

# Defender 5 Datasheet



>>>Delivering tomorrow's security infrastructure, today

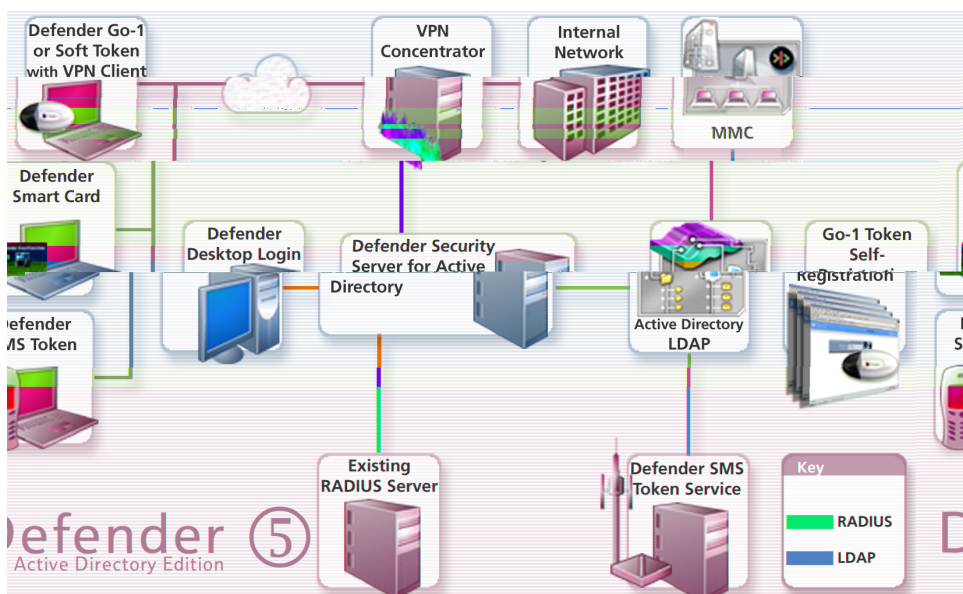
Defender represents the core component of a strategic security infrastructure, used to verify authentication requests and enforce authentication policies across enterprise networks.

PassGo Technologies' Defender represents a revolution in security technology; capable of scaling to accommodate the world's largest networks while protecting enterprise wide VPN, remote access and e-business applications.

## Highlights

### KEY POINTS

- Strong two-factor authentication
- Ensures only authorized users access protected resources
- Full flexibility to control degrees of authentication required
- Support for multiple tokens. Hardware, software and mobile SMS
- Secure and simple initialization, registration, distribution and administration of tokens
- Comprehensive administration and management using Microsoft® standard tools
- Tiered authentication architecture, one-, two- or three-factor
- High availability with multiple authentication servers for load balancing and fault tolerance
- Architected throughout on strong industry standards – providing strong reliable security solutions
- Works towards a 'Forensics Ready' security stance
- Infinitely scalable



## Scalability and Performance

Seamlessly integrated with Microsoft's® Active Directory®, Defender offers a truly extensible architecture which is capable of scaling to fit your business needs. Defender has been deployed across the globe in organizations spanning finance, high technology, government and health care to name a few, and is proven to deliver the highest levels of performance and availability.

# Defender 5

>>>Delivering tomorrow's security infrastructure, today



## User Authentication Where it's Required

Defender authentication can be used by your employees, business partners and customers, whether they are local, remote or mobile.

Whether they require access through VPN to remote access applications, wireless access points, network operating systems, intranets, extranets, Web servers or applications, Defender's strong two-factor authentication ensures that only authorized users are permitted access.

## Migration

The ability to undertake a gradual migration to Defender from incumbent legacy authentication solutions is of crucial importance to security administrators.

With Defender and the legacy system running side by side, Defender's RADIUS proxy feature enables administrators to direct user authentication requests to Defender. If the user is not yet defined within Defender, the authentication request is transparently passed, via the proxy feature, to the incumbent authentication solution.

This allows administrators to migrate users to Defender as and when their tokens expire.

## Centralized Administration

Defender has been architected to integrate fully with Microsoft's® distributed directory service, Active Directory®. This integration leverages all the advantages of the centralized management of the directory information, through a common, user familiar interface.

User token assignment is simply an additional attribute to a user's properties within the directory, consequently making the security administrator's role significantly easier.

## Two-Factor Authentication

With a vendor neutral position, PassGo Technologies can support a wide range of tokens including mobile (SMS), smart cards, software, PDA and USB hardware based tokens, offering a truly flexible and cost effective range of options to suit every requirement.

## Standards Compliance

Defender has been architected around the industry accepted standards of RADIUS and LDAP, with all inter-component communications being encrypted using triple DES ensuring a strong solution throughout.

## Security and Audit

Maintaining a transaction log of all authentication activity, Defender provides a comprehensive audit trail for security administrators monitoring the enterprise, helping to position your business in a forensics ready stance.

- Simple migration using RADIUS proxy feature, ensuring painless migration from other authentication solutions
- Vendor independent
- Full Microsoft® Active Directory® integration
- Secure low administration impact user self-registration
- RADIUS proxy supports user ID delimiters
- Defender desktop login enables strong two-factor authentication at the desktop
- RADIUS compliant
- Defender WebMail option for secure remote web based access to your e-mail
- Check Point OPSEC certified

**PassGo Technologies**  
[www.passgo.com](http://www.passgo.com)

651 Holiday Drive  
Suite 300, PMB #310  
Pittsburgh, PA 15220  
1.888.652.3983  
[sales@passgo.com](mailto:sales@passgo.com)

### Europe

Horton Manor  
Ilminster, Somerset  
TA19 9PY, UK  
+44 (0)1460 258300  
+44 (0)1460 258403 (fax)

*This document refers to a number of hardware and software products that are produced by other companies. In most, if not all cases, the names of these products are claimed as trademarks by the companies that manufacture them. It is not our intention to claim either the products or their names or trademarks as our own.*