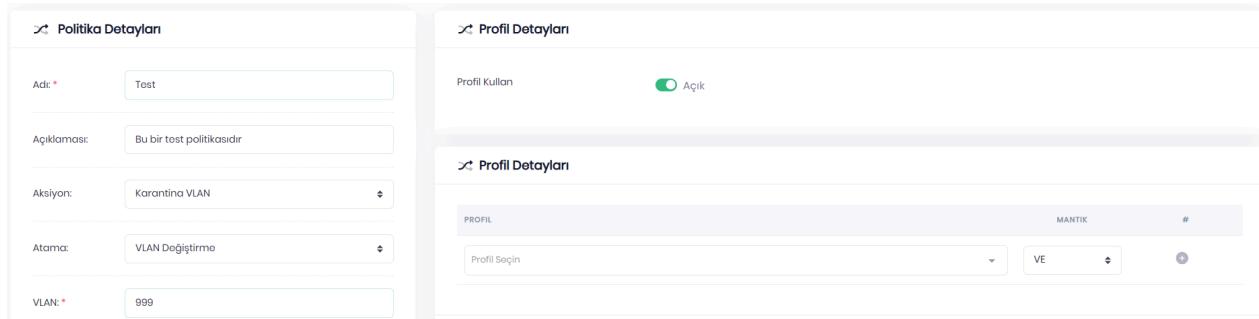
When "VLAN Change" is selected as the assignment;

Aksiyon:	Karantina VLAN
Atama:	VLAN Değiştirme
VLAN: *	999

The device is assigned to the switch port it is connected to, using the VLAN number specified in the "VLAN" section.

1.3.3.4.3) Quarantine and Profile Usage

If you want to control any profile in addition to assigning a quarantine VLAN, you need to enable the " **Use Profile** " option. When you enable this setting, an area where you can select profiles will open directly below the relevant screen.



1.3.3.4.4) General Use Regarding Quarantine

Defining a Quarantine VLAN on FastNAC is not mandatory. However, for general use, creating this policy and placing it at the bottom of the policy list will be more appropriate for the system to function correctly.

" **1.1) Getting Started** ", FastNAC checks policies in a top-down order. If a device gets stuck on any policy, other policies below that policy will not be checked. Therefore, the policy in the Quarantine VLAN action should be at the bottom of the list. For example, let's say we have 5 policies. These are;

Policy Name	Type of Policy	Action
IP_Phone	IP_Phone	-
Printers	VLAN Modification	20
IP_Cameras	VLAN Modification	30
Domain_Control	Interface VLAN	-
Quarantine	Quarantine VLAN -> VLAN Change	999

IP_Phone " -> " **Printers** " -> " **IP_Cameras** " -> " **Domain_Control** " will be checked

sequentially on a device connected to the network . If it doesn't comply with any of the policies, it will be flagged as the last policy, " **Quarantine** ", and assigned to VLAN 999.

If a quarantine-type policy is not written, and the device does not encounter any policy violations during policy checks, no action will be taken, and the device will remain in the port's existing VLAN.

1.3.3.5) Location VLAN

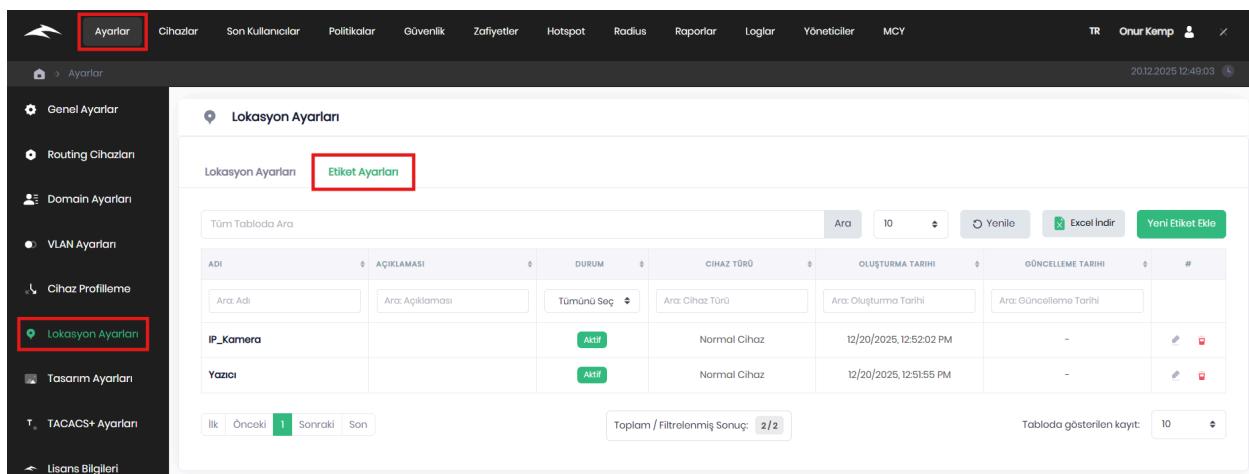
When "Location VLAN" is selected as the action type;

Aksiyon:	Lokasyon VLAN
Etket Seç:	İlgili etiketi seçiniz.

