



aXsGUARD Identifier

Dedicated and Easy to Maintain Authentication Solution

aXsGUARD is VASCO Data Security's product line of authentication and Internet security appliances. Built around proven VACMAN core technology, aXsGUARD Identifier offers strong user authentication for remote access to the corporate network or to web-based business applications. aXsGUARD Identifier is for enterprises which want a dedicated appliance for their authentication needs.

The number of mobile employees and home-based staff steadily grow; they require access to corporate applications and business critical data any time and anywhere. As a result, network administrators receive requests for flexible yet secure access to applications such as VPN, SSL-VPN, Outlook Web Access, Citrix Web Interface, Intranet, . . .

Remote access is one of the most valuable though most vulnerable features in a corporate network. Corporations no longer can afford to leave their systems and confidential business data unprotected. For hackers, it is child's play to access the corporate network by stealing user credentials.

aXsGUARD® Identifier addresses these security challenges by adding strong user authentication to multiple web-based applications. It is a simple and cost-effective solution, allowing corporations to authenticate their legitimate users and keep unauthorized users from accessing the corporate network.

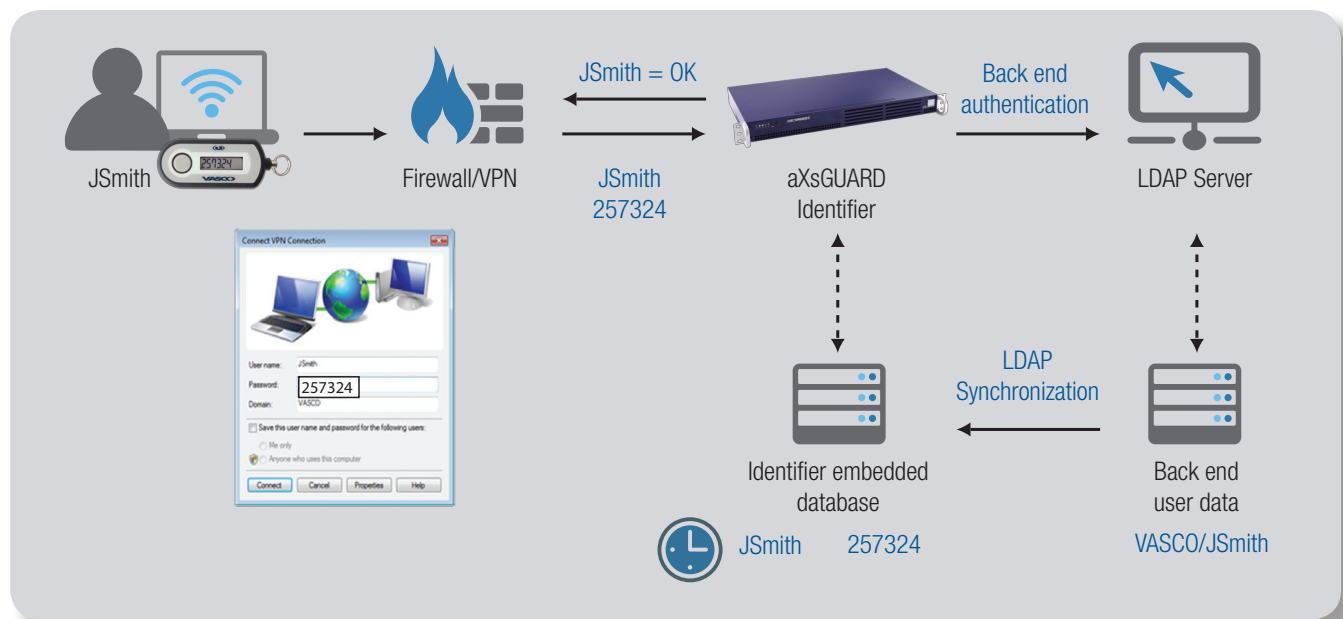
The solution has been designed for corporations which want to avoid sharing server resources for too many business critical applications. As a result they opt for a dedicated appliance to manage authentication requests without impacting the existing IT-infrastructure.

