

Scope of Service: Apex

DeKalb County Schools

5/8/2025

Account Executive:

Rob Huff

rhuff@stepcg.com



STEP

Contents

Statement of Confidentiality	2
Limitation of Liability.....	2
General:.....	2
STEP Executive Summary	3
STEP.....	3
Our Mission	3
OUR VALUES:.....	3
VISION:.....	3
STEP Apex Service Overview:	4
Included Service Feature Definitions.....	4
Apex Service Descriptions.....	6
Service Onboarding:.....	6
24/7/365 Monitoring.....	6
Customer Dashboards & Alerts.....	6
STEP CCC Support:	7
Vendor Management:	7
Network Audit:.....	7
Release Management:	8
MACD:	9
Customer Success Manager:.....	9
Quarterly Business Reviews:	9
A Compelling Solution	10
Customer Care Center – People, Process, Tools.....	11
Customer Care Center (CCC) Description.....	11
Root Cause Analysis.....	11
CCC Workflow	12
Customer Access.....	12
Detailed Service Level Agreement	13
Priority Level Definitions.....	14
General Responsibilities, Assumptions, & Terms.....	15
Customer Responsibilities.....	15
STEP Responsibilities	16
Terms.....	16
Contract Dates & Billing	19
Pricing Summary	19
Additional Services	19
Payment.....	19
Scope	19
Proposal Acceptance.....	20
Appendix A: Quoted Details.....	21



Statement of Confidentiality

This document contains proprietary and confidential information. All data submitted is provided in reliance upon the recipient's agreement not to use or disclose except in connection with its business dealings with STEP. The recipient of this document agrees to inform its present and future employees who receive or have access to the information contained in this document of its confidential nature, and to instruct each employee that he or she must not disclose any information concerning this document to others except to the extent that such matters are generally known to, and are available for use by, the public. The recipient of this document agrees that it will not duplicate or permit others to duplicate any material contained herein except for its own internal use.

By acceptance of this document, the recipient agrees to be bound by the foregoing statement.

Limitation of Liability

In performance of the services offering outlined in this Agreement, except for damages resulting from its fraud or gross negligence, STEP will in no event be liable for: (I) Any indirect, special, incidental or consequential damages, however caused and whether or not advised in advance of the possibility of such damages; or (II) Damages for the lost profits or lost data; or (III) cost of procurement of substitute goods technology or services. Except for liability resulting from its fraud or gross negligence, STEP entire liability arising from or relating to the subject matter of this Agreement shall be limited to the amount received by STEP under this Agreement.

General:

This document (this "Scope of Service") describes the Service elements, features, and deliverables related to the Managed Services offered by STEP.

Provision of this Service is governed by and subject to the terms and conditions set forth in the applicable agreement to which this Scope of Service is attached. In the event of a conflict between the terms of this Scope of Service and an understanding and/or an exclusion, the terms of this Scope of Service shall prevail.

The specific quantity and type of Service purchased by Customer will be documented in the applicable quotation and Scope of Service document issued to Customer is accepted by Customer's placement of a purchase order.

STEP

STEP Executive Summary

STEP

STEP is a highly innovative, award winning, nationwide IT services engineering firm headquartered in Northern Kentucky/Greater Cincinnati. STEP solutions are powered by strategic experts and best of breed technologies solving our customers' most complex IT challenges. STEP's team and expert engineers provide customers with solutions for cloud, security, collaboration, core infrastructure, and managed services. We are about doing what's right and sharing in our customers' successes. We have a culture that empowers talent and passion allowing employees to be innovative and execute. STEP is where innovation meets execution.

Our Mission

At STEP, our WHY is to explore what is possible, helping our customers use technology to solve business problems and achieve real business outcomes.

OUR VALUES:

Teamwork | Gratitude | Integrity | Passion

We are passionate.

We care about each other and our customers.

We empower our employees and customers.

We treat everybody with respect.

We are easy to do business with.

We are committed to innovation.

We have fun.

VISION:

To constantly innovate and be the leading IT Solution Provider in the markets we serve.

STEP

STEP Apex Service Overview:

A proactive service with 24x7x365 monitoring and troubleshooting by the CCC for incidents reported by our monitoring platform, Navigator, as well as responsibility for completing MACD changes requested by the customer. This service is for customers who are looking for a provider who can watch the network and make intelligent decisions about what happened, figure out what caused it, and how to fix it. Once the root cause has been identified, our staff will either resolve the problem or work with the customer to implement the recommendation to resolve the issue. With the Apex service level, the provider's responsibility is to monitor the environment, troubleshoot any anomalies, resolve the issue if that is remotely possible for configured metrics, and complete MACD requests.