Under the Action section, there is a "Tag". The "Select" input field opens. Here, the selected label is transferred to the specified VLAN number.

No assignment selection is made for the location VLAN type. Actions to be taken according to the selected profiles are performed via tags.

For VLAN label settings, go to "Settings" -> "Location" Settings" -> "Tags". You can check the labels in the "Settings" section;



ADI	AÇIKLAMASI	DURUM	CIHAZ TÜRÜ	OLUSTURMA TARİHİ	GÜNCELLEME TARİHİ
IP_Kamera		Aktif	Normal Cihaz	12/20/2025, 12:52:02 PM	-
Yazıcı		Aktif	Normal Cihaz	12/20/2025, 12:51:55 PM	-

To assign VLAN numbers to the tags you created, go to "Settings" -> "Location". You can edit the locations in the "Settings" section;

On the location editing screen, select "**Tag**". When you open the "**VLAN Settings**" section, you can enter VLAN definitions for the labels you created;

1.3.3.5.1) General Usage Regarding Location VLANs

Let's explain location VLANs in detail. For example, you have switches in multiple locations. We add these locations to FastNAC;

Lokasyon Ayarları		Etiket Ayarları					
Tüm Tabloda Ara							
ADI	AÇIKLAMASI	DURUM	OLUŞTURMA TARİHİ	GÜNCELLEME TARİHİ	#		
Ara: Adı	Ara: Açıklaması	Tümünü Seç	Ara: Oluşturma Tarihi	Ara: Güncelleme Tarihi			
B_Lokasyonu		Aktif	6/3/2025, 10:40 PM	6/1/2025, 10:22:22 AM			
A_Lokasyonu		Aktif	6/3/2025, 10:32 PM	6/1/2025, 10:22:29 AM			
Genel	Varsayılan Lokasyon	Aktif	8/28/2024, 11:37:58 AM	-			

For example, we added three locations: “ **General** ”, “ **Location A** ”, and “ **Location B** ”. Then we added two more tags: “ **IP_Camera** ” and “ **Printer** ”.

Lokasyon Ayarları		Etiket Ayarları					
Tüm Tabloda Ara							
ADI	AÇIKLAMASI	DURUM	CIHAZ TÜRÜ	OLUŞTURMA TARİHİ	GÜNCELLEME TARİHİ	#	
Ara: Adı	Ara: Açıklaması	Tümünü Seç	Ara: Cihaz Türü	Ara: Oluşturma Tarihi	Ara: Güncelleme Tarihi		
IP_Kamera		Aktif	Normal Cihaz	12/20/2025, 12:52:02 PM	-		
Yazıcı		Aktif	Normal Cihaz	12/20/2025, 12:51:55 PM	-		

“ **Location** ” section. We go to the “Edit **General** ” location section and select “ **Tags** ”. We open the “ **VLAN Settings** ” section.

Lokasyon Düzenle

Adı: *

Açıklama:

Etiket VLAN Ayarları: Açık

Tabloda Ara Yenile

Etiket VLAN'larını boş olarak kayıt ederseniz herhangi bir aksiyon alınmayacaktır.

ADI	AÇIKLAMA	CIHAZ TÜRÜ	VLAN
Yazıcı		Normal Cihaz	10
IP_Kamera		Normal Cihaz	20

İptal Et ► Düzenle

On this screen, we see the tags we created. We assign a VLAN to the “ **IP_Camera** ” and “ **Printer** ” tags within the “ **General** ” location and click the “ **Edit** ” button. (In the example above, VLAN 10 is assigned to “ **Printer** ” and VLAN 20 to “ **IP_Camera** ”.)

Next, we perform the same operation for “ **A_Location** ”, and this time we assign VLAN 100 to “ **Printer** ” and VLAN 200 to “ **IP_Camera** ”;

Lokasyon Düzenle

Adı: *	A_Lokasyonu		
Açıklama:			
Etiket VLAN Ayarları:	<input checked="" type="checkbox"/> Açık		
<input type="button" value="Tabloda Ara"/> <input type="button" value="Yenile"/>			
Etiket VLAN'larını boş olarak kayıt ederseniz herhangi bir aksiyon alınmamayacaktır.			
ADI	AÇIKLAMA	CIHAZ TÜRÜ	VLAN
Yazıcı		Normal Cihaz	100
IP_Kamera		Normal Cihaz	200

Finally, we perform the same operations in “ **B_Location** ”, and this time we define VLAN 500 for “ **Printer** ” and VLAN 700 for “ **IP_Camera** ”.

