Connect and Manage ANY and ALL IP Device Remotely and Securely with the IPT Security Gateway ONE

IPTECHVIEW™
READY
MxMSP™

Why do I need an IPT-SecGate-ONE? World-class remote service!

The IPT Security Gateway is a hardened professional tool to give your support team secure remote access to off-site equipment and enable full service to all of your equipment in record time. It expands the visibility and access of IPTECHVIEW's remote monitoring and management platform to IP devices on the network including non-supported brands and non-preconfigured solutions.

The device provides access to perform troubleshooting and diagnostics making remote support easy. This eliminates unnecessary truck rolls and provides the capability to remotely monitor equipment and log and share the amount of remote services performed.

Our solution is based on a hardened, fan-less, ruggedized solid-state network device with a redundant power supply that enables the IPTECHVIEW platform to manage all devices inside the LAN. The IPT Security Gate can "Cloudify" anything that has an IP address. The IPT Security Gateway can also be used as a temporary tool for doing initial remote setup on non-IPTechView devices.

The solution is more secure than managing devices inside a corporate network using port forwarding or PCs with remote login capabilities that might be accessed -, unsecured - and will not log nor monitor the network intelligently. The outcome is a secure world-class remote support service.

Why would I want an IPT-SecGate-ONE? Saves time and money!

Without adequate remote oversight, system outages and productivity loss is inevitable.Network security and operational integrity require remote monitoring and management of device health and network traffic. This is difficult to do remotely.

The IPT Security Gateway is Ideal for remote networks with non-native or IPTECHVIEW-supported devices. Setup is as simple as connecting the device to a network port and power. The system literally enables the same full serviceability over a secure remote connection that a qualified onsite technician would have.

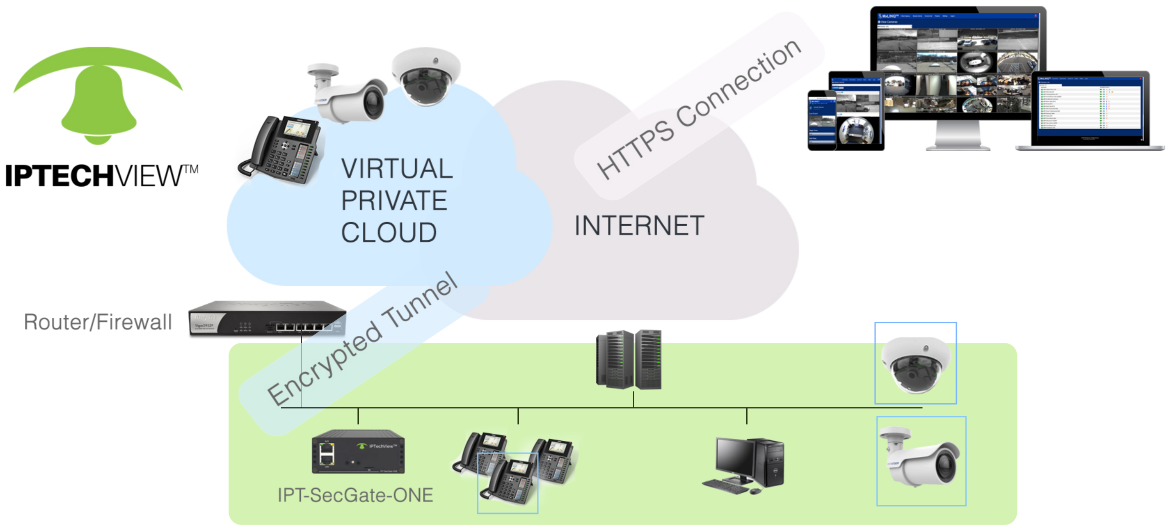
IPTECHVIEW Password Vault technology also enables more secure procedures and centralized management of device passwords. Access to remote systems can be granted to specific users only and two-factor authentication can be enforced to tighten systems monitoring and maintenance security. All access is logged to support time spent servicing a customer and simplify and ensure billing.

What can I used it with?

The IPT Security Gateway can be used with any on-premise device that has an IP address including IP phones, IP cameras, network equipment, printers, PCs - and more - that can be managed over a GUI from a browser.

How does it work?

The IPT Security Gateway is a plug-and-play device that establishes a 256-bit encrypted tunnel with the IPTECHVIEW platform and scans the network for local devices. On setup, the administrator determines what devices should be managed by IPTECHVIEW. The IPT Security Gateway then bridges connections to the specific devices in the LAN. Non-configured devices will remain private and inaccessible. This enables higher privacy and network security than using a local PC. Two Factor Authentication can be enforced.



How much is it? Where can I get it?

In North and South America the MSRP is US $495. For pricing in other countries, contact your local distributor.

Features:

Enables selecting of devices and tunnels and bridges devices within one C-Class and makes them available for management and monitoring by the IPTechView RMM.

Conducts independent local internet speed testing and other network security diagnostics.

Security & Privacy:

Each IPT Security Gateway device is secured with a unique device ID and random device key plus a password created at initial connection. It communicates over an encrypted VPN tunnel exclusively to IPTechView's secure server.

The solution was created with privacy and security in mind from the beginning and as a primary design requirement. Our goal was to combine secure remote access with transparency of what the device can and is doing. Therefore the device can be limited to bridge only the brands selected and also discloses its full functionality. End user IT staff can verify bridged device brands, list of IPs being bridged, device details, and validate functionality activated and the scope of activity of a device by checking on the device dashboard available via a GUI on the local network.

Specifications:

> 1 Gigabit Ethernet LAN Interface, 1 AUX Ethernet interface
> 1 Gbyte SDRAM
> 4 Gbyte MMC FLASH
> Device discovering (up to 253 devices)
> Up to 255 monitored, managed services
> Up to 15 video streaming devices
> Dual Power Input: 5V DC 2 Amp or 100-240 V AC 0.3 Amp
> Power Consumption 2.7W (idle), 6.5W (max)
> Rack-mountable (optional) devices
> Measurements 8" x 4" x 1.6" (20.5 x 10.5 x 4 cm)
> Weight: 1.6 lbs. (570 g)
> Operating temperature: 41°F - 104°F (5°C - 40°C)
> Storage temperature: 41°F - 140°F (5°C - 60°C)
> Non-condensing humidity: 5% - 90%