Services Included:
Service Onboarding
Service Desk
24/7/365 Monitoring
Device Configuration Backups
Dynamic Mapping
Customer Dashboards & Alerts*
CCC Support for incident response
Proactive CCC Engagement
Vendor Management
Network Audit
Release Management
MACD
Customer Success Manager

Please refer to the Pricing Summary for any Additional Services included in this Proposal

*Alerts to automated via ticket notification

Included Service Feature Definitions

Service Onboarding: Upon purchase of a STEP managed service offering, Transition Services to STEP support.

Service Desk: The single point of contact between the STEP and the users. The service desk manages incidents and service requests, and also handles communication with the users.

STEP

24/7/365 Monitoring: provides real time alerting to issues as reported by Navigator as either down/unreachable or in the case of a threshold violation.

Device Configuration Backups: Navigator also serves as a resource to automatically backup network device configurations. These backups assist with rapid systems recovery in the event of a catastrophic failure or ransomware. These config backups will be available to the customer via the Navigator web portal.

Dynamic Mapping: Allows for dynamically updated maps in Navigator to be generated. Discovery protocols need to be properly configured for this feature to work. This only applies to devices in Navigator.

Customer Dashboards & Alerts: STEP will provide standard dashboards and reports with the Navigator for additional insight into the customer's network. Alerts generated by the Navigator will result in a ticket being automatically created in the CCC Service Desk for investigation.

CCC Support for incident response: The Customer Care Center (CCC) will provide Tier 1 - 3 level support. The escalation process progresses from the lower tier to the higher tier. Engineers will troubleshoot, isolate issues, assess logs, and remediate issues utilizing incident management.

Vendor Management: STEP has direct access to the vendors for support and assistance as needed. The CCC will provide Tier 1 – 3 support and facilitate escalations to manufacturers as needed for additional Tier 3 – 4 support. The CCC will coordinate the engagement with the manufacturers.

Network Audit: STEP will provide a one-time Network Audit during the onboarding process to review the current state of the network, provide an action plan to remediate issues found, and provide corrective action for qualifying items.

Release Management: STEP will provide both Reactive and Proactive system patching for systems covered under this agreement. STEP will coordinate with the customer to schedule a maintenance window to perform patching activities.

MACD: Moves, Adds, Changes, & Deletes - MACD work is any request for changes to devices that falls outside of incident response, and will be performed remotely by STEP for systems covered under this service agreement.

Customer Success Manager: STEP will appoint a Customer Success Manager (CSM) to be a customer's business advocate. The CSM will partner with the customer to review business objectives, review customer concerns, review changes in the customer's environment and assist in providing alignment with customer initiatives. The Customer Success Manager (CSM) offers support for service level management, general STEP customer advocacy, and service escalation support from a designated service contact.

Quarterly Business Reviews: STEP will host a remote service review meeting on a quarterly basis and review operational data including incident tickets and historical trends in accordance with the agreed upon agenda. The review may include business outcomes from the previous review period and confirm alignment of the contracted services with customer's

STEP

business priorities, new requirements, and needs. STEP may review historical data, trends, delivery performance, operational risks and provide recommendations for improving service delivery. In addition, STEP may highlight modern technologies and services industry tools/capabilities.

Apex Service Descriptions

Service Onboarding:

Upon receipt of purchase order for a managed service, the Client will be contacted to set up a kickoff call to initiate the service onboarding. Transition Services will be assigned to collect customer and device specific information and add that to STEP's toolset. Transition Services will review the service with the customer, identify critical needs for the customer and configure alert priorities (as needed/applicable). They will verify the product support list, review the quote, and verify any limitations to coverage.

It is the customer's responsibility to provide accurate equipment information, IP address and credential information. STEP is not responsible for inaccurate information. If credential information is unknown, STEP will work with the manufacturer to reset passwords (if possible) which may be billable. STEP will add covered devices to Navigator, configure alerting and notification, create the standard Dashboard views for the customer, and provide user access to Navigator for the customer.

24/7/365 Monitoring

Data network monitoring provides real time alerting to issues as reported by STEP's monitoring tool, Navigator, as either down/unreachable or in the case of the threshold violation. Navigator utilizes either onsite or remote based data collectors, depending on the customer's environment. Protocols used for monitoring are described below:

SNMPv2 & SNMPv3 Monitoring: At this time, both protocols are supported by Navigator.

