Service Description
Infrastructure Management

Table of Contents

1.Introduction

CDI's Managed Services for infrastructure is designed to provide Clients with a comprehensive suite of 24 x 7 monitoring, maintenance and administration services.

2. Services Elements

MANAGE: A comprehensive and full set of managed services along with NOC staff that covers all aspects of management and administrative activities. Scope includes monitoring, alerting, full problem troubleshooting and remediation.
AID: A reduced level of managed services where NOC staff perform monitoring, alerting, and SOP (Standard Operating Procedures) based remediation of standard issues. Be notified of issues in your environment through both proactive and reactive alert mechanisms.
SmartEscalate: The next lower level of managed services is a combination of monitoring and escalation services and Self-Service options. Comprehensive checks for your environment are performed by the NOC staff, who verify, validate and triage alerts, and escalate issues to you, a service provider (SP).

Scope Of Services and Technology Offered	Manage	AID	SmartEscalate
ITOP Platform (Monitoring, Management, Tickets, Session Recordings, Remote Console, Reports, etc.,) Executive Dashboard (Web Portal), On-Demand, Weekly & Monthly Reports	CDI	CDI	CDI
24 X 7 Monitoring, Alert filtering, & Alert Priority from ISO27001 Certified NOC	CDI	CDI	CDI
Alert Validations using Run Book Automations (RBA)	CDI	CDI	CDI
Alert & Incident Prioritization With Multi-level Escalations	CDI	CDI	CDI
Bundled Antivirus : VIPRE Business Premium Edition [2]	CDI	CDI	CDI
Patch Rating Service, Patch Failure Alerts [2]	CDI	CDI	CDI
Patch Installations & Antivirus Definition Updates For Supported Antivirus Products	CDI	CDI	Client
Standard Operating Procedures (SOPs) Based Initial Remediation	CDI	CDI	Client
Troubleshooting And Full Remediation	CDI	Client	Client
3rd Party Vendor Escalations for Further Troubleshooting And Full Resolution Of Configuration Issues	CDI	Client	Client
Root Cause Analysis Of Critical Issues	CDI	Client	Client
Move, Add And Changes (MACs)	CDI	Client	Client

Run book Automations (RBA): Automated alert filtering and validations using script framework.

---

[2] Available only for windows servers

Customer must have valid maintenance or technical contract from vendor for network devices, Microsoft, non-Microsoft or 3rd party applications, and anti-virus products. Expiration of maintenance or technical support agreements places limits on MANAGE services. Software & hardware placed into 'End of Life' by vendor will be restricted to AID service only.

Any items not explicitly covered within this document are considered out of scope. We will review new requests or questions received from customers and add clarifications or define the items explicitly in the SOS documents.

3.Scope of Services

This document specifies the scope and schedule of the services delivered within the **Managed Services** agreement.

3.1. Supported Devices

IT Infrastructure	Supported Technology
Server Operating Systems	Windows: Windows Server 2003 and upwards Linux: Centos/ Redhat 5.3 & above, and Ubuntu 10.0 & above
Infrastructure Applications	File & Print, DNS, DHCP, Domain Controller(Active Directory), Email (Microsoft Exchange), Mobile (BlackBerry Enterprise Server), Virtual Hosts(VMware, Citrix Xen, Hyper-V), and Terminal Services/Remote Desktop Services
Backup Applications (if purchased separately)	Symantec, NT Backup, CA ARCserve, Vaultlogix, Acronis, Datto G Series and Veeam
Antivirus Products	Symantec, McAfee, Trend Micro, VIPRE Business Premium, Kaspersky, ESET NOD32, and Microsoft Security Essentials
Bundled Anti-virus	VIPRE Business Premium
Switches	LAN Switches – Core, Service Provider Switches - Aggregation
Routers	Branch Routers / Service Provider Edge Routers
Firewalls	Network Security
WAP	Wireless Access points & Controllers
EMC Storage	EMC CLARiiON, EMC Celerra, EMC VNX/VNXe

3.2. Key Monitoring Parameters

CDI monitors the customer's infrastructure using standard Windows WMI or SNMP data collection.

