IXIA FABRIC CONTROLLER CENTRALIZED MANAGER

DATA SHEET

CENTRALIZED NETWORK MANAGEMENT FOR IXIA VISIBILITY SOLUTIONS

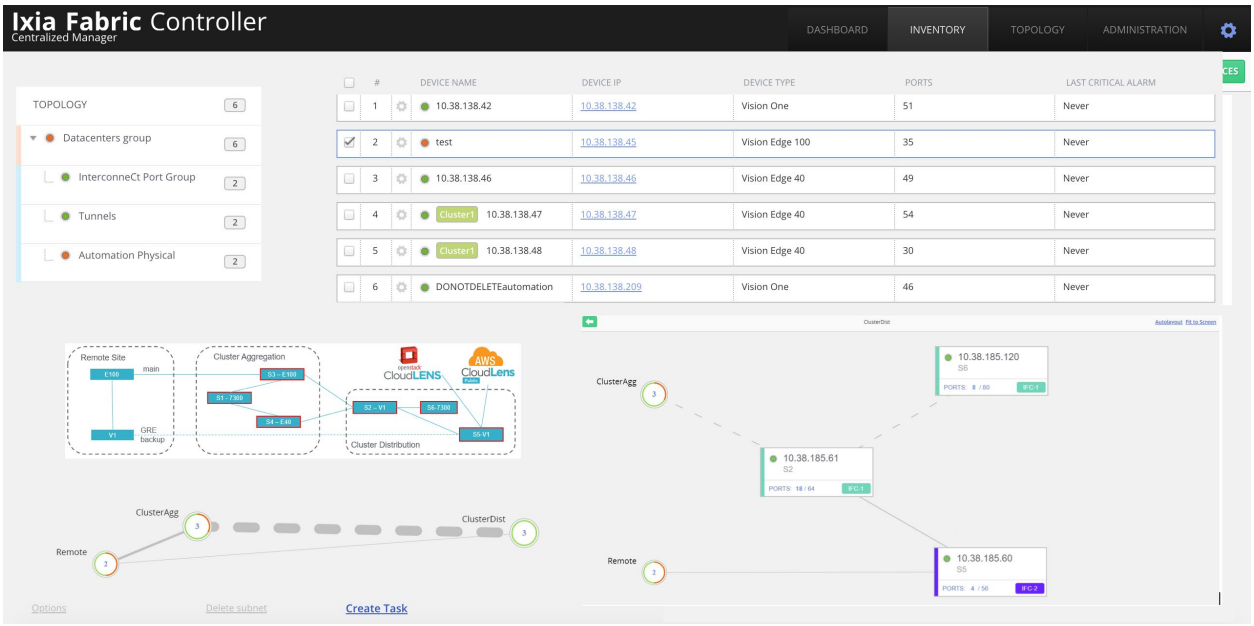
To cope with skyrocketing traffic volume and escalating security threats, today's networks employ sophisticated, pervasive monitoring capabilities. The resulting architecture incorporates dozens – or even hundreds – of taps and bypasses, data monitoring switches, and Network Packet Brokers (NPB), all integrated into a Monitoring Access Platform (MAP) within the network infrastructure. But along with the vital advantages of this architecture comes the challenge of managing these devices for configuration, monitoring, bulk software upgrades, and more.

Now, the IFC Centralized Manager has been enhanced to deliver even more high-performance and efficiency features. IFC CM also offers High Availability (HA) for robust, comprehensive management capabilities and lets you manage a wide deployment of wired, wireless, and/or virtual devices. This versatile platform also allows growing networks to expand their management and planned capabilities to keep pace with increasing needs as devices are added. IFC Centralized Manager eases configuration and monitoring of taps, virtual taps, data monitoring switches, and network packet brokers – turning them all into fully orchestrated and coordinated monitoring resources.

In addition to being a comprehensive Network Management System which provides functions such as periodic device discovery, schedule task batch execution, and complete events and alarms management, IFC CM was recently enhanced to include significant Single Pane of Glass (SPoG) features such as intelligent topology display and navigation, Single Sign On (SSO), zero touch provisioning, and IFC cluster integration.

