

HA Remote

VPN Client

In today's corporate environment, it is imperative that businesses have options to protect their assets and information through high assurance security technology and follow guidelines for homeland security directives. Remote access security and security within an enterprise are at higher risks now, more than ever. Organizations must address these new threats and worries with a higher grade of communications security.

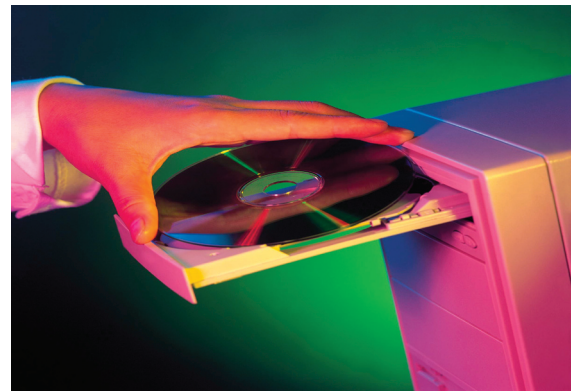
HighAssurance™ Remote is based on SafeNet's de facto standard VPN software product, SoftRemote®. HighAssurance Remote, which includes FIPS technology, device authentication, and the Advanced Encryption Standard (AES) algorithm, is a ground breaking stride towards security aimed at supporting the nation's homeland security efforts, containing numerous high-level security features not currently found in any VPN software product on the market.

WHAT IS HA REMOTE?

With pending FIPS 140-2 Level 2 certified technology and the foundation of the industry's clear standard for VPN software, the HighAssurance Remote client is high assurance VPN software that provides secure client-to-client or client-to-gateway communications over wireless LANs, TCP/IP networks, and dial-up connections. FIPS 140-2 Level 1 and 2 certification is of particular importance since Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services.

And with device authentication, HighAssurance Remote strengthens network access password security by ensuring that all computers that attempt to log on have a second form of identification—a device identifier.

Providing high assurance VPN capabilities to desktops and portable computers for all versions of Microsoft Windows, Solaris, and now including Red Hat Linux, HighAssurance Remote offers unparalleled extended features to remote access users connecting to the corporate VPN, protecting the user from growing hazards posed by hackers wielding tools like Trojan horses, spyware, and other malicious code. Covering both direct and remote access to the corporate network, as well as Internet access, HighAssurance Remote is an "always on" application, protecting the user's PC even when not connected to the corporate VPN.



HighAssurance Remote is built with SafeNet SecureIP Technology™, which provides the building blocks for security implementations that enable organizations to use the Internet and other shared networks for private communications.

Other high assurance features include AES algorithm, MD-5 and SHA-1 hashing algorithms, and compliance with current IPsec RFC standards.

WHO SHOULD USE HIGHASSURANCE REMOTE?

- Employees of critical U.S. infrastructure organizations
- Security conscious organizations including financial, government and commercial organizations
- "At home" and telecommuting users accessing a corporate VPN from a desktop PC or laptop using dial-up, cable modem, or DSL connections
- "Road warriors" remotely accessing a corporate VPN with a laptop using dial-up or ethernet users who have upgraded to Windows® XP

HIGH ASSURANCE VPN CAPABILITIES

HighAssurance Remote includes full compatibility with Microsoft® Windows® XP, support for NAT Traversal (NAT-T), device authentication, support for browser certificates, Section 508 Compliance, and policy protection.

Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they shall ensure that the EIT allows Federal employees with disabilities and members of the public seeking information or services from a Federal agency, to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees and members of the public who are not individuals with disabilities.

When you secure all the PCs connected to your network with device authentication, you can eliminate threats from malicious employees and hackers. The device authentication in HighAssurance Remote, is a strong, two factor authentication using a unique second identification factor associated with the PC itself which has been cryptographically protected.

Wireless & Security

HighAssurance Remote includes policy protection, ensuring the privacy and integrity of a security policy using PKCS7 encryption and PKCS5 password-based encryption. A unique feature only available in SafeNet's remote access clients is the support for browser certificates. HighAssurance Remote can use certificates available in the Microsoft® Internet Explorer browser for IPSec operations, allowing users the ability to import or request certificates using functionality native to their browser. Other features include interoperability with the Nortel Contivity VPN Switch, expanding the extensive interoperability of HighAssurance Remote, which eliminates the need for organizations to provide more than one VPN client to their users.

Compatible with all Microsoft® Windows® operation systems and any IPSec-compliant solution, HighAssurance Remote supports advanced interoperability protocols including: Layer 2 Tunneling Protocol (L2TP), and Extended Authentication Protocol (XAUTH) supporting RSA SecurID™, RADIUS, and Secure Computing SafeWord™ PremierAccess™. HighAssurance Remote also supports Simple Certificate Enrollment Protocol (SCEP), which provides interoperability with certificate authorities that support online certificate requests.

HA Remote SPECIFICATIONS:

• System Requirements

Disk Space - 10 MB

16MB RAM for Windows 95, 98

32 MB RAM for NT

64 MB for Me and 2000

64 MB for XP

• Encryption Algorithms

DES, 3DES, AES

Hash Algorithms

HMAC-MD5

HMAC-SHA-1

DES-MAC

• Compression

IPComp - Deflate and plug-in support for LZS

• Diffie-Hellman Group Support

Group 1 - MODP 768,

Group 2 - MODP 1024,

Group 5 - MODP 1536

• Authentication Mechanisms

Preshared keys, RSA signatures

• Device Authentication

Strong, two factor associated with the PC itself

OTHER ADVANCED FEATURES

- Gateway Hostname Resolution provides the ability to resolve the name of the Secure Gateway Tunnel entry using DNS, WINS, and LMHOST
- Automatic certificate selection - HighAssurance Remote automatically sends its own certificate based on the request of the peer instead of requiring it to be locally configured; and allows the client (based on configuration) to accept any ID from the peer as long as the accompanying certificate is issued by a "trusted" CA.
- Virtual Adapter support, which allows an IPSec gateway to assign network settings for improved network functionality with other applications HighAssurance Remote is built on SafeNet's CryptoGraphic Extensions (CGX) Library. A comprehensive library of encryption features, the CGX Library and HighAssurance Remote are currently being tested and validated for FIPS-140-2 Level 2 certification.

• Key Management

IKE (Internet Key Exchange)

• IPSec Modes

Tunnel, Transport

• IKE Modes

Main, Aggressive, Quick

• Certificate Acquisition

SCEP, PKCS #7 and PKCS #10, PKCS #12

Microsoft Internet Explorer

• Other Features

X.509 V3 support, LDAP directory support, CR

processing, centralized policy management, self-

signed certificate support XAUTH, IKE, support mode

configuration, L2TP support, redundant gateways, IKE

keepalives, pending FIPS 140-2 Level 2 certification,

diagnostic training, audit log, split tunneling, Stateful

Packet Inspection Firewall.

• Stated CA Compatibility

Entrust, Baltimore Technologies, VeriSign, RSA Keon,

Microsoft, Netscape

- Built in personal firewall (installation optional)