

ComBrio Virtual Service Infrastructure™

▶ Virtual Service Delivery

- Proactive device monitoring
- On-demand device access
- Increased bandwidth for device service
- Remote on-site appliance reduces network complexity
- Ubiquitous connectivity
- Rapid Deployment

▶ Virtual Service Control

- Centralized access control for all 3rd party vendors
- 3rd party connectivity approval/denial in real time
- Per device policy-based access rights

▶ Increases Security and Compliance

- Outbound initiated connections requiring no open inbound holes in firewall
- End-to-end audit trail for regulatory requirements
- User-defined reports based on device, time and authorization
- Global shutdown for immediate termination of all 3rd party activity
- Utilizes 128 bit SSL and AES standard encryption

ComBrio Virtual Service Infrastructure™ (VSI) is connectivity software for service organizations which provide secure remote device monitoring and management. VSI increases security, enhances regulatory compliance and improves service response times, thereby reducing costs for both the service organization and its enterprise customer.

VSI utilizes a unique outbound connection, ensuring security between the service organization and the enterprise IT organization. VSI is middleware residing between existing network management tools and target devices.

VSI establishes mutual consent between the service organization and its enterprise customer. Utilizing VSI, service organizations can continuously monitor devices and initiate on-demand remote management sessions, while assuring their customers' network is protected from security threats.

ComBrio Virtual Service Infrastructure is comprised of two suites:

VSI Service Delivery



VSI Service Delivery logically extends the physical reach of the service organization's network. Utilizing the Internet, VSI creates a secure infrastructure, removing geographical, physical and technical boundaries between the service organization and the remote sites it supports.

VSI Service Delivery provides:

- Proactive monitoring and 24/7 constant status on any remote device by presenting a virtual view of that device, without a dedicated connection or VPN
- Secure on-demand device management sessions via ComBrio's *Directed Circuit™* technology

VSI Service Control



VSI Service Control enables the enterprise customer to centrally control all 3rd party vendor access in real time, while providing a local audit trail for regulatory compliance.

VSI Service Control provides:

- A single intuitive interface for real time access management of all devices contracted to its service organization(s)
- A local audit trail detailing the activities of all 3rd party service organizations utilizing ComBrio's VSI Service Delivery



VSI Hardware Requirements

VSIadministrator:

Server (minimum requirements):

Type	x86 Based
Processor	3.6 GHZ or higher
Hard Disk Drive	36.4 Gb
Memory	4 Gb

VSImanager:

Server (minimum requirements):

Type	x86 Based
Processor	3.0 GHZ or higher
Hard Disk Drive	36.4 Gb
Memory	2 Gb

VSIenterprise:

Server (minimum requirements):

Type	x86 Based
Processor	3.0 GHZ or higher
Hard Disk Drive	36.4 Gb
Memory	2 Gb

VSIgateway Specifications

Protocols Supported:

Encapsulation	TCP/IP, ICMP, SNMP
---------------	--------------------

Interfaces:

WAN	10/100 auto-sensing
LAN	10/100 auto-sensing

Power Requirements:

Voltage	90 to 264VAC (400) 16 to 24 VDC (401)
Current Draw	1.2 Amps Max

Compliance:

Safety	UL, CSA
Emissions	FCC Class B

Dimensions:

H x W x D	1.7" x 16" x 10" (400) 1.7" x 7" x 9" (401)
Weight	4lbs

ComBrio Virtual Service Infrastructure Features

Management:

- On-demand device connectivity
- Protocol agnostic management tunnels
- E-mail notification for session initiation and termination
- 256 Byte AES encryption

Monitoring:

- Compatible with existing network management tools
- Guaranteed delivery of SNMP traps
- User-defined naming convention
- Devices can be monitored by either IP or DNS name
- 128 Byte SSL encryption

Security and Reporting:

- End-to-end audit trail for regulatory requirements
- NAT transversal for multiple firewalls
- Out-bound initiated connections
- Per session encryption

Policies:

- Automated resolution of IP address overlap
- External and internal authentication and authorization
- Access policies defined on a per device basis
- Each connection is enabled for a one-time only use by a unique set of rules & policies, which are destroyed upon session termination

Provisioning & Deployment:

- Browser-based graphical interfaces
- Rapid deployment and turn-up
- Remote and local administration
- System wide configuration backup and restore
- Scalable to 20,000 devices

For more information visit:
www.combrio.com