API Monitoring: Some products are monitored via the manufacturer supported API rather than SNMP.

Monitoring Development:

STEP may develop and/or collaborate with vendors to add additional monitoring features as necessary for new products. This may be due to roadmap or customer request. In the case of customer request this may be a billable event. Any customer requests can be submitted in the Service Desk. Each individual request will be assessed, and updates will be shared with the customer through the Service Desk.

Customer Dashboards & Alerts

STEP will provide standard Dashboard views in Navigator to provide insight into the health of your network infrastructure. There are multiple network overview dashboards as well as

STEP

device-specific views. Notification of alerts will be shared with the customer via automated ticket creation, and the CCC will proactively investigate any alerts received.

Feature Threshold Alerting

Basic threshold alerting allows for alerting triggers to be set on any monitored data source metric such as CPU utilization, memory utilization, port state (up/down) and port bandwidth utilization.

Multiple data sources may be used to monitor each asset. These will usually include OS specific data sources for the device which may include metrics such as:

- CPU/memory/disk utilization
- Host Uptime
- Status of port response (IE HTTP, HTTPS, DNS, etc.)
- TCP/UDP statistics such as segments, datagrams, drops, etc.
- ICMP Ping response time

Additional data sources may be applied to devices depending on vendor specific OIDs or APIs.

STEP CCC Support:

Tier 1-3 Support: STEP will provide Tier 1 - 2 level support with escalation to internal Tier 3 to respond to incidents reported by either Navigator or the customer and will provide fault management which will minimize the negative impact of incidents by restoring normal service of operation as quickly as possible. The escalation process progresses from the lower tier to the higher tier.

Vendor Management:

STEP will provide Technical Assistance Center (TAC) support to network OEM customers by coordinating/managing OEM support for hardware (including RMA coordination), firmware and software fixes to resolve incidents and provide fault management which will minimize the negative impact of incidents by restoring normal service of operation as quickly as possible. The CCC will escalate issues for assets under contract with the manufacturer for additional Tier 3 – 4 support as needed. This includes issue assessment, data collection, and manufacturer collaboration support.

Contract Support: As part of the Apex managed service, the customer is required to maintain all vendor maintenance agreements and subscriptions on covered devices. STEP is responsible for notifying and facilitating the renewal of vendor maintenance and subscription services purchased through STEP. The customer will be responsible for renewing all services not purchased through STEP.

Network Audit:

STEP will provide a one-time Network Audit during the onboarding process to review the health of the system and current system patches installed. A synopsis of the findings will be provided to the customer. After the assessment is complete, an action plan will be assembled to devise next steps.

STEP

Corrective Action:

STEP will complete corrective action for items meeting the following criteria:

- Proper configuration of DNS
- Proper configuration of NTP
- Syslog configuration to point devices to Navigator
- Configure CLI Audit
- Proper Loop Prevention configuration
- System Patching:
 - System patching is deemed as any installation of a firmware update that keeps the system on its current major supported release to resolve feature functionality / system stability issues.
 - System Upgrades are defined as software and or firmware upgrades that require a transition from one major release to another. If the dot release patching path requires upgrade to a new release, then the patching event must be treated as an upgrade event. System Upgrades are not covered under the Apex service agreement and would not be included in the Network Audit corrective action. STEP can be contracted to perform system upgrades as part of a project.

Additional changes that do not meet the requirements for included corrective action will be billable and treated as a project by STEP.

Release Management:

STEP will provide both Reactive and Proactive Release Management for covered devices under the Apex agreement. Release Management is comprised of system patching within the device's current major release. System upgrades, as defined below, are not included in the Apex service agreement and would be considered billable. All patching will be performed during a maintenance window agreed upon by both STEP and the customer.

System Patching: System patching is deemed as any installation of a firmware update that keeps the system on its current major supported release.

System Upgrades: System Upgrades are defined as software and or firmware upgrades that require a transition from one major release to another. If the dot release patching path requires upgrade to a new release, then the patching event must be treated as an upgrade event.

Reactive Release Management: Provides reactive patching for mission critical systems under contract that are experiencing service impacting issues. Reactive security patching is also included. Security patching is completed upon customer request and will be based on the manufacturer's recommendations and service impact.

