defguard

Product Data Sheet

Defguard 2.0 - Enterprise WireGuard® VPN & Zero-Trust Identity Platform

Self-hosted · EU jurisdiction · ISO 27001 certified · Open-source core · True VPN MFA · Full SSO/OIDC · Production-ready deployment

version 2.0.0 date 2026.02.11

Defguard sp. z o.o, Cyfrowa 6/317, 71-441 Szczecin, Poland

1. Product Overview

Defguard is an enterprise-grade, self-hosted WireGuard® VPN and identity management platform. It combines secure remote access, zero-trust multi-factor authentication, and a full OpenID Connect identity provider in a single, deployable product. All components run within the organisation's own infrastructure — no data, metadata, or traffic is ever routed through Defguard's servers.

Defguard is developed by Defguard sp. z o.o. (headquartered in Poland), operating entirely under EU law. The platform is ISO 27001 certified (Bureau Veritas Polska Sp. z o.o., Warsaw), GDPR-native, and NIS2-ready. Its open-core codebase is publicly available on GitHub and written in Rust for memory safety and portability.

Defguard 2.0 is available as a one-line install script, Docker Compose, Kubernetes, Terraform, OVA, and AWS AMI/CloudFormation — suitable for bare-metal, private cloud, and hybrid environments.

About	About Defguard
Features overview	Features Overview
Quick install	One-Line Install Script
Architecture	Architecture
Secure by design	Secure by Design

2. VPN & Network

2.1 WireGuard® Protocol

Defguard uses WireGuard® as its VPN data plane — selected for its modern cryptography, minimal attack surface, and performance. Both Linux/FreeBSD kernel-native WireGuard and a cross-platform userspace implementation (based on Defguard's own Rust library) are supported, including FreeBSD/OPNsense/PFsense.

- Linux and FreeBSD/OPNsense/PFsense kernel WireGuard support
- Cross-platform userspace WireGuard (Rust library)
- Import existing WireGuard server configuration via built-in wizard
- Automatic IP allocation for new peers within a VPN Location

VPN feature page	Zero-Trust VPN with 2FA/MFA
Userspace WG	Userspace WireGuard-go Implementation

2.2 Multiple VPN Locations & High Availability

Administrators can define multiple independent VPN Locations (networks/sites) within a single Defguard instance. Each Location can have multiple Gateways, providing active-active or active-passive high availability and failover across a cluster of routers or firewalls.

- Unlimited VPN Locations per instance
- Multiple Gateways per Location for HA/failover
- Per-Location access control: all users or specific groups only
- Dashboard and real-time statistics for connected users/devices

Create Location	Create/Manage VPN Location
Network overview	Network Overview Dashboard
High Availability	High Availability and Failover

2.3 Split Tunneling & Traffic Policy

Split tunneling is configured per VPN Location via the Allowed IPs field, which defines which network ranges are routed through the tunnel. The Client Traffic Policy setting gives administrators three enforcement modes:

- None — users may freely choose between predefined routes and full-tunnel
- Disable all traffic — only predefined routes are available; full-tunnel option is hidden
- Force all traffic — all traffic is routed through the VPN regardless of user preference

Allowed IPs	Create/Manage VPN Location (Allowed IPs)
Traffic Policy	VPN & Client Behaviour Customisation

2.4 Access Control List (ACL)

The ACL feature enables granular, per-resource access control within a connected VPN tunnel. Rules can allow or deny traffic by user, group, or device, targeting specific destination IP/CIDR ranges with optional port and protocol filtering. ACL Aliases allow sets of addresses or ports to be named and reused across rules. Changes are applied in real time.

Enterprise: ACL is an Enterprise feature.

ACL	Access Control List
ACL Aliases	ACL Aliases
ACL Internals	ACL Implementation Details

2.5 DNS, Static IPs & Advanced Network Options

- Custom DNS servers and search domains per VPN Location, pushed to connected clients
- Static IP assignment: administrators can assign fixed IPs to specific users or devices
- User SNAT Bindings: bind specific users to a source NAT address on the gateway so their traffic appears to originate from a designated IP
- Service Locations: a dedicated location type for connecting infrastructure services, separate from user-facing VPN Locations
- Network Devices: manage non-user WireGuard peers (IoT devices, servers, printers) within VPN Locations

DNS & Domains	DNS and Domains
Static IPs	Static IP Assignment
SNAT Bindings	User SNAT Bindings
Service Locations	Service Locations

Network Devices	Network Devices

2.6 Gateway Platform Support

The Defguard Gateway component can run on standard Linux servers as well as directly on network appliances, enabling deployment on existing firewall/router infrastructure without additional hardware.

