MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE

Last Modification Date: 08/09/2023
Exported and Shared on: 03/19/2024

For additional information, visit www.intervision.com

CONTENTS

1 MANAGED NETWORK SERVICES OVERVIEW

Managed Network and Monitoring Services provides organizations with the management and monitoring of their network infrastructure, to improve availability, whether the infrastructure is on premises, a third-party datacenter or the cloud. This Service Guide describes Managed Network Services in general (part one) and then describes the specific details of the managed network devices for which this service guide is intended (part two). This document clarifies the scope of the service, service level, roles and responsibilities, and other specifications of the service for customers of this service. This document may get updated from time to time to add additional clarification and details related to this service.

1.1 MANAGED NETWORK SERVICES - GENERAL SERVICE DETAILS

In Scope

- This Managed Service offers management and monitoring of devices and software according to this Service Guide and the InterVision Work Order to aid in resuming normal operations. Additional requests above and beyond will be based upon time and material expense to the Customer.
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions, testing and documenting each fault within the InterVision trouble ticket system
- Ownership of resolution of the problem on behalf of the Customer and act as an agent for the Customer under executed letters of agency
- Notify the Customer of the progress of all faults per Customer provided contact process.
- Critical software and firmware updates.
- Summary reports delivered via our monitoring portal to help the Customer understand traffic, clients and application usage
- Assistance with warranty replacement and vendor escalations.
- Changes to individual devices. Mass additions/deletions or changes (greater than 5) are not covered via the Managed Network Services agreement and will be considered project billable tasks.
- Safeguard customer's proprietary information using commercially reasonable efforts to securely access client network through an encrypted tunnel.
- ***If, during the life cycle of the contract, a device becomes of "Out of Scope / Unsupported", Operational Support will be reduced to the following:
    a. Actions related to Device Failures, including those due to failed recovery during the InterVision execution of Client Approved changes, are limited to:
        i. Device replacement (client provided device or new purchase) with existing configuration included.
        ii. Additional remediation at T&M.
    b. The risks of operating Unsupported Software with known vulnerabilities that cannot be addressed due to the lack of vendor support are considered "Accepted" by the client.
    c. All Operations Center related Incident Remediation efforts are limited to two hours in scope within standard contract language; any additional efforts are subject to T&M.
    d. Hardware Component failures are the responsibility of the client or must be addressed through T&M / Dispatch.
    e. Recurring Alerts for Out of Scope / Unsupported devices with no In Scope resolution paths available will be transitioned to Monitor Only.
    f. Actions requiring a change in code version (requested software enhancements / features that require newer version of code / updates to address vulnerabilities) are the responsibility of the client or must be addressed through T&M / Dispatch.

Out of Scope

- Hardware or Software installation or non-RMA replacement is not included with network support unless specifically stated below. Professional services may be engaged to assist with installation, upgrade or replacement.
- Software license and subscriptions are not included. Management devices and software provided as part of the Managed Service will be licensed.
- Netflow reporting is available as an additional optional paid service. The device to be covered by Netflow must support the application and have the necessary capabilities to provide reporting appropriate to need.
- Mass configuration changes to covered devices that are required, due to Customer upstream or downstream projects, are not covered as part of the service.
- Coverage for devices not under agreement are ineligible for support of any type.

Customer Requirements

To allow for successful monitoring and management of devices and execution of SLAs, Customer responsibilities include:

- Providing all network and device information for the InterVision Managed Services team and tools to discover the contracted devices and enable monitoring. This information includes network diagrams, site information, circuit information and Customer Vendors, Letters of Agency, and current software levels.
- Providing computing resources to run InterVision's monitoring and collection tools, and the means for the Collector to contact the InterVision Data Center.
- Performing configuration of devices and network, as necessary, to facilitate monitoring and management of the contracted devices. In the event the customer is unable or does not have the personnel to enable monitoring and management of devices, InterVision's Professional Services can be engaged for assistance at an incremental cost.
- Provide devices access - Remote access to devices must be available for support. The client is responsible for out of band access, along with in-band access.
- Provide a distribution list of Customer contacts to receive alarm triggered emails and reports
- Supply InterVision team with all the necessary security information including dial-in numbers, access ID's, passwords, SNMP community names necessary for InterVision to perform the Services
- Provide notification contact and escalation lists for use by InterVision during business and non-business hours.
- Provide InterVision team with site contact to facilitate access to equipment and connection terminations, along with out-of-hours access procedures
- Notify InterVision within 72 hours of any changes to the contracted devices via a service/change ticket.
- Execute letters of agency notifying vendors, such as carriers, that InterVision will represent the Customer by isolating and troubleshooting Customer's network problems
- All devices and applications must have vendor support contracts and operate at currently supported vendor versions.
- All devices must be in a supportable state, including current versions of software supported by vendor, with all critical patches applied, in a production capable state with no known failures or functions in order to be covered. Remediation efforts to bring software to current version including patches to make a device production capable will be billable to the customer.

