

DIGIPASS STRONG AUTHENTICATION FOR CHECK POINT CONNECTRA™

By adding DIGIPASS strong authentication to Check Point Connectra™, the customer has an easy-to-deploy remote access solution with enhanced security. Check Point Connectra™ is a remote access gateway which combines SSL VPN, IPSec VPN and intrusion prevention with centralized management and straightforward deployment. VASCO DIGIPASS offers one-time password (OTP) technology to protect user login and ensures that only authenticated users get access. IDENTIKEY, VASCO's authentication server verifies authentication requests on the back-end.

HOW DOES IT WORK?

When remotely connecting to the corporate network via Check Point Connectra™, the end-user is asked for an OTP generated by the VASCO DIGIPASS authenticator. Check Point Connectra™ will communicate with IDENTIKEY Server, VASCO's back-end authentication software, through RADIUS to validate the OTP. Upon successful validation of the OTP, the user is authenticated and Check Point Connectra™ will set up the SSL VPN connection.

BENEFITS

Secure remote access

- Adding two factor authentication to remote access
- Secure access to corporate network assets any time and anywhere
- Prevents unauthorized network access

Seamless integration

- Use of standard RADIUS protocol
- Leverages existing IT infrastructure
- Up and running in no time

Scalable

- More users can simply be added
- Can be reused to secure more/other business applications
- Caters for all your strong authentication needs

Low Total Cost of Ownership

- Little to no cost for user administration and support
- No additional infrastructure investments

Secure your laptop and remote network access with VASCO and Check Point

User-friendly pre-boot encryption and enhanced security for remote access by combining VASCO strong authentication with Check Point

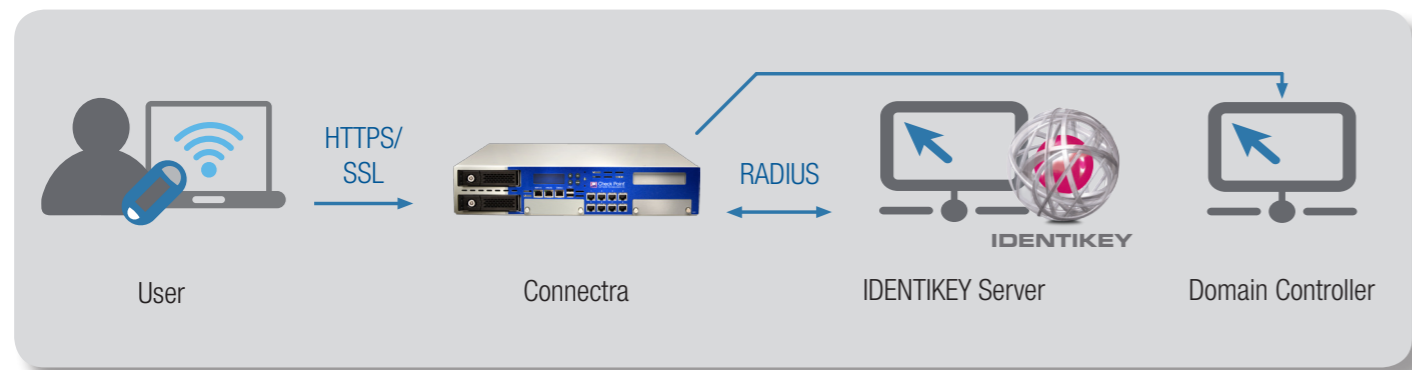
Nowadays when employees use their PC, they want to read e-mail, use software and documents, access files on the corporate network, work with applications and access websites. With the workforce becoming more mobile, the employees want to do all this anywhere and anytime. SSL VPN technology ensures the access to the corporate network. At the same time IT administrators need to make sure that corporate resources are accessed in a secure way while working from home or being on the road.

Furthermore with the workforce becoming mobile, laptops have become standard equipment for travelling staff. Laptops are stored in car trunks, airplane compartments; as a result they are more easily lost or stolen. Next to securing the access from anywhere at any given time, the IT administrators need to ensure that the data stored on the laptop are also secure. As a result they increasingly adopt pre-boot encryption, document and disc encryption.

DIGIPASS strong authentication adds an additional security layer to remote access, preventing unauthorized users to access the corporate network assets. VASCO's PKI-based offering consisting of DIGIPASS CertiID and DIGIPASS Key devices adds an extra encryption layer to laptop access, Windows log-on, document and disc encryption.