- Linux (all major distributions)
- FreeBSD / OPNsense / PFsense — kernel WireGuard
- OPNsense — dedicated gateway configuration documentation
- MikroTik routers — dedicated deployment guide

OPNsense Gateway	Running Gateway on OPNsense Firewall
MikroTik Gateway	Running Gateway on MikroTik Routers
OPNsense config	OPNsense Configuration

3. Security & Authentication

3.1 Multi-Factor Authentication at VPN Connection Time

Defguard enforces MFA at the moment of VPN connection — not only at web login. The mechanism uses per-location pre-shared keys (PSKs) as one-time authorisation tokens: when MFA is enabled for a Location, a peer is only added to the gateway's WireGuard interface after the user completes the MFA challenge and a PSK is exchanged. Without a valid session key, the connection cannot be established.

Supported MFA methods at VPN connection time:

- TOTP (Time-based One-Time Password, e.g. Google Authenticator)
- Email token
- Mobile biometric authentication — user scans a QR code shown in the desktop client with their enrolled mobile device and authenticates via the device's biometric system (Face ID / Touch ID)

WebAuthn / FIDO2 hardware keys (e.g. YubiKey, passkeys) are supported as an MFA method for Defguard web/SSO login but are not listed as an available method in the desktop client's VPN connection MFA flow.

MFA feature page	Multi-Factor Authentication (MFA/2FA)
Internal SSO MFA	Internal SSO-Based MFA
External SSO MFA	External SSO-Based MFA
MFA setup (users)	Setting Up 2FA/MFA (End-User Guide)

3.2 Platform-Level 2FA/MFA (Web Login & SSO)

For web login and SSO authentication flows, Defguard supports:

- TOTP (Time-based One-Time Password)
- WebAuthn / FIDO2 — hardware key authentication (e.g. YubiKey, Face ID, Touch ID, passkeys)
- Email tokens

3.3 SSH Authentication

Defguard can act as an SSH certificate authority, managing SSH public key authentication for users. This allows organisations to centralise SSH access control alongside VPN access management within a single platform.

SSH Authentication	SSH Authentication

3.4 Forward Authentication

Defguard can serve as a forward authentication provider for reverse proxies (e.g. Nginx, Traefik), enabling SSO-protected access to internal web applications without modifying those applications.

Forward Auth	Forward Auth

3.5 YubiKey Provisioning

Administrators can provision YubiKey hardware security keys for users directly from the Defguard admin interface with a single click, streamlining hardware key deployment at scale.

YubiKey Provisioning	YubiKey Provisioning

3.6 Secure by Design Architecture

Defguard's architecture separates the control plane (Core) from the data plane (Gateways). Communication between Core and Gateways uses gRPC over mTLS. The Core is designed to be kept off the public internet. Every administrative action is logged for traceability. The entire codebase is written in Rust (memory-safe, no runtime) and is publicly auditable. Public penetration testing reports are available at defguard.net/pentesting/.

Secure by Design	Secure by Design
Architecture	Architecture
gRPC SSL	Securing gRPC Communication

4. Identity & Access Management

4.1 Internal OpenID Connect (OIDC) Identity Provider

Defguard is a full-featured, built-in OIDC Identity Provider. Organisations can use Defguard as their sole internal SSO platform — enabling Single Sign-On across all OIDC-compatible applications without any dependency on third-party cloud authentication services.

Internal OIDC/SSO	Internal SSO (OpenID Connect Provider)

4.2 External SSO / OIDC Provider Federation

Defguard can federate with external identity providers for user authentication. Explicitly documented external providers:

- Google
- Microsoft (Azure AD / Entra ID)
- Okta
- JumpCloud
- Keycloak
- Zitadel
- Custom OIDC (generic configuration)

External OIDC	External SSO/OpenID Providers

4.3 LDAP & Active Directory

Defguard supports LDAP and Active Directory integration, including two-way synchronisation of users and groups. Tested with OpenLDAP and Microsoft Active Directory.

LDAP / AD	LDAP and Active Directory Integration

4.4 Role-Based Access Control (RBAC)

Group-based access control is enforced throughout the platform. VPN Locations can be restricted to specific groups. ACL rules can target individual users, groups, or devices. This implements the principle of least privilege: users access only the locations and network resources their group membership permits.