Operating Systems

WINDOWS OPERATING SYSTEM
Device Availability: Up/Down
Device Health: (CPU, Memory and Disk Utilization)
Windows Services: Up/Down (Default: All services with start-up type "Automatic")
Windows Event Logs: Critical Application, System Logs
Server Hardware Monitoring: Disk, Memory Modules, Chassis Temperature

LINUX OPERATING SYSTEM
Device Availability: Up/Down
Device Health: (CPU, Memory and Disk Utilization)
Linux Interfaces: Up/Down
Logs: Critical Logs
Server Hardware Monitoring: Disk, Memory Modules, Chassis Temperature

Blackberry Server

BES SRP Connection State
besSysHealthSrpConnectedState,besSysHealthSrpLastConnectDate, besSysHealthSrpReconnectSuccess, besSysHealthSrpReconnectsFail, besSysHealthSrpTotalSecNotConnected, besSysHealthSrpLastErrorText, besSysHealthSrpLastErrorTime

Active Directory

Active Directory - NTDS
DRA - DRA Inbound Bytes Total/Sec, DRA Inbound Object Updates Remaining in Packet, DRA Inbound Objects Applied/sec, DRA Outbound Bytes Total/sec, DRA Outbound Objects/sec, DRA Pending Replication Synchronizations
DS - DS Client Binds/sec, DS Directory Reads/sec, DS Directory Writes/sec, DS Server Binds/sec
LDAP - LDAP Bind Time, LDAP Client Sessions, LDAP Searches/sec, LDAP UDP operations/sec, LDAP Writes/sec, Kerberos Authentications, NTLM Authentications

Microsoft Exchange

Performance counters for database disks
Logical Disk(*)\Avg. Disk sec/Read & Write, Physical Disk(*)\Avg. Disk sec/Read & Write
Information Store RPC Processing Counters
MSExchangeIS\RPC Requests, MSExchangeIS\RPC Averaged Latency, MSExchangeIS\RPC Operations/sec, MSExchangeIS\RPC Num. of Slow Packets, MSExchangeIS Client (*)\RPC Average Latency
Message Queuing Counters
MSExchangeIS Mailbox(_Total)\Messages Queued for Submission, MSExchangeIS Public(_Total)\Messages Queued for Submission
Transport Queue Length Counters

Blackberry Messaging
Messages Error/Pending/Expired

Terminal Service Performance Counters
Windows Server 2003: Terminal Services\Active Sessions\Inactive Sessions\Total Sessions, **Terminal Services Session**\%Processor Time (All Instances)\ Pool Nonpaged Bytes (All Instances) \Pool Paged Bytes (All Instances)
Windows Server 2008 onwards: Terminal Service Gateway \Current Connections \Failed Connection Authorization \Failed connections

\MSExchangeTransport Queues(_total)\Aggregate Delivery Queue Length (All Queues), \MSExchangeTransport Queues(_total) \Active Remote Delivery Queue Length, \MSExchangeTransport Queues(_total)\Active Mailbox Delivery Queue Length, \MSExchangeTransport Queues(_total) \Submission, \MSExchangeTransport Queues(_total) \Largest Delivery Queue Length

Outlook Web access Counters
MS Exchange OWA\Average Response Time, MS Exchange OWA\Average Search Time

SWITCHES, ROUTERS & FIREWALL
Device Availability: Up/Down
Device Health: (CPU and Memory utilization)
Interface Status: Up/Down
Interface Performance: – Utilization, In/Out Traffic Rate
Interface Errors: Error and Discard Rate, CRC and Collision Errors
Buffer Usage – Small, Medium, Large and Huger Buffer Utilization and Failures
VPN – IKE and IPsec Tunnel Availability
Hardware Monitoring: Disk, Memory Modules, Chassis Temperature, Fan, Power, and Voltage Status

STORAGE SYSTEM
Device Availability: Up/Down
Device Health: (CPU, Memory and Disk Utilization)
Event Logs: Critical application, System Logs
Hardware Monitoring
Disk, Memory Modules, Chassis Temperature
Storage RAID Monitoring - SAN
Inventory – Storage Processors, Front end (FC, Gb) Ports, Back End (FC,SAS) Ports, Disk Drives
Configuration Details – LUN details, Raid Groups, Host-Port Mappings
Availability – SP Status, SP Port Status, FC/Gb/SAS Ports Status, Disk Drive Status, LUN Status and Raid Group Status
Performance – Array, Device Drive, LUN, Storage Pool and Storage Volume Statistics

