Trustwave®

Trustwave Managed Two-Factor Authentication

STRONG AUTHENTICATION WITHOUT THE HASSLE

The Problems With Hardware-Token-Based Authentication

Legacy hardware-token-based authentication systems require the tracking and management of a separate physical device for each employee—a cumbersome and costly affair. Devices wear out, get damaged or lost, and create excess support tickets for the Virtual Private Network (VPN) in the process. All too often this either reduced productivity or deterred organizations from using strong authentication. The cost and cycles required for IT to manage hardware tokens diverted resources away from other needed security solutions, as well.

An Innovative Solution Inspired by Compliance Needs

Inspired by the Payment Card Industry Data Security Standard (PCI DSS) and dissatisfaction expressed by customers over current solutions on the market, Trustwave developed a two-factor authentication solution that couples digital certificates with an organization's existing VPN infrastructure. This certificate-based authentication drastically reduces the cost of an authentication solution while eliminating the need to track inventory of physical tokens and maintain associated technology such as servers.

While the service's utility extends beyond just PCI DSS compliance, Trustwave developed the solution with PCI DSS requirement 8.3 in mind:

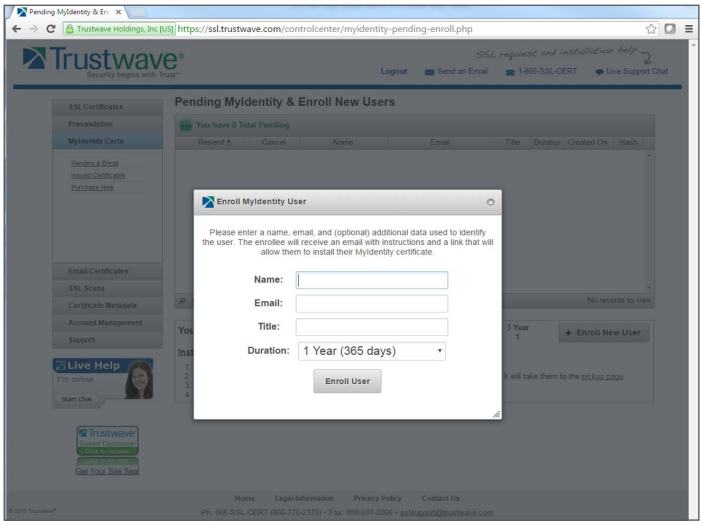
Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service or terminal access controller access control system with tokens; or virtual private network with individual certificates.

Any organization that processes, stores or transmits cardholder data must comply with every requirement of the PCI DSS, and the Trustwave two-factor authentication solution is an innovative, cost-effective method to fulfill requirement 8.3 of the standard. The PCI DSS allows for an individual certificate-based VPN authentication solution to satisfy the requirement. This is an important distinction because the costs of a certificate-based solution can be just one fifth of those associated with a token-based solution. In addition, a certificate-based solution includes a much more reasonable ongoing cost structure.

The Trustwave authentication service utilizes proven digital certificate technology to provide a managed two-factor authentication system that works without the need for hardware tokens or additional network resources.

Key Features and Benefits

- On-Demand reduces infrastructure complexity, labor and cost
- No hardware tokens reduces up-front and replacement costs, user training and hassle
- Two-Factor authentication supports PCI compliance, and other mandates
- Strong-authentication prevents wide range of known and unknown malware and hacking techniques dependent upon taking over legitimate user accounts



How A Certificate-Based Two-Factor Authentication Works in Practice

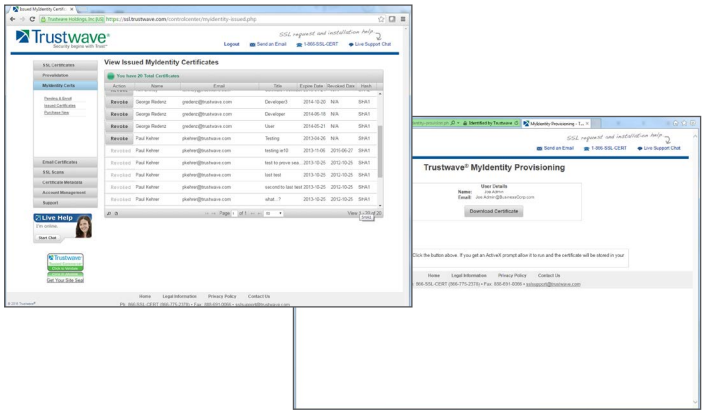
The Trustwave solution leverages your current VPN authentication infrastructure, including your corporate directory system and VPN hardware, and can be implemented and operational with just four easy steps:

1. You deploy a trusted root certificate to your VPN hardware devices to provide a point from which administrators can control user access.
2. Network administrators log into the co-branded Trustwave management portal to provision certificates for employees and contractors.
3. Users access a simple co-branded Web portal to set a certificate password, download the certificate and install it on their remote system.
4. When a user logs into the VPN, they are prompted to use the certificate and password for authentication.

The solution's intuitive Web portal allows administrators to easily enroll and revoke access for an organization's remote workforce almost instantaneously. In addition, the Web portal provides easy-to-follow instructions and training for remote employees.

The Superior Choice: Certificate-Based Authentication

Traditional authentication practices that depend on hardware tokens are especially complex and costly for a growing organization. Issuing certificates for authentication purposes is a flexible solution for any organization and can easily scale to tens of thousands or more employees. The table below compares the costs of token-based and certificate-based authentication structures and the reasons why Trustwave's on-demand, two-factor authentication solution is a more cost-effective alternative:



Costs	Token Based Authentication	Trustwave Authentication Service	Reason for Savings with Trustwave
Up-front implementation	$$$$$	$	• No hardware to purchase • No software to license
Per user	$$$	$	• No hardware manufacturing cost
Hardware and Infrastructure	$$$$	N/A	• No customer infrastructure needed • No hardware needed
On-going maintenance	$$$	$	• No hardware maintenance • No software maintenance • No Certificate Authority audit requirements • Self-service enrollment • No token replacements • Self-service revocations

The managed Trustwave two-factor authentication solution greatly reduces the on-going maintenance and administrative costs of authentication. Additionally, the certificate-based solution demonstrates a compelling Return on Investment (ROI) for any organization. Please contact your Trustwave sales representative for further questions, a demonstration of the technology or a custom price comparison.

Why Certificate-Based Authentication beats Tokens

- Lower total cost of ownership
- Easier to maintain, no replacements
- Leverages existing infrastructure
- Easy to use Web self-service portal

For more information: www.trustwave.com