Proactive Release Management: Allows for systems to be updated to the latest or preferred firmware/software release. Proactive patching is done at the customer's request and is limited to once per year.

STEP

MACD:

MACD worked is deemed as remote modifications to any existing supported systems listed in the service agreement that includes this service entitlement.

- Moves add and changes are limited to:
 - Changes that can be performed remotely for existing configured features or protocols.
 - Changes that do not require engineering or modifications to current architecture.
- STEP is only responsible for changes to systems that are under contract. Any 3rd party or uncontracted system that is not covered, a project shall be opened.
- MAC work does not include onsite modification or hardware support.
- The customer agrees to provide assistance with system access, if applicable.

MACD work is available as outlined below. Changes will be scheduled within 72 hours / 3 business days of the request, provided all the information has been received to make the change.

MACD is limited to 20 hours' worth of work per month with no carry-over of unused hours.

Customer Success Manager:

A Customer Success Manager is a customer's business advocate and will partner with the customer to review business objectives, review customer concerns, review changes in the customer's environment and assist in providing alignment with customer initiatives.

The Customer Success Manager (CSM) offers support for service level management, general STEP customer advocacy and service escalation support from a designated service contact. This "trusted advisor" works to ensure that every customer service contact with STEP, no matter the solution, receives an exceptional customer experience. This builds customer loyalty and peace of mind, allowing the customer to increase focus on their core business. This position aims to provide a more personal level of service that enables STEP to gain and retain stronger customer relationships, leverage its strengths as a solutions provider, and distinguish itself from the break/fix services approach that is prevalent in the marketplace.

The CSM acts on the customer's behalf to bring visibility of issues and concerns to the appropriate groups within STEP. Additionally, the CSM will be asked to manage the customer's service experience across all STEP solutions and supporting the customer's service model evolution. In short, the CSM is a "virtual" extension of the customer's team within STEP.

Quarterly Business Reviews:

The CSM will provide business reviews of a customer's environment. The business review provides direct insights into the customer's environment and STEP engagements throughout the course of the quarter. The detailed report often covers but is not limited to: incidents created, data analytics showing trends to help customers understand problematic areas, alarm distribution by site, incident arrival method, incident durations, and aged incident review.

STEP

A Compelling Solution

Our solution is a market driven, innovative service management offer that enables the customer to take charge of their network while retaining the experience and expertise that STEP has to offer.

The STEP Apex Service is built upon the industry-recognized best-practice IT Service Management framework, Information Technology Infrastructure Library – ITIL. ITIL is globally recognized as a best-practice framework for the delivery of IT Services for all types of organizations, particularly in the large enterprise and government sectors.

The STEP Apex Service is designed to provide 24/7/365 Service Desk, delivering the following benefits:

- STEP's industry leading networking expertise
- 24/7/365 CCC Support
- Direct Vendor Escalation Paths
- Remote incident response and management
- Core services include:
 - Service Onboarding
 - Service Desk
 - Tier 1-3 Support
 - OEM Direct Support (Vendor Support)

STEP

Customer Care Center – People, Process, Tools

Customer Care Center (CCC) Description

The STEP Customer Care Center provides a full suite of monitoring and STEP maintenance services to our customers. STEP Customer Care Center has the capabilities to provide a high level of confidence and customer satisfaction knowing that STEP is there; 24x7x365 monitoring, maintaining and supporting our customer's network. STEP's CCC solutions are flexible enough to conform to customer requirements and integrate into their processes for seamless operational flow. The CCC is a geographically diverse organization, utilizing multi-layer secured cloud-based applications. We offer both on-prem data collectors, as well as remote options. Remote collectors are located in a secured access facility, and fully redundant with battery backup for operational stability.

Our CCC has a large number of both vendor and industry certifications to provide Tier 1 – 3 support directly to our customers. We are certified with all vendor partners with certs ranging from basic config to architectural design, including expert-level certifications. STEP has received numerous awards from our vendors for our technical expertise.

- Detailed incidents shall be created with the CCC once an issue has been reported.
- Customers who open tickets with the CCC are responsible for providing an accurate description, the severity of the issue, the impact, and the correct location that the issue is occurring.
- The client will assign a point/point(s) of contact who will engage directly with the CCC (as needed). In addition, the customer will provide contact information for any 3rd party relationships that STEP is responsible for working with under this contact / service.
- If alternative unsupported connectivity methods are utilized and/or no direct connectivity is available, the Time to Service and STEP response may be limited and/or delayed.
- The CCC will escalate issues within the tiered structure once that tier has exhausted all resources. A Subject Matter Expert (SME) may be needed to troubleshoot across platforms. That SME will cross collaborate, if needed and will provide the necessary guidance to help bring the issue to remediation.
- STEP will record and manage service requests for information.
- STEP will provide advice, standard troubleshooting and/or support.