SAN Switch Monitoring
Inventory – Fabric Switch and Port Details
Interface – Bandwidth Utilization, Error Rate, In/Out Traffic, In/Out Utilization, Discard Rate
Status – Fabric Switch Status, Switch Port Status
Storage Controller Processors, Storage Controller Cache Memory, Storage Controller & Disk Drive Cabinet Power Supply & Fans, Storage Ports (Storage Controller / Disk Drive Cabinets), Disk Drives, LUNs
Storage RAID Monitoring - NAS
Latency Statistic Per Protocol - Average latency for NFS v3 and CIFS Operations, Average latency for iSCSI read/write, FCP read/write and NFS v3 read/write Operations
Disk – Average, Read, Write Volume Latency, Total, Read and Write Volume OPS, Total, Read and Write Aggregates, Aggregates CP Reads, Disk read/write Throughput
CPU – CPU Utilization, CPU Count
Network – Send/Receive Throughput, Send/Receive Packet Rate, Error rate, Packet Drop rate, Read/Write ops per sec

3.3. Standard Operating Procedures (SOPs)

MANAGE and ***AID*** level services supports execution of pre-defined SOPs. This means that the SOPs are executed when an alert is triggered for the issue on your infrastructure.

- Incoming alerts will be initially validated to identify false alerts or alerts where no action is required
- Actionable alerts will be ticketed by the NOC engineer and any documented Standard Operating Procedure (SOP) will be executed as first level of support

- In case of ***MANAGE***: If the SOPs fail to resolve the problem, the ticket will be updated and immediately escalated to a designated customer contact and to the next level of NOC technicians for further ***troubleshooting and remediation***
- In case of ***AID***: If the SOPs fail to resolve the problem, the ticket will be updated and immediately escalated to a designated customer contact for further troubleshooting and remediation

List of SOPs executed: Examples: List of Operating System and application SOPs executed by CDI.

Servers

Windows Server Status (Up/Down)	Operating System	CDI runs diagnostics to check the status of the problematic Windows server from other server in the same network to eliminate any LAN/WAN connectivity issues
Server shutdown (Unexpected) Alerts	Operating System	CDI will validate the event logs to identify if the sever shutdown is unexpected
Server in Hung State	Operating System	CDI will restart the server if it is hung (through DRAC / ILO)
Memory Utilization Alert	Operating System	CDI will validate the high utilization, and identify the process causing high memory utilization
Processor Utilization Alert	Operating System	CDI will validate the high utilization, and identify the process causing high memory utilization
Disk Space Alert	Operating System	CDI will validating the alert by logging into the server and identifying the folders which are occupying high disk space, run disk clean-up to free-up disk space and notify the customer of folders occupying high disk space
Hardware Error	Operating System	CDI will run hardware diagnostic check to validate the hardware fault.
Windows Event Log (critical)	Operating System	CDI will execute set of instructions when specific critical event occurs
RPC Server Problems (Replication, Win login, Trust relationships)	Active Directory	CDI will check the replication status, run SOP to initiate the failed replication
Fixing errors with Sysvol	Active Directory	CDI will identify the Sysvol errors and execute SOP for first-level resolution
Domain controllers not advertising itself	Active Directory	CDI will identify the errors and execute SOP for first-level level resolution
Object Name Conflicts	Active Directory	CDI will Identify the Object conflict and run SOP to resolve.
Mail Flow (Queue Management) in Exchange	MS Exchange	CDI will checking the mail queue, update the customer, and take further action based on customer update
Mail Client Login Issues	MS Exchange	CDI will check if the IIS is running and able to resolve client URL internally to identify if it's an internal or external issue. Run appropriate SOP as first level resolution
Mail Certificate Expire Issues	MS Exchange	CDI will run SOP to verify the certificate validity and any possible issues based on the alert received
Exchange Information Store Status	MS Exchange	CDI will check the status of Information store based on the alert received. Run SOPs to start the IS service
Licenses issue	Terminal Server	CDI will verify if the enough TS licenses are available and configured
Terminal Server Services not running	Terminal Server	CDI will validate the services which are not running and starting them if required
User Profile issue	Terminal Server	CDI will verify the user profile and profile registry