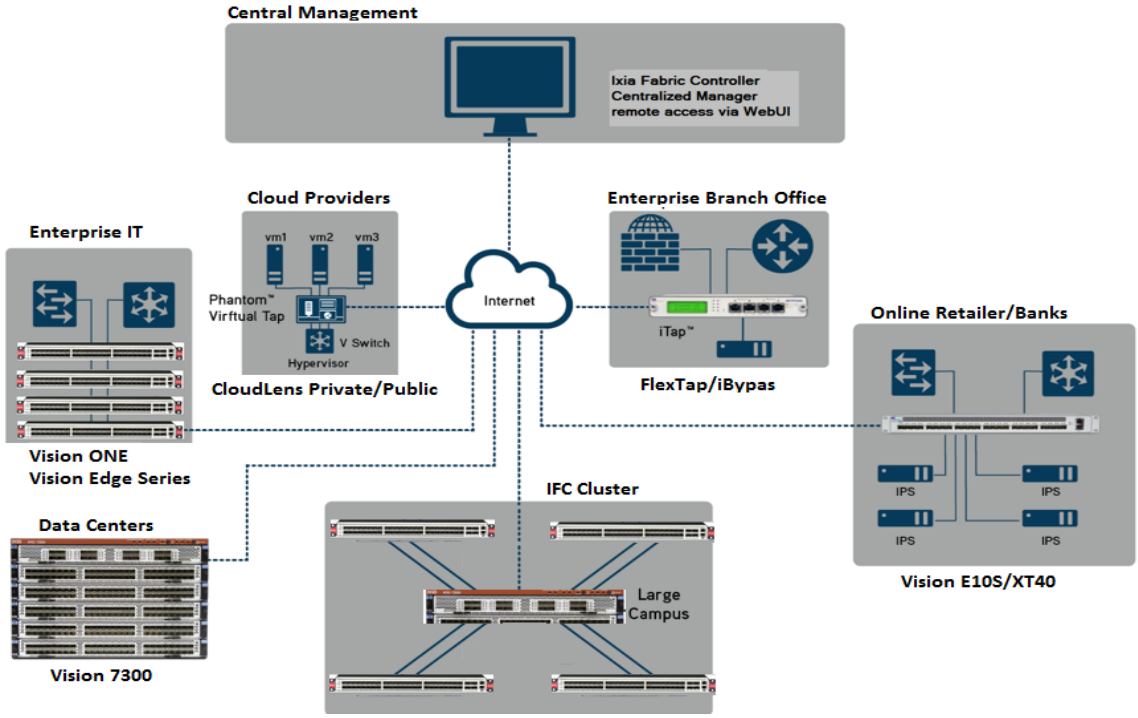
HIGHLIGHTS

- Centralized manager to offer single pane of glass operation for large numbers of managed devices via auto discovery
- Innovative topology visualization with node grouping and interconnect links; and size, color, width all proportional to the actual # of nodes in group, alarms in each group, and physical bandwidth of the link
- Single Sign On (SSO) and zero touch provisioning for discovered Vision devices
- Physical or virtual implementation: support for VMware and KVM
- High Availability (HA) with floating IP between master and slave units
- Master/slave can be cross-form configuration: physical-physical, virtual-physical, and physical-virtual
- Northbound Interface to support fault management with another NMS
- Device configuration and management
- Alarms and events management
- Audit trail
- Scheduler to support software upgrade, script/policy execution, and configuration import/export across many devices
- Event triggered response to execute custom scripts
- At-a-glance dashboard views
- Snapshot and historical data views
- Trap and email forwarding
- Business logic alerts
- Monitors traffic levels and quality across the network
- Expanded RADIUS, TACACS+ and LDAP authentication



IFC CM OFFERS A SINGLE PANE OF GLASS FOR VISIBILITY MANAGEMENT

IFC CM is delivered either as a physical appliance or as a virtual appliance in VMware or Oracle Virtual Box format. As a software solution, IFC CM virtual appliance is available at a significantly lower cost than the physical one. Deployment is amazingly simple too, thanks to a fast, fully automated discovery process that can quickly identify all supported Ixia Vision products, Ixia iTap/iBypass/xStream family of products, and even third- party devices throughout the network. IFC CM also checks continuously for devices being removed or taken offline. It also checks periodically for devices newly added. A dynamic network topology map instantly shows the “up” or “down” status of all supported devices, in addition to custom status based on active alarms (Minor, Major, Critical, SNMP error). Click on a device object/icon to drill down into detailed device status and configuration information, as well as the status of attached links.



RELIABILITY AND SECURITY FEATURES

IFC Centralized Manager offers a spectrum of new features to expand authentication support and more. Your management and administration duties will be easier than ever, thanks to enhanced network visibility and security, plus extended virtual support. The newly enhanced High Availability (HA) feature supports master and slave units in complete sync with one floating IP address; allowing instant takeover by the Slave when the master fails. Best of all, the master and slave units can be either physical or virtual or a combination of both, enabling maximum deployment flexibility.

COMPREHENSIVE CONFIGURATION AND FAULT MANAGEMENT

IFC CM supports a scheduler that allows automated task execution across many devices. Common management tasks include, for example, script and policy execution, software upgrades, configuration import and export, and many more. More sophisticated mechanism is implemented to allow you to execute customer scripts when one or more general events device specific events take place in the entire managed network.