ACL & Groups	Access Control List

4.5 User Self-Service Portal

Beyond initial enrollment, users have an ongoing self-service web portal where they can manage their own MFA methods, add or remove WireGuard devices, revoke access to granted applications, and reset their password — reducing administrative overhead.

User overview	Using Defguard – End-User Overview
Password reset	Password Change / Reset

5. Client Applications

5.1 Desktop Client – Windows & macOS

Native desktop applications for Windows and macOS, written in Rust using the Tauri framework. Supports secure enrollment via token (delivered by email or manually). On macOS, available through the Mac App Store.

- Automatic configuration of all VPN Locations the user has access to upon enrollment
- MFA at VPN connection time: TOTP, email token, and mobile biometric flow
- Real-time configuration sync (Enterprise): policy and network changes propagate automatically in ~30–60 seconds
- macOS: available on Mac App Store

Desktop Client	Desktop Client (End-User Guide)
Desktop MFA	Using MFA – Desktop Client
Auto-provisioning	Desktop Client Auto-Provisioning
Real-time sync	Automatic Real-Time Client Configuration & Sync

5.2 Mobile Client – iOS & Android

Native mobile applications for iOS and Android. Supports QR code enrollment for frictionless onboarding. The mobile client is also the device used in Defguard's biometric MFA flow: the user scans a QR code displayed in the desktop client, authenticates biometrically on the mobile device, and only then does the VPN connection proceed.

Mobile Client	Mobile Client (End-User Guide)
Biometric MFA	Multi-Factor Authentication – Mobile Biometrics

5.3 CLI Client

A command-line client is available for Linux and headless environments, providing the same VPN connection capabilities as the desktop client without a graphical interface.

CLI Client	CLI Client

5.4 Standard WireGuard Clients

Any standard WireGuard® client (e.g. the official WireGuard app on Windows, macOS, iOS, Android, or Linux) can connect to a Defguard-managed Location by adding a device manually. This ensures compatibility with any WireGuard-capable device.

Other WG clients	Other WireGuard® Clients

5.5 Remote User Enrollment

Defguard provides a dedicated secure enrollment flow for onboarding users remotely over the internet. Users receive a time-limited enrollment token by email, then self-configure their VPN devices and MFA during the enrollment process. A customisable onboarding message can be presented to users after enrollment completes.

Enterprise: Real-time automatic config sync to already-enrolled clients requires Enterprise licence.

Remote enrollment	Remote User Enrollment
Enrollment (users)	Enrollment & Onboarding (End-User Guide)

6. Observability & Compliance

6.1 Activity & Audit Logs

Defguard records detailed activity and audit logs for all platform events. Features of the logging system:

- User event logging with detailed metadata
- Advanced filtering and search by user, module, event type, and time range
- Role-based visibility: users can view only their own events; admins see all
- Logs grouped by module: Defguard platform, enrollment, VPN
- Real-time log streaming to external SIEM tools (Enterprise feature)

Enterprise: Real-time SIEM log streaming is an Enterprise feature.

Audit Logs	Activity & Audit Logs
SIEM Streaming	Activity Log Streaming to SIEM (Enterprise)
Integrations	Integrations

6.2 Notifications

Defguard sends email notifications via SMTP for the following event types:

- User and administrator notifications (e.g. enrollment invitation, enrollment completion)
- Gateway disconnect / reconnect: administrators are notified when a gateway becomes inactive for a configured period
- New version available notifications

Notifications	Notifications
Email (SMTP setup)	Email Notifications (SMTP Setup)
Gateway notifications	Gateway Notifications
Version notifications	New Version Notifications

6.3 Compliance & Certifications

ISO 27001 Certified Certificate issued by Bureau Veritas Polska Sp. z o.o., Warsaw	**EU Jurisdiction** Headquartered in Poland; operates entirely under EU law; zero foreign legal exposure
GDPR Native Architecture designed for full GDPR compliance; data residency on organisation's own infrastructure	**NIS2 Ready** VPN-level MFA, audit logs, and access controls aligned with NIS2 requirements
Open Source Full codebase publicly auditable on GitHub (open-core model, AGPL licence)	**SBOM** Software Bill of Materials provided in compliance with EU Cyber Resilience Act
Public Pentest Reports Penetration testing reports published at defguard.net/pentesting/	**Rust Codebase** Memory-safe language eliminates entire classes of memory vulnerability