Network Devices

Switch/Router/Firewall	Device Status (Up/Down) critical alerts	CDI will run diagnostics to check the status of the problematic device from other devices in the same network to eliminate any LAN/WAN issues.
Switch/Router/Firewall	Memory , Processor, Buffer Utilization High on any network device	CDI will validate the utilization by logging into the device; identify the reason for high utilization.
Switch/Router/Firewall	Inbound/Outbound errors on the interfaces.	CDI will check the errors on the interfaces and clears the errors. If the errors persist on the WAN link at the same rate. CDI will check the physical connectivity issue then escalates to the ISP.
Switch/Router/Firewall	Interfaces/Link down	CDI will Log on to the device and check if the interface is "admin down" or "protocol down". In case of Admin down, alert the customer and if "Line protocol down", check the logs to see if the issue is due to network flap.
Router/Firewall	VPN tunnels(Mainly for firewalls nonetheless can be applied for Routers)	CDI will check the tunnel status and find the reason if the tunnel goes down.

Storage

Storage Status (Up/Down)	CDI will check and validate Up/Down status of the Storage Devices. If the device offline is due to hardware failure or malfunction, CDI will collect diagnostic logs and tests will be performed for the problematic storage devices, with the help of Storage Vendor and after the approval of the Customer. Health Check will be performed for Storage Devices which are alerted but not down All these tasks will either be performed from the Storage Console or Management Station
Shutdown (Unexpected)	CDI will validate the logs to identify if the sever shutdown is unexpected
Server in Hung State	CDI will try to gather diagnostics logs or system logs if it is permissible for Non responding or hung Storage devices, perform initial analysis and further follow up with the Storage Vendor to analyze, isolate and bring back the server online. These tasks can be performed either from the Storage Console or the Management Station
Memory Utilization Alert	CDI will validate the high utilization, and identify the process causing high memory utilization
Processor Utilization Alert	CDI will validate the high utilization, and identify the process causing high processor utilization
Disk Space Alert	CDI will validate the alert by logging into the server and identifying the Lun's/folders which are occupying high disk space, run SOP to free-up disk space and notify the customer
Backup Job Monitoring	CDI will validate the backup jobs for job failures and restart the backup jobs if sufficient time is available to complete the job
Hardware Error	CDI will identify and validate the hardware faults. Defective hardware parts replacement for will be followed by with the vendor
RAID Failures	CDI will execute SOPS to identify RAID failures, which will aid in troubleshooting the issue for Storage disk access or performance.
Rebuilding Failed Disks	CDI will execute SOPS to monitor the failed disks rebuild process and ensure normalcy is restored
LUN Connectivity/Access Issues	CDI will execute SOPS to Identify the LUN access and connectivity issues
NFS/CISF Mount Lost	CDI will execute SOPS to identify the NFS/CIFS mount issues due to host, network or Storage issues
Smart Thermal Shutdown	CDI will execute SOP to enable and disable smart thermal shutdown
Controller Issues	CDI will validate controller tasks such as rescan controller and set reconstruct rate
LUN Backup Failed	CDI will execute SOPS to validate the LUN backup failures and provide remedy
Storage Port Availability Issues	CDI will execute SOPS to monitor the Storage ports availability and traffic

3.4. Troubleshooting and Full Remediation

For **MANAGE**, CDI's NOC will remotely troubleshoot and fix issues for alerts that are generated from the existing configuration of your network infrastructure. Following are some of the tasks and activities performed:

- If the SOPs fail to resolve the problem, then the ticket will be updated and immediately escalated to the domain expert within the NOC team to troubleshoot the issue and remediate it in a comprehensive fashion
- If the problem involves a 3rd party vendor for any configuration issues with the applications and operating systems, then the CDI NOC will contact the vendor technical support for further troubleshooting and full remediation
- Root cause analysis of critical (P0) incidents are performed to identify underlying problem
- If an incident is raised, then the CDI NOC will fix it within the predefined SLO
- If a remediation activity is performed, then it is logged into an ITIL based ticketing system and the ticket is updated with its complete chronology as well as the steps taken to remediate the incident

3.5. 3rd Party Vendor Escalations

3rd party vendor support is limited to application and operation system configuration issues.