Root Cause Analysis

A root cause analysis is performed at an infrastructure level. An OEM manufacturer root cause analysis may be subject to additional charges based on customer's contract.

A Root Cause Analysis (RCA) will be provided per a customer's official request with the CCC for critical outages only and will be done in collaboration with the manufacturer.

The level of detail provided for a root cause analysis is dependent on the customer's level of service and is highlighted below per service agreement:

- Apex – Full Write-up including supporting data and recommendations

STEP

Log availability and system access will determine the level of detail included in the system analysis.

If data is not available, an RCA may not be possible.

The RCA will become best effort, if the customer is not running supported software and / or firmware. The timeline for delivery of an RCA may vary depending on the amount of analysis required and manufacture engagement, if required. The minimum turnaround time is 72 hours/3 business days.

CCC Workflow

Our CCC utilizes a web-based portal to facilitate incident reporting, management, escalation and remediation. Once an incident is reported to the CCC by a customer, an incident ticket is created in our portal.

Since many different parties, systems and processes are involved in the ultimate resolution of an incident, an incident management process is followed to facilitate and provide a single point of contact to ensure the smooth flow between various parties within the required time frames and under the appropriate circumstances. In implementing this process, it ensures proper resource management, prioritization, timely communications, and correct escalation management takes place.

Escalation activities provide for several escalation levels for critical incidents based on the length of time the service incident has been ongoing, less periods where both the customer and STEP agree that the escalation timer should be stopped for any reason.

Customer Access

Flexibility in getting access to the support you need when you need it is a priority to STEP. The Service Desk customer portal is your online resource for incident reporting and management. Our platform allows customer visibility into all their current incidents and the current status of any given incident. Customers may use our portal to report new incidents or to update the status of existing incident tickets. Alternatively, customers may also call or email the CCC to report an incident. We are continuing to enhance our customer access with new features and functionality to ensure that customers have access to the CCC 24x7x365 regardless of their device or location.

STEP

Detailed Service Level Agreement

Priority Level	Response Time
Priority 1 – Critical	15 minutes
Priority 2 – High	30 minutes
Priority 3 – Important	4 hours
Priority 4 – Normal	8 hours

The customer sets the initial priority for a ticket if they call the CCC to report an incident or the customer selects the priority when they create the incident via the web portal. If the incident is created via our automated monitoring systems, the priority is set using a pre-defined set of rules created by STEP following the industry's best practices. However, at any time the customer can call into the CCC and request a change in the incident priority (upgraded or downgraded).

Customer Initiated Support Requests:

All customer-initiated support requests must be done using one of the following methods. Any other method of communication is not supported for incident response.

- Critical issues should always be raised via the toll-free number: 888-234-0045
- Customers can open a ticket with the CCC utilizing the web portal: stepcg.myportallogin.com
 - The customer is responsible for setting the initial incident priority when reporting an incident. If a priority is not selected, it will be opened as a Priority 3.
 - Tickets submitted for questions or change requests will be set with a default of Priority 4.
- Customers can also open a ticket via email to our ticketing system: customersupport@stepcg.com
 - All emailed requests will be opened as a Priority 3.

STEP Initiated Incidents

- The automated alarming will adhere to the recommended manufacturer best practices.
- The designated priorities are defined using STEP's best practices; however, the customer can change the severity of any automated incidents by contacting the CCC.

STEP

Priority Level Definitions

Priority 1 - Critical: the problem results in extremely serious interruptions to a production system. It has affected, or could affect, the entire user community resulting in a total service outage. Tasks that should be executed immediately cannot be executed because of a complete crash of the system or interruptions in main functions of the production system. Data integrity is compromised, and the service request requires immediate processing as the issue can result in financial losses.

Priority 2 - High: the problem results in serious interruptions to normal operations, will negatively impact an enterprise-wide installation, urgent deadlines or at risk. In a production system, important tasks cannot be performed, but the error does not impair essential operations. Processing can still continue in a restricted manner, and data integrity may be at risk. The service request requires timely processing, because the malfunction could cause serious interruptions to critical processes or negatively impact business.