VASCO AND CHECK POINT

VASCO's IDENTIKEY, DIGIPASS CertiID and DIGIPASS Key range are Check Point OPSEC certified. OPSEC certification facilitates the bundling of VASCO's solutions with Check Point's product offering. VASCO IDENTIKEY and DIGIPASS can be bundled with Check Point Connectra™ adding strong authentication to your remote access. VASCO DIGIPASS CertiID and the DIGIPASS Key devices can be bundled with Check Point Full Disk Encryption for pre-boot security, Windows log-on, document and disc encryption and with Check Point Endpoint Security to enhance the security of VPN access.



www.vasco.com

CORPORATE HQ
CHICAGO (North America)
 phone: +1 630 932 88 44
 info-usa@vasco.com

INTERNATIONAL HQ
ZURICH (Europe)
 phone: +41 43 555 3500
 email: info_europe@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

	Authentication type					Integration type					DIGIPASS					Documentation		
	Remote	Web	Application	LAN	Preboot & Encryption	DIGIPASS Pack	IDENTIKEY	IDENTIFIER	DIGIPASS Plug-In	DIGIPASS CertiID	DIGIPASS for Mobile	DIGIPASS GO Series	DIGIPASS KEY 200	DIGIPASS KEY 860	DIGIPASS KEY 1	DIGIPASS smart card	Integration Guide	Compatibility Guide
Check Point																		
Check Point Connectra	x					x	x	x	x	x	x	x	x	x	x	x	x	x
Check Point Full Disk Encryption					x			x		x		x	x			x	x	x
Check Point End Point Security	x	x	x	x	x	x	x	x		x		x	x			x	x	x
Checkpoint VPN client	x					x	x	x	x	x	x	x	x	x	x	x	x	x

DIGIPASS CertiID and DIGIPASS KEY for Check Point endpoint security

PKI-BASED SECURE VPN ACCESS FOR CHECK POINT ENDPOINT SECURITY

By adding VASCO CertiID and DIGIPASS Key 200 or DIGIPASS Key 860 to Check Point Endpoint Security™ you can combine pre-boot encryption, certificate based Windows log-on, document and disc encryption with secure VPN access.

Check Point Endpoint Security™ is a single agent that combines all the critical components for total security on the endpoint. Check Point Endpoint Security combines the protection of the endpoint against a rising number of web based threats with a single easy login unlocking all security system on the PC with data security and remote access. VASCO's DIGIPASS CertiID combined with DIGIPASS key offers certificate based strong user authentication to protect user login and ensures that only authenticated users get remote network access.

HOW DOES IT WORK?

When remotely connecting to the corporate network using VPN, the end-user will launch the VPN application on his desktop. This application will request a user login. The end-user will plug his DIGIPASS Key 200 or DIGIPASS Key 860 in the USB port and type his PIN. This PIN will allow for Check Point Endpoint Security to use the PKI-certificate stored on the DIGIPASS Key for VPN authentication. Check Point Endpoint Security also allows to use the same technology for pre-boot encryption, PKI-based Windows log-on, document and disc encryption.

BENEFITS

Secure remote access

- Adding certificate based two-factor authentication to remote access
- Secure access to corporate network assets anytime and anywhere
- Prevents unauthorized network access

Pre-boot encryption, Windows log-on, document and disc encryption

- Adding certificate based two-factor authentication to your laptops
- Prevents data breaches and unauthorized data access
- Enhanced security in case laptops are lost or stolen