If the CDI Services team determines a configuration issue that relates to a 3rd party vendor, then CDI will contact the vendor's technical support team to resolve any configuration issues with the applications and operating systems. Under these conditions the following requirements take effect:

- The CDI SLO may be impacted by the terms of the SLO and contract that the customer has with the vendor's technical support organization
- CDI recommends that the customer maintain valid support contracts for the entire infrastructure managed by CDI
- CDI requires that the customer authorize CDI to act on their behalf when it interacts with the vendor tech support organization

3.5.1. ISP Vendor Escalations and Follow-ups

CDI will drive ISP vendor escalations for internet, leased lines, or MPLS circuits for the following events (a) link down (b) high latency (c) high interface errors. CDI will create a ticket and escalate the issue according to the escalation matrix provided in the portal.

Deliverables:

To deliver the SLOs, CDI will follow the process defined below as part of CDI delivery model:

- CDI will monitor WAN connectivity and if there is a problem CDI will contact the ISP or create online ticket or both.
- All ISP related issues, such as, internet or WAN links down will be escalated to the ISP either by phone call or online ticket or both. CDI will also escalate the issue to the customer following the standard escalation process
- Summary of conversations with the ISP will be updated in the ticket
- CDI recommends the customer or customer to maintain valid support contracts with all ISPs they use
- It is required that the customer and/or customer authorize CDI to act on their behalf during any escalation with the ISP
- The response and resolution SLOs of CDI for any issue escalated by CDI to the ISP is now dependent on the response and resolution SLOs provided by the ISP. As a result, the response and resolution SLOs of CDI may be impacted negatively for this issue if the ISP is not responsive.

3.6. Configuration Backup Of Network Devices

For **MANAGE**, configurations of network devices are periodically backed up. CDI performs a backup of the network device configuration every 15 days. The configuration backup will be stored in the cloud and managed by the CDI ITOP Platform.

NOTE: Configuration backup is an automated process and is supported on only selected device types. If an automated process is not supported by the device, then CDI will not be able to backup network device configuration.

Deliverables:

- If the backup configuration event triggers other issues on the device, then the CDI team will be engaged to resolve the issue if it is within the scope of the defined SLO

3.7. Administrative Activities

For MANAGE, the CDI NOC team will perform administrative activities as part of the Move, Add and Changes (MACs).

3.7.1. Move, Add and Changes (MACs)

Included MACs are those that can be done remotely, are administrative, and do not require design services or service disruption to implement
Client can create a ticket and assign it to the NOC for executing MAC requests similar to those shown below:

- User ID Creation/deletion in Active Directory
- Creating / Disabling/Deleting DLs/Groups
- Adding/removing the users to the different DLs
- User mailbox creation/deletion in Exchange per request from customer
- Password Change
- Create\Delete BlackBerry user account
- Erase a Blackberry device, Move users to different BlackBerry Server in same BB Domain
- Adding / Removing Users in local groups on Terminal server
- VPN user MAC requests
- Existing VPN Tunnel parameter tuning
- SSID changes on WAP device

3.8. Preventive Maintenance

The following preventive maintenance activities are done on a scheduled basis:

3.8.1. Windows Patch Management

CDI's service includes the scanning of servers for missing patches every Wednesday and the publishing of the results of the patch scan and actions to be taken for approval in the portal.

- If installation of the patch fails, CDI will take corrective action and the failed patches will be re-installed during the next scheduled patch maintenance schedule approved by the customer
- Windows patches on servers have to be approved by the customer
- The installation of security patches on servers that have been approved will be scheduled as defined by the customer
- Windows security patches and critical only patches are tested by CDI using known IT standard best practices – CDI then rates the patches as Whitelisted or Blacklisted.

Supported Operating Systems and Applications

Operating Systems Windows, Linux	Windows Server 2003 and upwards
Application *(Default)*	MS Office
Application *(On Request)*	Active Directory, Microsoft Exchange Blackberry, Virtual Hosts(VMware, Xen Server and Hyper-V), Backup application, webservers, Citrix, MS SQL, and Microsoft SharePoint

Patch Configuration and Policy

Default patch approval configuration	Manual Approve for Servers Auto Approve: Optional (Customer choice)
How does "Auto patch Approval" works?	▸ "Auto approve" policy in the portal will approve Security and Critical Operating System patches only ▸ Customer can approve application patches from the Portal

Sanity Checks (Servers Only): After Windows Patch Installation and Server Reboot

CDI conducts sanity checks on Windows servers after a patch installation and server reboot. Sanity checks include the following:

