

Defender

Secure, Authorized Access for Remote Users

Keeping corporate information safe and secure is a vital concern for every organization. However, as the reliance on sharing information with employees, partners, and customers via the Internet grows, it's no longer practical to shield information from users outside of the enterprise. What is required is a solution that provides secure access to authorized users only. Because they can be easily guessed, cracked, or forgotten, traditional static passwords and IDs have proven to be inadequate for protecting enterprise resources. Defender solves the password challenge with a highly scalable authentication solution for dial-up, VPN, firewall, and other remote access environments.

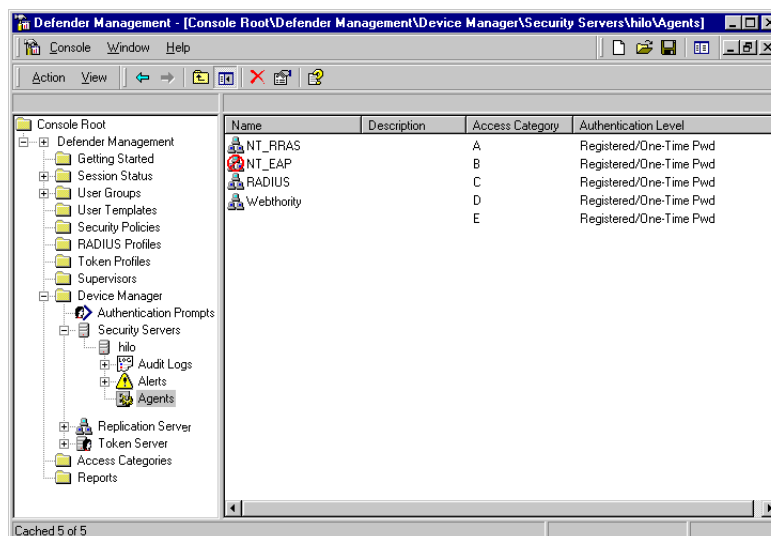
Two-Factor Authentication Stops Unauthorized Access

Using a proven two-factor authentication process, Defender uniquely authenticates authorized remote users, giving them access to the key data and information they need, while protecting sensitive corporate resources from unauthorized use. To ensure secure access, Defender utilizes a token and a user-defined PIN that are unique to each authorized user. Only authorized users with access to their user-specific token and unique PIN can gain secure access to a system or network. Potential intruders cannot compute the one-time password generated by standards-based technology, and, the password itself protects the system because it is valid only once, ensuring that any attempt to capture and re-use it poses no threat.

Highlights

KEY POINTS

- Ensures that only authorized remote users can access the network
- Enables secure and easy initialization and registration of software tokens
- Offers comprehensive administration and management from a Microsoft Management Console snap-in GUI
- Provides high availability for Defender Security Servers with a license for a backup server with automated switchover
- Implements standards throughout its architecture to provide reliable, industry-standard security solutions



Defender

Secure, Authorized Access for Remote Users



Components of the Defender Secure Logon System

Defender Security Server (DSS)

As the authentication authority for remote access, the DSS provides two-factor authentication for VPNs, communication servers, and firewalls. Using challenge-and-response or synchronized authentication processes and the user's unique token and PIN, DSS ensures that only authorized users gain access to the network.

Defender Tokens

Defender is the only security solution that electronically distributes and registers software tokens. The easy-to-use tokens compute a one-time password when queried by the DSS. Defender's system of creating, distributing, installing, registering, using, and maintaining tokens provides a cost-effective, automated solution that is secure and easy to use for both end-users and administrators. Defender also supports hardware tokens, software tokens on secured diskettes, and tokens on smart cards. All tokens require entry of a user-unique PIN for activation and production of a unique one-time password.

Defender Management Console (DMC)

The management console within Defender is a snap-in to the Microsoft Management Console. The DMC reports usage and audit information while managing user IDs, tokens, multiple distributed security servers, security policies, administrators, RADIUS profiles, user groups, and templates from a central console.

Defender RADIUS Server

The Defender RADIUS Server allows communication servers and firewalls that support RADIUS to use the DSS for two-factor authentication. Defender also works with other RADIUS servers that have an embedded Defender agent.

Seamless Integration with Webthority

Webthority includes a built-in Defender agent on the server-side, enabling the client to use Defender software tokens automatically.

Defender Supported Environment

Server Software

- Microsoft® SQL Server 2000 or 7.0
- Windows® 2000
- Windows NT® 4.0

Software Tokens

- Windows 2000
- Windows NT
- Windows ME
- Windows 98/95
- Windows XP

Note: The DSS and Defender RADIUS Server may also be used on Sun systems running the following versions of Solaris: Sun Solaris 2.6 and 8

PassGo Family

Defender

Secure, authorized access for remote users

Defender Webmail

Remote corporate e-mail from anywhere, securely

Webthority

Secure web access for distributed web server environments

Privilege Manager for UNIX

Secure delegation of UNIX account privileges and full audit trail

SSO Plus

Simple, flexible password management

Helpdesk Password ReSync

Enabling end-users to reset their own passwords

SSO and InSync

Simplified access and control

Resource Manager for UNIX

User administration and enhanced security for UNIX

OS/390 Suite

NC-Syncom, NC-Pass, NCI/XF, NC-Access and MultSess

PassGo Technologies

www.passgo.com

651 Holiday Drive
Suite 300, PMB #310
Pittsburgh, PA 15220
1.888.652.3983
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.