1.2 SERVICE LEVEL OFFERS

- Monitoring Service provides 24/7 monitoring and customer notification. Notification includes automated alerts as well as notification via service personal to client for critical events. This does not include trouble shooting and device support. Support is available for changes to monitoring settings and assistance with reports.
- Standard Service offers 24/7/365 phone and ticket support. it does not include dispatch for onsite support.
- Enhanced Service offers 24/7/365 phone and ticket support. It includes dispatch for onsite support[1, 2] where remote support is unable to fulfill eligible service events such as RMA device replacement.

- Premium Service is available for SD-WAN devices. See Managed SD-WAN Service description and details for additional details

[1] *Applies to devices covered under Managed Network Services in the continental US. International onsite coverage may be added via a custom scope of work.*
[2] *Onsite support is at the discretion of InterVision as determined necessary*

1.3 SUPPORT

Service	Monitor Only	Standard	Enhanced	Premium
Event notification	Included	Included	Included	Included
Phone & Ticket Support 24 hours, 7 days a week	Included for monitoring issues	Included, with SLA	Included, with SLA	Included, with SLA
Onsite Support 7AM-7PM MON-FRI**	Not Included	Not Included, No SLA.	Included, with SLA	Included, with SLA
Onsite Support Off-Hours**	Not Included	Not Included, No SLA	Included, with SLA	Included, with SLA
Phone Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included	Not Included
Onsite Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included	Not Included

* All coverage times are based on the local time zone of the supported device.
** Applies to devices covered under Managed Services in the continental US. International onsite coverage may be added via a custom scope of work.

- In the event that an outage or network problem occurs which is determined to be a site related issue InterVision managed service team will document the Incident within its ticketing system. Examples of site related Incidents are: Loss of power to site, damage to premise cabling, accidental disconnection of site cabling or Equipment.
- In the event that an outage or network problem occurs which is determined to be a Broadband Carrier circuit failure, InterVision will, via a Letter of Agency from Customer, contact the relevant Carrier or ISP and report the Incident for resolution. InterVision will then continue to manage the problem and follow up with the Carrier or ISP to ensure service is restored as quickly as possible.
- In the event that an outage or network problem occurs which is determined to be a failure of CPE, InterVision will diagnose and attempt to resolve the issue remotely. If the outage cannot be resolved remotely, InterVision will escalate to the Customer and/or technician dispatch when needed. Determination of the necessity of on-site services is at the sole discretion of InterVision, If dispatch is requested and cancelled within 48 hours of requested dispatch time, a $500 cancellation fee will be applied.

1.4 REPORTING

For all Managed Network Services, the following reports are available provided quarterly.

- Hardware availability
- Device performance and capacity
- Trouble tickets
- Change tickets
- Monthly overview reports
- SLA reports

1.5 SERVICE ACTIVATION

InterVision employs a structured process to help ensure a smooth transition to Managed Infrastructure and Monitoring services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

Steps to activate service

1. Data gathering
    a. Customer service manual
    b. Order form
2. Monitoring collector/ Support workstation Deployment and Configuration
3. Onboard customer devices
4. Add data from step one into systems
5. Finalize customer onboarding
6. Send any found issues with onboarding for client to review
7. Go Live/ Customer training
8. Perform true up / Project Closeout