- Windows services: Check for services where "Start-up" type is "Automatic" and "Status" is "Started". CDI will re-start the Windows service if "Start-up" type is "Automatic" and "Status" is "Stopped".
- Event logs: Application and system event logs that show "Severity Level" as "Error" will be checked

Note:

- *Default Windows patch management includes installation of security patches and critical patches. It is the responsibility of the customer to hold a genuine Windows license for the server.*
- *It is important to note that a device will be rebooted following any patch installation that requires rebooting. Therefore, customer's approval of the patching time window should take into consideration the possibility of a device reboot.*
- ***Windows Patch Testing:** Windows security patches are tested by CDI using known IT standard best practices. Windows security patches released by Microsoft are first installed in a restricted test environment (that supports standard applications & tools). It is then tested for installation issues, standard application compatibility, and malfunction. CDI personnel will also periodically review forums on patch testing to understand other known issues. CDI testing procedures are best effort in a limited testing environment. After installation of whitelisted Windows security and critical patches, CDI does not accept any liability resulting from crashes or malfunction of devices and applications, should they occur.*

3.8.2. Antivirus Definition Updates

This activity includes checking the anti-virus definitions on the windows server and updates to those definitions on a scheduled basis. Additionally, the following is done:

- Anti-virus or anti-malware definitions will be updated on a daily basis by default
- The customer will be alerted if any major issue such as corruption or license expiry is observed either with the anti-virus or anti-malware application or with its definition update
- If the anti-virus or anti-malware update event fails in its regular schedule, then CDI will validate and run the definition updates once again. If the definition updates fail two consecutive times or if the definition versions are older than two days, then CDI will remedy the issues as per the SLO under effect.
- All issues arising out of anti-virus definition updates are categorized at a "P3 Priority"

- If the anti-virus or anti-malware update event causes system related issues, then the CDI Services team will engage as per the SLO under effect.

Supported Anti-Virus Products
Symantec, McAfee, Trend Micro, Kaspersky, ESET NOD32, Microsoft Security Essentials, and VIPRE

3.8.3. Bundled Anti-Virus and Malware (Optional)

CDI bundles VIPRE Business Premium with its services and will be provided to customers who opt for it. The CDI services team will make available a copy of the VIPRE Business Premium MSI package to the customer. The customer may perform a self-install of the software, or request CDI to install it on its servers during the on-boarding process. For these environments, the following apply:

- The VIPRE client configuration is updated every 4 hours, and managed by CDI from a central VIPRE console
- The VIPRE clients will periodically download definition file updates from the local update server, or from the VIPRE update site over the internet
- Scheduled anti-virus scans run every Friday at 4PM on all the managed clients
- CDI will escalate to the customer if virus infections are identified but still remain not cleaned. It will not create a ticket or notify the customer if the virus is already cleaned by VIPRE antivirus solution
- The CDI team checks virus infection logs every 8 hours
- CDI accepts no liability if systems are infected by a virus not caught by the VIPRE software, or if the VIPRE software cannot catch new or existing viruses on the server

3.8.4. Preventive Maintenance Schedules

Servers

Maintenance Activity	Frequency	Schedule
Anti-virus or Anti-malware definition updates	Daily or Weekly	2 PM if daily;
Patch Scan		Wednesday 1 PM
Patch Management (Install)	Monthly	One weekend in the month (Sat. or Sun.)

4. Customer Visibility and Auditability

4.1.1. Auditability

All remote activities performed by CDI NOC engineers are recorded and available for the customer to replay and review via the session recordings capability in the CDI ITOP Platform.

4.1.2. Infrastructure Visibility Portal

CDI's services provide visibility into your IT infrastructure via the CDI ITOP Platform. This provides access to current status of the devices across different locations, while providing useful trending reports for advanced analysis.

4.1.3. Reports

CDI's services also include reports that offer a comprehensive view of performance and availability of the customer's infrastructure.
You can generate on-demand and/or schedule reports from the CDI ITOP that include the following:

- Inventory reports
- Problem & incident management reports

Additionally, monthly reports are available which includes:

- Executive summary reports
- Executive reports

Appendix A. Service Level Objectives

All activities will be performed in an SLO based service delivery model. However, because there is no lockdown on the environment, important onsite operational requirements such as availability, capacity, and outages will be the responsibility of your IT team. Your IT team should inform us of any device addition or deletion, as well as any changes to your IT infrastructure. The following table describes the various priority levels associated with incidents. The sources of alerts are either from the monitoring system or from user requests entered via the ticketing system, phone or emails.