About (EU / open-source)	About Defguard

7. Deployment

7.1 Deployment Options

One-line install script Fastest path to a running instance on a Linux server	**Docker Compose** Container-based deployment with compose file provided
Kubernetes Helm chart and manifests for Kubernetes clusters	**Terraform** Infrastructure-as-code provisioning module
OVA Virtual appliance for VMware / VirtualBox environments	**AWS AMI / CloudFormation** Amazon Machine Image and CloudFormation template for AWS deployments
Standalone packages .deb and .rpm packages for direct installation	**NGINX Reverse Proxy** Documented configuration for NGINX as reverse proxy in front of Core

Deploying to Prod.	Deploying to Production
Docker Compose	Docker Compose
Kubernetes	Kubernetes
Terraform	Terraform
OVA	OVA
AWS AMI	Amazon Machine Image (AMI) / CloudFormation
Standalone packages	Standalone Package-Based Installation
NGINX reverse proxy	Reverse Proxy Configuration (NGINX)

7.2 Operational Tools

- Health check endpoint for monitoring and load balancer integration
- Production deployment verification guide: step-by-step checklist for validating a live deployment
- Linux Kernel WireGuard tuning guide for high-throughput environments
- gRPC SSL/mTLS configuration for Core-to-Gateway communication security

- Migration guides for upgrading between versions
- Pre-production and development release channel available for testing

Health check	Health Check
Prod. verification	Production Deployment Verification Guide
WireGuard tuning	Linux Kernel WireGuard Tuning
gRPC SSL	Securing gRPC Communication
Migration guides	Migration Guides
HW / OS / network	Hardware, OS, Network & Firewall Recommendations

8. Integration & Extensibility

8.1 REST API

Defguard exposes a REST API, secured with API tokens, for programmatic management of users, devices, VPN locations, and policies. This enables integration with existing tooling, CI/CD pipelines, and automation workflows.

API Tokens / REST API	REST API & API Tokens

8.2 Webhooks

Defguard supports outbound webhooks, allowing external systems to be notified of platform events in real time. Webhooks enable integration with SIEM platforms, ticketing systems, and custom automation.

Webhooks	Webhooks

8.3 SIEM Integration

Activity and audit logs can be streamed in real time to external SIEM systems. Integration guides are provided in the Integrations section of the 2.0 documentation.

Enterprise: Real-time SIEM log streaming is an Enterprise feature.

SIEM Streaming	Activity Log Streaming to SIEM (Enterprise)
Integrations	Integrations Overview

9. Licensing & Support

9.1 Licence Model

Defguard uses an open-core model. The base platform is open-source (AGPL). Enterprise features (ACL, real-time client config sync, SIEM streaming, and others) require an Enterprise licence.

Subscription Licence Renews monthly via Defguard's licensing server	**Offline Licence** Does not contact Defguard licensing servers; purchased directly from Defguard sales; issued for a custom period — suitable for air-gapped or restricted environments
Evaluation Licence 14-day evaluation licence available	**Open-Source (AGPL)** Core platform source code publicly available on GitHub

Licence documentation	Purchasing and Using the Licence

9.2 Enterprise Support

- Custom SLA agreements
- Priority issue resolution: critical issues addressed within one business day
- Pre-scheduled support calls with Defguard engineers
- Server migration and licence transfer assistance

Licence & support	Enterprise Licence & Features
Migration / transfer	Server Migration and Licence Transfer
Troubleshooting	Troubleshooting Guide

9.3 Enterprise Feature Summary

Access Control List (ACL) Per-user/group/device allow-deny rules with real-time enforcement	**Real-Time Client Config Sync** Policy and network changes propagate automatically to enrolled desktop clients (~30–60 s)

SIEM Log Streaming Real-time streaming of audit logs to external SIEM tools	**Offline Licence** No external licensing server contact required
Custom SLA Tailored service level agreements with dedicated engineer support	**Priority Support** Critical issues addressed within one business day

All Enterprise features	Enterprise Licence – Full Feature List

10. Client Compatibility Reference

The following table summarises the supported client platforms and their key capabilities. For a detailed feature compatibility matrix, refer to the official documentation.

Platform	Enrollment	VPN Connect	MFA at VPN	Auto Config Sync
Desktop – Windows	Token / email	Yes	TOTP, Email, Mobile biometric	Enterprise
Desktop – macOS	Token / email	Yes	TOTP, Email, Mobile biometric	Enterprise
Mobile – iOS	QR code / token	Yes	Biometric (acts as MFA device)	N/A
Mobile – Android	QR code / token	Yes	Biometric (acts as MFA device)	N/A
CLI (Linux)	Token	Yes	TOTP, Email	—
WireGuard® (3rd party)	Manual config	Yes	Not supported	—

Compatibility matrix Client Application Feature Compatibility