1.6 SERVICE DELIVERY - INCIDENT AND DEVICE IMPACT CLASSIFICATION

The Managed Infrastructure and Monitoring service employs a sophisticated algorithm called the Ticket Enrichment Engine that utilizes the severity of the incident, and the business criticality of the device to determine the appropriate priority levels. Devices such as SD-WAN, routers and firewalls are defaulted to classification as critical devices, and are automatically prioritized higher than other devices. Customers are able to designate other devices as critical, to decrease/increase their prioritization based upon their business impact

Severity 1	No Ticket	
Severity 2	No Ticket	
Severity 3	No Ticket	
Severity 4	Notification Ticket Closed State	
Severity 5	Notification Ticket Closed State	Upgrade Eligible

InterVision

Severity 6	P3 Ticket	
Severity 7	P3 Ticket	Upgrade Eligible
Severity 8	P2 Ticket	
Severity 9	P2 Ticket	Upgrade Eligible
Severity 10	P1 Ticket	

Emergency (P1 or P2) services require a phone call to create an incident.

2 SERVICE SPECIFICATIONS - MANAGED ROUTER AND SWITCHES

The Managed Network Services service for routers and switches covers the availability and performance monitoring of the covered devices performing the data packet forwarding function for an organization.

This managed service is based upon each instance of a physical or virtual router, switch, or supported policy management device.

- Chassis based switches are charged based upon the number of blades within each chassis
- Stacked switches are charged for each individual member switch in the stack.
- As the number of routers or switches increase, fees for this service may increase.
- This is a managed service for client owned equipment.
- Only Essential level monitoring, break/fix support, and vendor escalation is available for supported policy management devices.
- **SD-WAN technology support not included in standard service coverage. See Managed SD-WAN Service Guide.**

This service falls under the Managed Network Service scope detailed in the Service Description above.

For a list of supported devices, please contact your account representative.

2.1 ROLES AND RESPONSIBILITIES MATRIX

	Client	Hosted Cafe'	Extended Services*
General			
Router/Switch information (account. password, location, MAC address,…)	X		
Router/Switch SNMP string	X		

	Client	Hosted Cafe'	Extended Services*
Client escalation information	X		
Vendor support contracts	X		
Installation and Configuration			
Initial design and configuration of router and WAN/LAN	X		X
Physical or virtual router/switch install	X		X
Switch Port Configuration		X	
Implement Quality of Service (QOS)	X		X
Monitoring			
Provide Circuit bandwidth information	X		
Setup monitoring and logging		X	
Update monitoring thresholds per client requirements		X	
Manage notification profiles		X	
Setup dashboard in Managed Network Services portal		X	
Reports setup		X	
Incident and Problem Management			
Incident management		X	
Root cause analysis		X	
Vendor management (Escalations, RMA,...)		X	

	Client	Hosted Cafe'	Extended Services*
Troubleshoot down router/switch		X	
Troubleshoot circuits		X	
Troubleshoot NAT and port forwarding rules		X	
Troubleshoot remote access vpn (IPSEC/ SSL)		X	
Troubleshoot High Availability Features for Routers		X	
Patch Management			
Firmware updates (to resolve issues)		X	
Critical Security vulnerability patching (as required)		X	
Software – minor feature releases, non-critical patches	X		X
Software - major upgrades	X		X
Management			
Administer device accounts		X	
Administer user access	X		
Change Management			
Log and store changes information via backup of config (Cisco/Juniper Devices only)		X	
HW physical replacement (Enhanced Only)		X	

	Client	Hosted Cafe'	Extended Services*
HW replacement configuration migration to new device (if compatible with config backup)		X	X
Create new vLANs or Gateways	X		X
Extend existing vLAN		X	
Create new authentication methods	X		X
Create new remote access vpn (IPSEC/SSL)		X	
Create new site to site vpn	X		X
Create and Implement High Availability Features	X		X
Create Access Control Lists	X		X
Implement or extend existing ACL		X	
Performance Tuning and Management	X		X
Capacity Analysis			
Performance Tuning and Management	X		X
Capacity Analysis	X		X
Life Cycle Management Notification (EOL, EOS)	X		
Reporting			
Standard Reports		X	
Custom Operations Reports	X		X

*Extended services are optional services that can be provided with incremental fees. These service may be additional managed or extended services.