Seamless integration

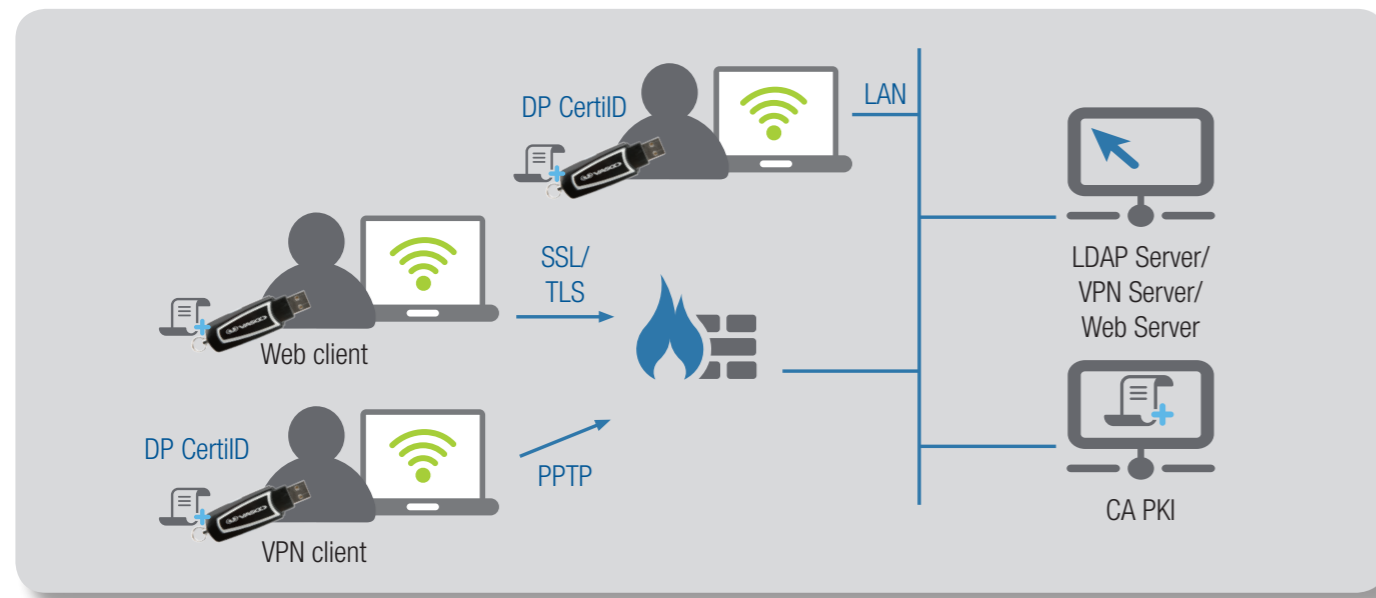
- Leverages existing IT infrastructure
- Up and running in no time
- Allows a transparent migration from OTP to PKI

Scalable

- More users can simply be added
- Can be reused to secure more/other business applications
- Caters for all your strong authentication needs

Low Total Cost of Ownership

- Little to no cost for user administration and support
- No additional infrastructure investments



DIGIPASS CertiID and DIGIPASS KEY for Check Point full disk encryption

PKI-BASED PRE-BOOT ENCRYPTION FOR CHECK POINT FULL DISK ENCRYPTION

By adding VASCO CertiID and DIGIPASS Key 200 or DIGIPASS Key 860 to Check Point Full Disk Encryption, you have a plug & play solution which enhances pre-boot security of laptops which also allows you to use the same solution for Windows log-on, document and disc encryption. It protects corporate information stored on laptops against unauthorized access and it prevents data breaches when laptops are lost or stolen.

Laptops and desktop hard drives are automatically encrypted to protect business critical information and prevent data breaches. Check Point Full Disk Encryption provides the highest level of data security with multi-factor pre-boot authentication and the strongest encryption algorithms. The entire hard drive content is automatically encrypted. By adding VASCO's PKI-based authentication solution, you use certificate based authentication which further enhances the security of laptop to access encrypted business critical information which is easy-to-use.

VASCO's certificate based strong authentication works both when a laptop is connected or unconnected to the corporate network.

HOW DOES IT WORK?

When the end-user starts up the PC, the PC will ask for a pre-boot password. The end-user will plug his DIGIPASS Key 200 or DIGIPASS Key 860 into the USB-port after which the end-user will enter his PIN code. The PIN code allows Check Point Full Disk Encryption to access the certificate stored on the DIGIPASS Key device and use the certificate for authentication. Upon verification, the end-user will be able to access the PC.

Once pre-boot authentication has been done, the end-user still has to perform a Windows log-on, this can be done either by traditional username and password, or he can also use the PKI-certificate on the DIGIPASS Key for Windows log-on. Once logged on, the certificate on the DIGIPASS Key can also be used to access encrypted documents and discs.

BENEFITS

Pre-boot encryption, Windows log-on, document and disc encryption

- Adding certificate based two-factor authentication to your laptops
- Prevents data breaches and unauthorized data access
- Enhanced security in case laptops are lost or stolen

Seamless integration

- Use of standard RADIUS protocol
- Leverages existing IT infrastructure
- Up and running in no time
- Allows a transparent migration from OTP to PKI

Scalable

- More users can simply be added
- Can be reused to secure more/other business applications
- Caters for all your strong authentication needs

Low Total Cost of Ownership

- Little to no cost for user administration and support
- No additional infrastructure investments