Multiple hardware versions are available for the smallest SME to the largest multi-national depending on the number of users. All aXsGUARD Identifier hardware versions are equipped with the aXsGUARD Identifier Core OS and offer the same software capabilities.

HOW DOES IT WORK?

Instead of using a log-in and static password, employees will use their DIGIPASS® to log on to a Web- or VPN server. The DIGIPASS will generate a One-Time Password (OTP), which can only be used once and which replaces the insecure static password. aXsGUARD Identifier will verify this OTP and will be able to prove the users' identity quickly and easily.

VASCO® has a wide range of DIGIPASS authenticators consisting of one-button devices, pin-pad authenticators, card readers and software based solutions for web browser or mobile phone. Customers can choose from this range and find the authentication device which best fits their needs.



Benefits

Easy to install and manage

- An intuitive web based user interface with wizards helps administrators to setup aXsGUARD Identifier in no time.
- Automatic updates with a complete fail safe mechanism make updates hassle free. Depending on the maintenance contract VASCO also offers remote support on the appliance itself.
- Dedicated task assignment allows administrators to delegate tasks like user or DIGIPASS management or reporting without endangering the appliance runtime environment.
- Self registration allows end-users to activate their DIGIPASS themselves on a secure website.
- Difficult configuration tasks like setting up replication between multiple aXsGUARD Identifiers can be done with a few simple clicks.
- All administration functions are conveniently accessible through a web-based user interface, allowing remote or outsourced administration, offering new opportunities for managed services providers.

Centralized user management

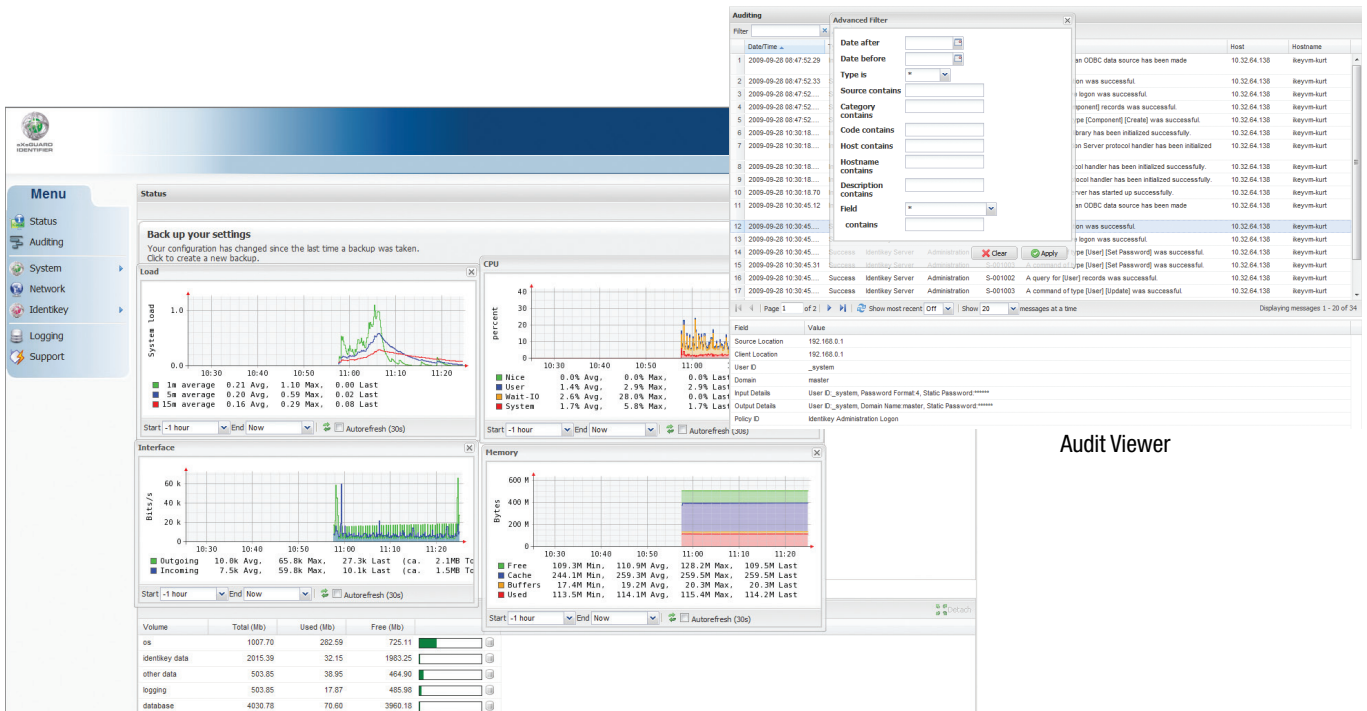
- Thanks to LDAP synchronization, the user management only happens in the main LDAP database (Microsoft Active Directory, Novell e-Directory, or any other LDAP) the company is using. This enhances security and minimizes the administrative tasks of user management.
- Adjustable filters allow to specify which groups of users need to be synchronized towards the aXsGUARD Identifier.
- It is possible to synchronize multiple LDAP domains with only one aXsGUARD Identifier.

