DrayTek

IAM

Identity & Access Management

DrayTek IAM is a built-in framework within DrayOS 5 routers that brings Zero Trust security to your network gateway.It enables granular control of user identities, device access, and privileges, replacing legacy IP-based firewall rules with identity-centric access policies.

Key Benefits

- **Role-based Access Control (RBAC):** Define user roles and privileges rather than relying on IP-based rules.
- **Zero Trust Architecture:** "Never trust, always verify" - every access request is validated.
- **Multi-Factor Authentication (MFA):** Enforce two-step authentication and restrict access by device, location, or group.
- **Unified Management:** Integrates with router user accounts, guest hotspot, MAC lists, VLANs, and device inventory for complete control.

Features at a Glance

- **Users & Groups:** Create user profiles and assign them to groups with defined privileges. Supports MFA using TOTP.
- **Access Policies:** Define which users or devices can access specific network resources or services.
- **Group Policies:** Combine IP/content filters, conditional access policies, and VLAN-based restrictions.
- **Conditional Access:** Apply additional authentication or device validation; manage access by VLAN, device, or time period.
- **Resource Management:** Catalog local devices (servers/workstations) by IP/MAC and enforce resource-based access control.

Technical Specifications

- Embedded in DrayOS 5 (starting from Vigor2136 Series onward).
- Supports MFA (TOTP) and Single Sign-On (where applicable).
- Role-Based Access Control (RBAC) for users and groups.
- Device-based access control via MAC address and VLAN membership.
- Policy enforcement integrated with firewall, guest hotspot, and VLAN configuration.
- Configuration backup and restore for identity continuity.

Use Cases

- **Branch Office Security:** Control which users/devices may access internal servers, guest Wi-Fi, or the internet.
- **Campus or Multi-Tenant Networks:** Segment access by role (e.g., student, staff, guest) with different VLAN and policy rules.
- **Remote Work:** Enforce user and device authentication for VPN or remote access tied to verified identities.

Why Choose DrayTek IAM

- **Integrated Platform:** IAM is built into DrayOS 5 routers-no additional hardware required.
- **Simplified Deployment:** Centralized policies and user management through a familiar web interface.
- **Unified Security Posture:** Integrates identity, device, network, and resource-level controls.
- **Cost-Effective:** Uses existing DrayTek infrastructure-no need for a separate IAM appliance or subscription.

Licensing & Compatibility

- IAM is included in DrayOS 5 routers; no separate IAM license is required.
- Compatible with supported DrayTek models—check firmware release for details.
- Scalable via DrayTek central management platforms such as VigorACS (licensed).
- Functionality varies depending on firmware version and router model.

Getting Started

1. Update your DrayOS 5 router to the latest firmware version.
2. Navigate to **IAM > Users & Groups** to create user accounts and enable MFA.
3. Define **IAM Policies** under **IAM > Access Policies**, assigning rules based on user, device, and VLAN.
4. Use **IAM > Resources** to register critical internal assets by IP/MAC and apply access policies.
5. Monitor and audit access activities via system logs and enforce conditional access for higher security.

E-mail: info@draytek.com Tel: +886 3 5972727 Fax: +886 3 598 2121