Priority Definitions

Priority	Resolution SLO	Mode of escalation
P0: Critical	This is an EMERGENCY condition that **significantly** restricts the use of an application, system, network or device to perform any critical business function. This could mean that several departments in the organization are impacted. Direct calls will be made by the NOC to the designated IT contact.	Phone, Email and Ticket
P1: High	The reported issue may **severely** restrict use of an application, system, or device in the network. This could mean that a single department is impacted but the overall network and servers are functioning.	Email and Ticket
P2: Medium	The reported issue may restrict the use of one or more features of the application, system, network or device, but the business or financial impact is not severe.	Email and Ticket
P3: Low	The reported anomaly in the system does not substantially restrict the use of one or more features of the application, system, network or device to perform necessary business functions.	Email and Ticket

Service Levels for *SmartEscalate* and *AID*

Priority	Service Response Time	Customer Notification (During Business Hours)	Customer Notification (After Business Hours)
P0: Critical	15 min.	Call within 15 min.	Call within 30 min.
P1: High	2 hrs.	Email sent and ticket updated within 2 hrs.	Email sent and ticket updated within 2 hrs.
P2: Medium	4 hrs.	Email sent and ticket updated within 4 hrs.	Email sent and ticket updated within 4 hrs.
P3: Low	12hrs.	Email sent and ticket updated within 12 hrs.	Email sent and ticket updated within 12 hrs.

Service Levels for *MANAGE*

Priority	Service Response Time	Customer Notification (During Business Hours)	Customer Notification (After Business Hours)	Resolution SLO	Measured
P0: Critical	15 Min	Call within 15 Min	Call within 30 Min	85% of the cases resolved in 12 Hours	Quarterly
P1: High	2 Hours	Email sent and Ticket updated within 2 Hours	Email sent and Ticket updated within 2 Hours	85% of the cases resolved in 24 Hours	Quarterly
P2: Medium	4 Hours	Email sent and Ticket updated within 4 Hours	Email sent and Ticket updated within 4 Hours	85% of the cases resolved in 60 Hours	Quarterly
P3: Low	12Hours	Email sent and Ticket updated within 12 Hours	Email sent and Ticket updated within 12 Hours	85% of the cases resolved in 120 Hours	Quarterly

- Resolution SLOs are void for those cases that are escalated to vendor tech support, hardware vendor, ISP, or third party vendors
- Resolution SLO is calculated from the time ticket is assigned to the NOC team (L2/L3/CoE)
- Resolution SLO timer is paused during the following ticket statuses: (a) “Handed-over to Customer” (b) “On-Hold” (c) “Under Observation” (d) “Resolved”

Appendix B. Services Not Included in the Base Monthly Fee

The following list of service activities are not included in the Base Monthly Fee. These services are available on a T&M or Project basis:

- Services that are not the result of a disruption, require design services, and require the disruption of service to implement
- Any service that is required onsite.

Examples are:

Active Directory	**Microsoft Exchange**
Plan, Prepare and Install Active Directory Installation and Rename or decommission a domain controller	New Server deployment, provisioning , configurations & migrations
Add/remove the global catalogue to a domain controller and verify global catalogue readiness	New site architect/design/re-design/ migrations of Windows Servers, Data to the remote office or branch office.
Move/Restore and rebuild SYSVOL manually or by using the Active Directory Installation Wizard	Exchange Server Infrastructure Changes, Setup/Management of Server roles, Client access server role, Hub Transport Server role, Edge Transport Server Role, Unified Message Server Role
Create/remove Trusts and Add/remove a site or subnet to the network. Link sites for replication and move a domain controller to a different site	New Set up/installation of new Exchange 2007/2010 Environment, Migration/upgrading of Exchange 2003 to 2007/2010 Environments, Analysis and Best Practice implementation on Customer Environment for Exchange 2003/2007/2010, Upgrading/Migrating from Exchange 2007 single Role to Multiple Roles, Upgrading/Migrating from Non-Clustered Exchange 2007 to Clustered/fully Redundant Exchange/Email Infrastructure