Extensive reporting and auditing functions

- The audit console monitors incoming and outgoing RADIUS and web authentication requests. An extensive search mechanism, displaying auditing lines on the fly, helps administrators to quickly solve possible authentication issues.
- Functionality information statistics provide critical details allowing administrators to easily manage the remote access environment.
- Standard or customized reports in XML format.
- Extensive log searching and the possibility to export the log search to an external syslog server.

Other functionality

- Scalability: A flexible license system allows easy expansion of users and DIGIPASS
- Optional lifetime hardware maintenance ensures your appliance (hardware and software) is never out of date.
- Multiple aXsGUARD Identifiers can be cascaded through replication resulting in multiple aXsGUARD Identifiers in branch offices for authentication, and a central aXsGUARD Identifier for reporting, both equipped with failover.



aXsGUARD Identifier Statistics

Audit Viewer



**aXsGUARD
IDENTIFIER**

aXsGUARD Identifier hardware



SPECIFICATIONS	AG3442	AG5502	AG7552
Recommended users	250	10.000	100.000
Authentications/sec	5	50	975
Software	Identikey 3.0.7.	Identikey 3.0.7.	Identikey 3.0.7.
Operating System	Identifier Core OS 8.0	Identifier Core OS 8.0	Identifier Core OS 8.0
Chassis Form Factor	1U Rack Mount	1U Rack Mount	2U Rack Mount
Processor Type	Atom	DUAL Core	Quad Core
Memory	1GB	4GB	12GB
Disk n/size	1 x 320 GB	1 x 500 GB	2x 1 TB
Hot Swappable	No	No	yes
Raid formatted	None	None	RAID 1
Power Supply	AC 100~240V, 50/60 Hz, 4-2 Amp Max 200W max 80 PLUS Certified	AC 100~240V, 50/60 Hz, 4-2 Amp Max 200W max 80 PLUS Certified	AC 100~240V, 50/60 Hz, 10-4 Amp Max 700W max 80 PLUS Certified
Power Redundancy	no	no	Hot swappable
Network Ports	2 GE NIC Bridged ports	2 GE NIC Bridged ports	2 GE NIC Bridged ports
Management	Web GUI SSH consoleport	Web GUI SSH consoleport	Web GUI SSH consoleport
Dimensions (W/H/D)	437mm x 43mm x 249mm 17.2" x 1.7" x 9.8"	426mm x 43mm x 365mm 16.8" x 1.7" x 14"	437mm x 89mm x 450mm 17.2" x 3.5" x 17.7"
Weight	6,7 kg (<15lbs)	7.7 kg (<17 lbs)	17.6 kg (<38.8 lbs)
Compliance to standards	Safety UL, C-UL, CE EMC FCC, CE Environment RoHS	Safety UL, C-UL, CE EMC FCC, CE Environment RoHS	Safety UL, C-UL, CE EMC FCC, CE Environment RoHS
Mounting Position	Horizontal orientation, 19" Rack, 1 U	Horizontal orientation, 19" Rack, 1 U	Horizontal orientation, 19" Rack, 1 U
Operating Temperature	10 to 35 °C, 50 to 90 °F	10 to 35 °C, 50 to 90 °F	10 to 35 °C, 50 to 90 °F
Operating Humidity	8 to 90% (non-condensing)	8 to 90% (non-condensing)	8 to 90% (non-condensing)
Storage Temperature	-40 to +70 °C, -40 to 158 °F	-40 to +70 °C, -40 to 158 °F	-40 to +70 °C, -40 to 158 °F
Storage Humidity	5 to 95% (non-condensing)	5 to 95% (non-condensing)	5 to 95% (non-condensing)
Reliability MTBF	45,000 hours (5 yrs)	45,000 hours (5 yrs)	45,000 hours (5 yrs)

