

# AIMdefense

## AIMdefense System Migration Guide from ICM Defense on AIMdefense

## AIMdefense Guide to System Migration from ICM Defense to AIMdefense

**Please read these instructions carefully before starting the migration!**

**If you use DynDNS, please save the old data from the config, as these will have to be set up again after the migration.**

**If you use the Unifi module, please read the Unifi update instructions first.**

**A system migration to AIMdefense is only possible from version ICM Defense 22.7. If you have an ICM version older than 22.7, please first update to ICM version 22.7 and then start the system migration to AIMdefense. Otherwise, only a new installation using an ISO file is possible.**

- Access the firewall via SSH and log in with:

User Name:            **root**  
Password:             **sysadm**

- Select option 8 for **Shell**.

```
0) Logout                7) Ping host
1) Assign interfaces     8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system       12) Update from console
6) Reboot system          13) Restore a backup

Enter an option: 8

root@AIM:~ # curl -s -o migrate.sh https://pkg.aimdefense.tech/migrate.sh
root@AIM:~ # sh migrate.sh
```

Run **“curl -s -o migrate.sh https://pkg.aimdefense.tech/migrate.sh”** (do not pipe!).

```

  _ _ _ _ _
 /_/_/_/_/_/
/_/_/_/_/_/
/_/_/_/_/_/
Migration Tool v1.6.1

Please make sure this system has access to the internet!
Are you sure you want to continue? [y/N] █

```

- Confirm with "Y".

```

>>> Cleaning up... done
>>> Reboot now? [y/N] █

```

- Confirm with "Y".

• If DynDNS was set up, please set it up again. The DynDNS address changes as follows:

- “dyn.tgfw.de” becomes “dyn.aimdefense.tech”.
- “icm.tgfw.de” becomes “aim.aimdefense.tech”.
- “tg” becomes “s2f”.

Examples of this:

- tg-1-22.dyn.tgfw.de => s2f-1-22.dyn.aimdefense.tech
- 33321-2.icm.tgfw.de => 33321-2.aim.aimdefense.tech

To set up DynDNS with the new **ddclient**, please use the DynDNS instructions (please update until it installs itself).

You can find the path to this in the provided DynDNS instructions.

The migration log can be found at `/root/migration_Zeitstempel.log`.

The screenshot displays the AIMdefense configuration interface. On the left is a navigation sidebar with categories like Lobby, Reporting, System, Access, Interfaces, Network Services, Firewall, VPN, Certificates, High Availability, Monitoring, Wireless, Other Services, Services, Data Recovery, Power, AIMdefense, and Logout. The main content area shows the 'Firewall' settings, with the 'Logging' section expanded. Under 'Logging', there are five entries: 'Default block' (checked), 'Default pass' (checked), 'Outbound NAT' (unchecked), 'Bogon networks' (checked), and 'Private networks' (checked). Below this is the 'Miscellaneous' section with settings for 'Keep counters' (unchecked), 'Debug' (set to 'Generate debug messages only'), 'Firewall Optimization' (set to 'normal'), 'Bind states to interface' (unchecked), 'Disable Firewall' (unchecked), 'Firewall Adaptive Timeouts' (set to 'start'), 'Firewall Maximum States' (input field), 'Firewall Maximum Fragments' (input field), 'Firewall Maximum Table Entries' (set to '200000'), 'Static route filtering' (unchecked), 'Disable reply-to' (unchecked), 'Disable anti-lockout' (unchecked), 'Aliases Resolve Interval' (input field), and 'Check certificate of aliases URLs' (unchecked). The 'Anti DDOS' section has 'Enable syncookies' set to 'never (default)'. A 'Save' button is located at the bottom right of the settings area.

In order to activate all **aliases** (can be found under "**Firewall**" -> "**AIMdefense**" -> "**Settings**"), the default entry must first be set to "**2000000**" under **Firewall** → **Settings** → **Advanced** → "**Firewall Maximum Table Entries**". (Default is 1000000, which is too low.)

The screenshot displays the 'Firewall: AIMdefense: Settings' page in the AIMdefense web interface. The left sidebar contains a navigation menu with various system and security options. The main panel is divided into sections for configuration:

- IPv4**: The active tab for the firewall settings.
- AIMdefense Basic**:
  - AIMdefense Basic Alias:
  - Enable VOIP:
- AIMdefense Advanced**:
  - Enable Abuse:
  - Enable Attack:
  - Enable Compromised:
  - Enable Malicious:
  - Enable Malware:
  - Enable Phishing:
  - Enable Proxies:
- AIMdefense Firewall Rules**:
  - Hints for Firewall Rules:
  - Rule interfaces: WAN (dropdown menu)
  - Clear All:
  - Direction: any (dropdown menu)

At the bottom of the settings area, there are buttons for 'Add Rule', 'Remove Rules', and 'Apply'.

**Technical note:** In rare cases it can happen that the login shell of existing users on the AIMdefense can be set to “nologin” during the update and they can no longer log in afterwards. If you are affected by this, please follow the troubleshooting steps below:

Click “**Access / Usermanagement /Users**” User Edit and then change the “**Login shell**” again by entering: `/bin/sh` and save.

