

The Leader in Endpoint Data Protection

Advanced Authentication

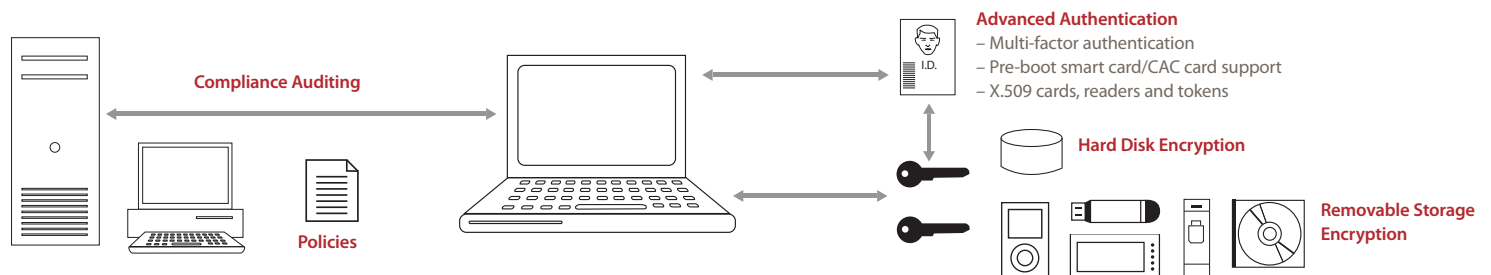
GuardianEdge Advanced Authentication extends the security of the GuardianEdge Data Protection Platform with multi-factor authentication. For systems protected with GuardianEdge Hard Disk Encryption, the solution increases the security of user log-ons, ensuring that only authorized users can access endpoint data. With GuardianEdge Removable Storage Encryption, multi-factor authentication increases the safety of data on removable storage devices and media with strong access control.

A key component of the GuardianEdge endpoint data protection platform, GuardianEdge Advanced Authentication provides support for multi-factor authentication in both the pre-boot execution environment for hard disks and for authenticating to encrypted data stored on removable storage such as CD/DVDs, USB thumb drives, removable hard drives, and other devices. With GuardianEdge Advanced Authentication, enterprises and government agencies can use multi-factor authentication to limit access to their systems and data, including the capability to leverage an existing PKI infrastructure with either software or hardware authentication keys.

Key features

- Pre-boot environment support for multi-factor authentication with GuardianEdge Hard Disk Encryption
- Smart card/common access card (CAC) support
- Extensive support for readers and tokens
- Protect encrypted data stored on removable media from unauthorized access

Protecting Data with Strong, Multi-factor Authentication



Technology Overview

To further safeguard the data on PCs and removable media, multi-factor authentication extends access control with hardware or software certificates and tokens.

GuardianEdge Advanced Authentication extends the security of the GuardianEdge Data Protection Platform with multi-factor authentication. For systems protected with GuardianEdge Hard Disk Encryption, the solution increases the security of user log-ons, ensuring

that only authorized users can access endpoint data. With GuardianEdge Removable Storage Encryption, multi-factor authentication increases the safety of data on removable storage devices and media with strong access control.

Technical Information

Supported GuardianEdge Products

- GuardianEdge Hard Disk Encryption (pre-boot environment authentication)
- GuardianEdge Removable Storage Encryption (data access)

Supported Readers

- Axalto Reflex USB v2 & v3, 20 PCMCIA v2 & v3, Ic v3
- ActivIdentity USB v2, V3, USB Reader 3.0, PCMCIA, ActivKey Sim
- Dell keyboard w/ SmartCard reader
- Dell D600/620 – O2Micro 02711EC1 PCMCIA/Smart Card Controller
- Fujitsu 4220 – O2Micro – Smartcard Reader/PCMCIA\O2MICRO-SMARTCARDBUS_READER-2E10\1
- Dell D610/410 – Texas Instruments PCI GemCore-Based Smart Card Controller
- Dell D800 – Texas Instruments UltraMedia GemCore-Based Smart Card Interface Controller
- Dell Keyboard SK-3106
- GemCore SIM Pro, Express, Twin, Pinpad, Key, 433 SW
- SCM SCR 131, 331 USB, 331-DI NTTCom USB/SCR 331-DI USB, 3310 NTTCom USB/SCR 3310 USB, 3311 USB, 3320 USB, 333 USB, 3340 ExpressCard 54, 335 USB, 338 Smart Card Keyboard, 531, 532 USB, 355 USB, 201 PCMCIA, 241 PCMCIA, 243 PCMCIA
- USB CCID Compatible
- Dell 420 – O2Micro OZ776 USB CCID Smartcard Reader/Ricoh R/RL/5C476(II) or Compatible CardBus Controller
- Dell 430 – O2Micro OZ776 USB CCID Smartcard Reader/Ricoh R/RL/5C476(II) or Compatible CardBus Controller

Supported Cards and Tokens

- Aladdin eToken Pro (USB & Smartcard), NG-OTP (USB)
- Axalto Cyberflex 32K, 64K v1, 64K v2c, e-Gate 32K/Cyberflex Access e-Gate 32K, Access 64K v1, Access 64K v2, Cyberflex Access 64K V1 SM4v2
- Cyberflex Access 64K v1 SM4.1, Access 64K V1 SM 2.1, Access 64K Contact only, CAC longlife body, Access 128K Dual Access, CAC longlife body
- Gemplus GemXpresso 64K v2, GemXpresso ProR3 E64K PK- FIPS V1, GemXpresso PRO R3 E64 PK Standard Version, GXP3, GemXpresso 72K Dual Access, CAC longlife body

- Oberthur CosmopolIC 32K, 32K v4, 32K V4 Fast ATR, 64K v5, 64K v5.2, 64K dual interface v5.2d, 64K v5.2 Fast ATR, GalactIC 2.1-5032 Mask 2.1R
- Safenet DKCOS v2 smart cards, iKey 2032 USB Token, FIPS 201 card, FIPS 201 w/HID Prox card
- Schlumberger Access 32K v2
- RSA SID800, Smart Card 5200

PKI Environment Support

- Supports X.509-compliant Public Key Infrastructure systems

Guardian Edge Data Protection Platform Integration

- Single Management Console – Provides a single, Active Directory integrated management console for administering the GuardianEdge suite of endpoint data protection controls
- Shared Services – Shared security and management services across data protection applications
- Auditing and Reporting – Unified auditing and reporting environment
- Lightweight client environment – Single sign-on integration. Secure client/server communications. Minimal to no intrusion into existing user workflows and operation

Active Directory Integrated Administration and Management

- Tightly integrated with Microsoft® Active Directory®, enabling GPO-based policy deployment
- Easily scales to meet enterprise requirements
- Role-based policy administration
- Detailed audit records to verify policy enforcement

Key/Password Administration and Recovery

- Simple and secure administrative access to encrypted PCs in the event of lost tokens or passwords with self-service or admin-assisted recovery
- Central master certificate (private key) digital certificate based recovery of encrypted data on portable media devices

Corporate Headquarters

475 Brannan St., Suite 400
San Francisco, California
94107-5421

t. +1.800.440.0419

t. +1.415.683.2200

f. +1.415.683.2349

www.GuardianEdge.com

GuardianEdge is a trademark of GuardianEdge Technologies Inc. All other products and services mentioned are the trademarks of their respective companies.