we create a profile named “ **Writer** ” and the Action is “ **Location** ”. We select “ **VLAN** ” and choose “ **Printer** ” as the label;

Politika Detayları	Profile Details
Adı: *	Yazıcı
Açıklaması:	
Aksiyon:	Lokasyon VLAN
Etiket Seç:	İlgili etiketi seçiniz.
Radius:	<input type="button" value="Yazıcı"/> <input type="button" value="IP_Kamera"/> <input type="button" value="Press enter to select"/>
<input type="button" value="Politika Düzenle"/>	

If we were to interpret this policy;

Any device connected to the "**Printer**" profile;

- If it is in the "General" location, the label will be assigned to VLAN 10, which we specified as the VLAN assignment.
- If it is in the "A_Location" location, the label will be assigned to VLAN 100, which you specified as the VLAN assignment.
- If it is in the "B_Location" location, the label is assigned to VLAN 500, which we specified as the VLAN assignment.

We can interpret this as "to be assigned". Location VLAN action eliminates the need to add separate profiles/policies for each location. You can control devices through a single profile/policy.

1.3.3.6) No Action

As an action genre, "**Action**" When "**Alma**" is selected;

Aksiyon:

Aksiyon Alma



No action is taken on devices connected to the selected profiles. It can be used for certain special cases. For example, a policy such as "No action should be taken on the device connected to the profile, but it should notify me when it tries to access the network" can be set as "**Action**". You can create it with "**Alma**".

1.3.4) Radius

When the "Radius" option is enabled;

Radius:



Açık

Bu politikayı Radius bağlantı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

FastNAC allows you to create policies using a hybrid approach with both next-generation and traditional (Radius) methods. You need to enable this setting to specify that the policy will be controlled via Radius connections.

"**Radius**" setting is enabled, the Action type should be "**VLAN**". "**Change**" and "**Quarantine VLANs**" are included. You can find details of these action types under the heading "**1.3.3) Action Types**".

1.3.5) VPN

"**VPN**" option is turned on;

Radius:

Açık

Bu politikayı Radius bağlantısı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

You are indicating that the relevant policy will be checked for devices connecting via VPN. When the "**VPN**" **setting is enabled**, "**Auth**" and "**Deauth**" appear as the Action types .

1.3.5.1) Auth Type

Auth " is selected as the action type ;

Aksiyon:

Auth



Radius:

Kapalı

Bu politikayı Radius bağlantısı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

VPN:

Açık

Bu politikayı VPN bağlantısı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

By connecting the device to the relevant profiles, you are authorizing it and allowing it to access the network.

1.3.5.2) Deauth Type

Deauth " is selected as the action type ;

Aksiyon:

Deauth



Radius:

Kapalı

Bu politikayı Radius bağlantısı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

VPN:

Açık

Bu politikayı VPN bağlantısı üzerinde kontrol etmek istiyorsanız bu ayarı açmalısınız.

By associating with these profiles, you prevent the device from connecting to the VPN.

1.3.6) Situation

" **Status** " section, you can select the status of the policy;

Durum:

Aktif



Aktif

Devre Dışı

- If "**Active**" is selected, the policy will continue to operate.
- "**Circuit**" If the "**outside**" option is chosen, the policy will not work.

1.3.7) Notifications

"**Notifications**" section, you can enable email notifications for devices that fall under the relevant policy.

Bildirimler: Eposta Bildirimleri

If a device violates the relevant policy, go to "**Settings**" -> "**General**" **Settings** -> **Notifications Settings** -> **Submission** It sends notification emails to the email addresses added in the "**Addresses**" section.

Note: For email notifications to be sent in the policies, the General Notification setting must be enabled. "**Settings**" -> "**General**" **Settings** -> **Notifications Settings** -> **Notifications** You need to check that the "**Policies**" section is enabled in the "**Features**" section.

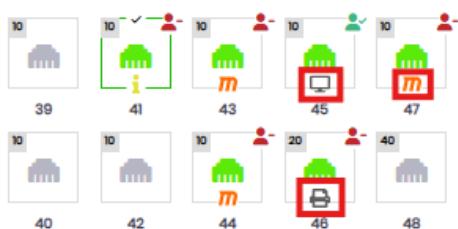
1.3.8) Icon (Port Visualization)

You can choose to add icons to devices connected to the relevant profile;

Ikon

Ikon Seç ▾

Policy icons are displayed below the ports on the switch detail pages. When you access the switch detail page, you can see in real-time which device is connected to which port.



The icons on this screen come from the policy section. For any device that violates a policy, the icon you select will appear under the port.

FastNAC comes with 16 icons by default. You can also add your own icons to the system. Go to "**Settings**" -> "**Design**". **Settings**" -> "**Icon** In the "**Settings**" section, under "**New**" You can upload icons from your computer using the "**Add Icon**" button.

Note: The icon formats you wish to upload must be "**image/svg**", "**png**", "**jpeg**", or "**jpg**".