2.2 MONITORING

Managed Network Services for Routers and Switches will monitor the following:

Monitor	Trap Freq	Threshold	Severity
Device Down- Not Responding to ICMP Pings (NT)	5 pings every 2 minutes	80% for 240 seconds	10
Network Memory Critical	3- minutes	85%	9
Critical Network Device Interface Staying Down	1-minutes	5 minutes	9
Network CPU Critical (NT)	3-minutes	90% for 600 seconds	7
Critical Interface- High Utilization (NT)	1-minutes	85% for 600 seconds	7
Network Memory Warning	3-minutes	50-84% for 600 seconds	5
Network Interface Error Critical (NT)	1-minutes	510% for 600 seconds	5
Dropped Pings- Not Responding to ICMP Pings (NT)	5 pings every 2 minutes	100% for 120 seconds	2
Network CPU Warning (NT)	3-minutes	75-89% for 600 seconds	1

Refer to the service delivery section for description of severity levels and mapping to operations center priority levels. (ex. Severity 10 is our highest severity and maps to our Priority 1 service level.)

- Monitoring routing protocol peers is optional and not configured by default.
- Monitor the routing protocol is only over a reliable network.

Reliable Definition – A reliable network is one that is backed by carrier SLA's that include at least five 9's of uptime and less than .5% of packet loss, and less than 70ms of latency across the network. These are typically private networks that consist of MPLS, Ethernet, or Private Lines. Any type of cable modem, DSL, cellular wireless and some fixed wireless networks or Internet VPN networks would not be considered reliable.

Reliability and Monitoring Disclaimer

InterVision

If a monitored customer network becomes unreliable and falls in the category of fixed wireless or Internet VPN, Hosted Cafe' has the right to discontinue monitoring of the routing protocol peers until such time the network is deemed reliable again.

- If a backup link is present on a router and is considered an "unreliable network" and routing protocol monitoring of the primary circuit is required and uses BGP then; 1) the BGP peer must be the interface IP of the primary circuit, and 2) the backup circuit cannot use BGP and must use EIGRP or OSPF.

2.3 SUPPORT FOR ATTACHED CELLULAR WAN EXTENDER DEVICES

Essential level service is available for supported Network Attached Cellular WAN Extender devices. In order to be eligible for full support, the next hop LAN device (router/firewall/SDWAN) must also fall under an Essential or Premium support contract. If the next hop LAN device is not covered, support for the Cellular WAN Extender device will be reduced to Monitor Only support.

Managed Cellular WAN Extender Responsibility Matrix	Client	InterVision Managed Service	InterVision Professional Services
Initial device install and setup	X		
Provide access and monitoring information	X		
Provide vendor and carrier contract and contact information	X		
Setup availability monitoring		X	
Incident management		X	
Root cause analysis		X	
Vendor management (Escalations, RMA,...)		X	
Device break/fix troubleshooting		X	
Carrier contact and escalation		X	
Ownership and provisioning of carrier SIM cards	X		X

Managed Cellular WAN Extender Responsibility Matrix	Client	InterVision Managed Service	InterVision Professional Services
Dispatch to install RMAed device or replacement SIM card (only available if the covered next hop LAN device has dispatch support)		X	
Software updates to resolve break/fix incidents		X	
Non-break/fix related software updates	X		X
Extender device configuration	X		X

2.4 DEFINITIONS

Enhanced- Hosted Cafe' will place the Customer premise equipment ("CPE"), Cloud Services, and Software under support and monitoring service. With this version of the Service the customer receives both unlimited phone support and onsite support as detailed in an applicable Service Order.

Hosted Cafe' - Hosted Cafe is a name for the InterVision managed services organizaiton and team. It is used to differentiate the services from other services such as professional services or Customer IT operations.

Monitor only- Hosted Cafe' will place the Customer premise equipment ("CPE") under support and monitoring only service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order . There is no phone support or onsite support with this service.

RMA - Return Merchadise Authorizaiton. This refers to like-for-like device replacement under vendor warrenty.

Standard- Hosted Cafe' will place the Customer premise equipment ("CPE"), Cloud Services, and Software under support and monitoring service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order and includes unlimited phone support.

©2020 Intervision. InterVision reserves the right to update this document at any time for any reason. The services and capabilities in this document may change without notice.