

***DrayTek***

*DrayOS5*  
***Account & Permission***



# Inhoudsopgave

- Account & Permission..... 3
  - Local Admin Account..... 3
  - Role & Permission ..... 4
  - User & MFA Security..... 6

## Account & Permission

Account & Permission geeft de DrayOS5 gebruiker de mogelijkheid om zelf de gebruikersaccounts te beheren en hun toegangsrechten te configureren.

### Local Admin Account

De **Local Admin**-accounts zijn de accounts die toegang hebben tot de WebUI van de DrayTek. Standaard is er één account aanwezig, namelijk de admin-gebruiker. Door op Edit te klikken, kunt u het admin-account beheren. Daarnaast kunt u tot vier extra gebruikers aanmaken.

Account	Role	Status	Allow Login from WAN	Last Login at	Last Login IP	Created Time	Option
admin	Administrator	Active	Disable	2024-11-04 08:26:35	192.168.1.11	2021-10-24 11:10:17	Edit

Hier kunt u het wachtwoord of de rol van de admin gebruiker wijzigen. Daarnaast kunt u MFA inschakelen en aangeven of de gebruiker vanaf WAN mag inloggen.

De rol van de gebruiker bepaalt de rechten die deze gebruiker heeft. Deze rechten kunt u instellen in het **Role & Permission**-menu, dat op de volgende pagina verder wordt besproken.

Account: admin

Current Password: [password field]

New Password: [password field]

Confirm New Password: [password field]

- At least 8 characters
- Uppercase characters
- Lowercase characters
- Numbers or Special characters -!@#%&^&#0\_=/?[]{}<>\

Role: Administrator

Status: Active

Allow Login from WAN: [toggle]

Enable Email: [toggle]

Enable SMS: [toggle]

MFA

Enable MFA: [toggle]

Account Info

Created Time: 2021-10-24 11:10:17

## Role & Permission

Bij Role & Permission zijn er al twee gebruikersrollen vooraf gedefinieerd: de Administrator-rol, die alle rechten heeft, en de Guest-rol, die alleen Read-only rechten heeft. U kunt zelf een eigen rol aanmaken en per menuonderdeel bepalen wat deze gebruikersrol niet mag zien (Deny), wel mag zien (Read-only) en mag wijzigen (Read-write).

System Maintenance / Account & Permission

Local Admin Account **Role & Permission** User & MFA Security

### Role & Permission

[+Add](#) Max: 5

Role	Administrator	Guest	Users
<b>Left Menu Path</b>			
▶ Device Menu	Deny	Deny	Deny ▼
▶ Dashboard	Read-write	Read-only	Read-only ▼
▶ Configuration	Read-write	Read-only	Read-only ▼
▶ Security	Read-write	Read-only	Read-only ▼
▶ IAM	Read-write	Read-only	Read-only ▼
▶ VPN	Read-write	Read-only	Read-only ▼
▶ Monitoring	Read-write	Read-only	Read-only ▼
▶ Utility	Read-write	Read-only	Read-only ▼
▶ System Maintenance	Read-write	Read-only	Read-only ▼
▶ Virtual Controller	Deny	Deny	Deny ▼
▶ Wireless	Read-write	Read-only	Read-only ▼
▶ Switch	Read-write	Read-only	Read-only ▼

Onderstaand voorbeeld geeft een gebruikersrol weer voor een gebruiker die enkel rechten heeft om de Wireless LAN instellingen van zijn netwerk te wijzigen. De overige configuratie instellingen zijn enkel read-only.

Role & Permission				
+Add		Max: 5		
Role	Administrator	Guest	Users	Thuisgebruiker
Left Menu Path				Delete
▶ Device Menu	Deny	Deny	Deny	Deny
▶ Dashboard	Read-write	Read-only	Read-only	Read-only
▼ Configuration	Read-write	Read-only	Read-only	----
Physical Interface	Read-write	Read-only	Read-only	Read-only
WAN	Read-write	Read-only	Read-only	Read-only
LAN	Read-write	Read-only	Read-only	Read-only
DNS	Read-write	Read-only	Read-only	Read-only
Wireless LAN	Read-write	Read-only	Read-only	Read-write
Routing	Read-write	Read-only	Read-only	Read-only
RIP	Read-write	Read-only	Read-only	Read-only

De gebruikersrol kunt u vervolgens koppelen aan een Local Admin Account.

The screenshot shows the DrayTek Vigor2136ax web interface. The user is logged in as 'thuisgebruiker'. The page title is 'Configuration / LAN'. The breadcrumb trail is 'LANs > Blind IP to MAC > DHCP Options > Inter-LAN Routing > VLAN List > Interface VLAN > LAN Port 802.1X'. A red warning message states 'Read-Only Mode. All changes will be discarded.' Below this, there is a table for LANs with the following data:

Name	Usage	IPv4 Address	Subnet Mask	IPv4 DHCP Server	Primary DNS	IPv6 Assignment	Router IPv6 Address Table	Option
LAN1	NAT	172.31.254.1	255.255.255.0/24	On	8.8.8.8	Manual		Edit

## User & MFA Security

Brute Force Protection staat standaard ingeschakeld op uw DrayOS5-apparaat. Dit betekent dat bij 5 foutieve inlogpogingen de gebruiker op een blocklist wordt geplaatst voor 300 seconden. Na deze periode wordt het IP-adres vrijgegeven en kan de gebruiker opnieuw proberen in te loggen.

### User & MFA Security

---

#### Brute Force Protection

Maximum Login Attempts (Times, 3-255)

Penalty Period (Sec., 300-86400)

Enable User Account Lockout

Daarnaast kunt u User Account Lockout inschakelen, deze feature zal bij 10 foutieve login pogingen alle user accounts tijdelijk op disable zetten.

Enable User Account Lockout

Login Attempts (Times, 3-255)

Unlock User Account After

Send Lock Email to Users

### **Voorbehoud**

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

### **Copyright verklaring**

© 2024 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

### **Trademarks**

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.