IMPROVED DATA VISUALIZATION

IFC Centralized Manager gathers data in real time from discovered Ixia or third-party devices, archives that data in a database for historical trend analysis, and then presents it in rich graphical formats through a web browser interface. Both IT and business users benefit from the efficiency, accuracy, and cost savings they realize by employing IFC CM to monitor network health and trouble spots. But it doesn't stop there: IFC CM is also a vital resource for growth, capacity planning, and compliance activities.

IFC CM's enriched capabilities include more visibility and presentation options, with an increased number of charts or dashboards per user – and users can now customize their own views of interest. IFC CM will even remember and create a user-specific dashboard upon login to save time and offer up relevant data faster.

Traffic statistics displayed include bandwidth utilization, byte and packet counts, errors, and jumbo frames, all viewable on a device-by-device basis. In addition, a dashboard can be configured to confederate the data from multiple links and devices for an at-a-glance overview of network traffic activity.

SECURITY AND USER MANAGEMENT

The IFC CM platform delivers a total solution to all NMS security-related issues. All user actions are inspected and audited against a permissions profile and logged to an audit trail. The system's security is structured in three layers:

- External authentication via RADIUS and TACACS
- Authenticated and encrypted sessions between the client web browsers and the server throughout a user's entire sessions
- User authentication by a login session based on a user name and password
- Role-based access control and device locking to ensure that a given user can perform certain actions on specific devices with read or write permissions. These are based on a global policy that meets the organization's compliance standards

SPECIFICATIONS

SPECIFICATIONS	
Functional	• Fast, automatic device discovery • Device configuration and fault management • High Availability with master and slave redundancy in physical, virtual, or combined • Innovative topology visualization with color coded node groups and interconnect links of different shapes to reflect physical interconnects, IFC Cluster interconnects, or L2GRE tunnel • Single Sign On and Zero Touch provisioning for discovered Vision devices • LLDP auto discovery and topology display for SPANs, TOOLs, and interconnect links • Data visualization: snapshot and historical, utilization, total bytes, total packets, jumbo packets, CRC errors, dashboard views • Dashboard of graphs • Security: profile-based permissions and views, comprehensive audit trail, and role-based access control • Data export (print, export to CSV file) • Device management (device dependent): port settings, device system settings, device user accounts • Device-dependent event logging and fault management • Scheduler for bulk software upgrade, script and policy execution, and configuration import/export
Virtual and Physical Appliance (Optional)	Virtual Appliance • VMware vSphere 5.x and 6.0 support • CentOS 7 (64-bit) • 2GB RAM • 20GB HDD • 4 CPU Physical appliances • Dell PowerEdge R640 XL Server • 64GB RAM • 640G SSD • Intel Xeon Silver 4110 2.1G, 8C/16T, 9.6GT/s 2UPI

SPECIFICATIONS	
Operating	• Operating Temperature: 10˚C to 35˚C • Storage Temperature: -10˚C to 70˚C • Relative Humidity: 10% min, 90% max, non-condensing
Mechanical	• Dimensions: 1.75” high x 23.5” deep x 19” wide • Mounting: 19” rack mount (1U) • Weight: 26 lbs (11.8kg)
Electrical Specifications	• Power: 100-240 VAC, 47-63Hz 650W PFC • Redundancy: Dual modules • Maintenance: Power supplies are hot-swappable Indicators • Power, disk activity, network 1 activity, network 2 activity, over temperature warning
Certifications	• FCC, CE, VCCI, and C-Tick certified • Fully RoHS and WEEE compliant
Supported Web Browsers	• Internet Explorer, Firefox, Safari, Chrome

SPECIFICATIONS	
Supported Devices	• Ixia Vision ONE, Vision 7300, Vision Edge 40/100/E10S • Ixia NTO ControlTower • Ixia GTP Session Controller • Ixia TradeView • Ixia xStream 40 and xStream 10 • Ixia Director, Ixia Director Pro • Ixia xBalancer • Ixia iTap and iTap2 • Ixia iBypass 1G • Ixia iBypass 10G • Ixia iBypass 3 CU3 • Ixia iBypass HD • Ixia iBypass VHD • Ixia iBypass 40-10 • Ixia iBypass DUO • ISIP1

ORDERING INFORMATION

PART NUMBER	DESCRIPTION
991-0135	Ixia Vision Management Appliance; Support running IFC CM and Hawkeye Manager. Adjunct or separate node license must be purchased.
LIC-VA025-M	IFC Centralized Manager, 25 nodes
LIC-VA050-M	IFC Centralized Manager, 50 nodes
LIC-VA0100-M	IFC Centralized Manager, 100 nodes
LIC-VA0250-M	IFC Centralized Manager, 250 nodes
LIC-VA0500-M	IFC Centralized Manager, 500 nodes

Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info