aXsGUARD Identifier CORE OS

FUNCTIONS

- Dedicated Software and Hardware, build for 1 function: Strong user authentication
- Full option authentication server with reporting
- Optimized for easy administration
- Automated updates
- Remote support possibilities

FEATURES

- WEB base GUI for appliance administration and Identikey® administration
- Wizards for Installation and registration
- Wizards for replication of data between aXsGUARD appliances
- LDAP synchronization from:
 - Microsoft Active Directory
 - Novell e-Directory
 - Generic LDAP
- Automated updating system, online and offline
- Backend authentication towards Microsoft Active Directory
- Command line Rescue tool
- Build-in database for auditing en logging storage
- Live Audit Viewer
- Log file viewer with export functionality towards external syslog server
- Build-in backup functionality of settings towards file server
- Built-in connectivity towards SMS Gateway for Virtual DIGIPASS
- Support of all types of DIGIPASS

BENEFITS

- Fast up and running Strong User Authentication solution
- Reduce the maintenance cost of your authentication solution
- Lowest TCO with hard and software maintenance contract

IDENTIKEY for aXsGUARD Identifier

FUNCTIONS

- Strong authentication in a standalone appliance
- Offers complete authentication solution
- Central administration of users, DIGIPASS authenticators and authentication policies

FEATURES

- Supports strong two-factor user authentication
- Verification of DIGIPASS authentication requests from Radius clients and web filters (OWA, CITRIX,IIS)
- Policy based authentication
- Flexible DIGIPASS assign procedures (self-assign, auto assign)
- Dynamic user registration
- Virtual DIGIPASS (SMS-based) support
- Web-based Administration GUI
- Delegated administration
- Support of radius based clients
- Support of multiple backend authentication environments
- Comprehensive audit system
- XML-based reporting
- Internal database for user and DIGIPASS storage
- Step by step Installation wizard

BENEFITS

- Designed to fit the needs of any size organization
- Web-based administration interface offers far-reaching possibilities for service providers
- Easy to integrate, administer and audit
- High availability: Server Replication and Load Balancing
- Built around VASCO's solid and proven VACMAN® core technology
- Complete authentication solution

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security serving a customer base of approximately 8,500 companies in more than 100 countries, including more than 1,250 international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

BRUSSELS (Europe)

phone: +32.2.609.97.00
 email: info-europe@vasco.com

BOSTON (North America)

phone: +1.508.366.3400
 email: info-usa@vasco.com

SYDNEY (Pacific)

phone: +61.2.8061.3700
 email: info-australia@vasco.com

SINGAPORE (Asia)

phone: +65.6323.0906
 email: info-asia@vasco.com