Priority 3 - Important: the problem causes interruptions in normal operations. It does not prevent operation of a production system, or there could be minor degradation in performance. The error is attributed to malfunctioning or incorrect behavior of software or hardware. The issue will affect users by degradation to performance with no interruption to service.

Priority 4 - Normal: the problem results in minimal or no interruptions to normal operations (no business impact). The issue consists of "how to" questions or end user requests including issues related to operational awareness, installation and configuration inquiries, enhancement requests, MACD requests, or documentation questions.

STEP

General Responsibilities, Assumptions, & Terms

Customer Responsibilities

Remote Support Access

- Customer is responsible for providing appropriate remote network access (including VPN access/credentials) as appropriate/if applicable.
- Customer is responsible for providing usernames and passwords for all covered devices.
- Customer is responsible for providing a point of contact with physical network/security access onsite while STEP provides remote support as appropriate/if applicable.

Onsite Support Access

- In the event that travel to any of the sites within the Service Contract is required, the customer will provide access to the physical locations including access to local equipment and office space. Onsite travel is not included in this service offering and will be billable.

Vendor Software & Hardware Support

- STEP requires the customer to continue renewing the necessary software/hardware support to allow for the systems to remain on current release as recommended by the manufacturers except where STEP has been contracted to provide replacement hardware or hardware/software has reached manufacturer end-of-support. Customer acknowledges that STEP is not liable for software defects and may not be able to provide software patches for those systems not entitled to manufacturer software distribution.
- If no manufacturer support contract is available for an End of Life (EOL) or End of Support (EOS) device, STEP will provide best effort CCC support for those products.
- The customer is responsible for maintaining supported software releases on covered equipment as recommended by the manufacturer.

Hardware & Software Licensing

The customer will be responsible for procuring all applicable hardware/software/licenses (not being provided by STEP) and have all equipment ready and prepared for the Support Services as outlined in this contract.

Points of Contact

The customer will assign a point/s of contact who will engage directly with the STEP CCC. In addition, the customer will provide contact information for any 3rd party relationships that STEP is responsible for working with under this contract.

Documentation

Customer will provide the following documentation which will aid the STEP technical consultants in ensuring a meticulous review of the network infrastructure and ecosystem:

- Network architecture illustrations/drawings/Visio delineating all devices, if applicable
- Network documentation showing IP addresses, VLANs, subnets for devices, if applicable

Communication Channels

STEP

The customer must utilize proper communication channels when reporting an incident to STEP (as defined in this document). Any other method of communication is not a supported means for ticket creation/incident reporting.

Other

Customer will provide access and assume financial responsibility for certificates issued from an external Trusted Root Authority as required for the operation of the service.

STEP Responsibilities

- Provide Transition Services to guide and lead the onboarding process
- Inform the customer of any concerns identified during the onboarding process
- Provide escalation contacts within STEP
- Create and maintain customer portal access
- Maintain & support Navigator
- Provide timely support for incidents and service requests as defined in this document
- Minimize Risk of Service Impact

Terms

Customer-Supplied Hardware & Software:

Unless specified in this proposal STEP is responsible only for the monitoring hardware/software provided by STEP. Any additional customer hardware or software is not covered under this contract including but not limited to customer-supplied UPS, virtual machine hosts, physical servers, network devices and associated cabling as well as any licensing. If STEP is supporting Virtual Machines on a customer-supplied Virtual Host customer must notify and work with the STEP CCC to ensure that platform updates will not cause any unnecessary downtime or conflicts with the supported Virtual Machines.

Pre-Existing Conditions:

Pre-Existing Conditions that are classified as project work meet the following criteria:

- The issue is pre-existing and unknown to STEP prior to Managed Services onboarding
- The amount of time to explore, design or remediate exceeds 3 hours.
- The issue impacts functionality, system stability, user experience, and/or any condition that has a negative impact on the system or installed applications.

STEP will provide the following information for conditions that meet project work criteria.

- An explanation of the pre-existing condition
- The recommended options for remediation

Password Management:

STEP

- Customer acknowledges and agrees that STEP disclaims all liability for password management that for any reason a system is compromised, passwords expire or become non-functional.
- STEP will comply with manufacturer best practices.
- STEP is solely responsible for STEP managed passwords.
- STEP passwords will not be shared.
- STEP passwords will comply with its password policy.
- All exchanges of sensitive information will be only shared in an encrypted format.
- Privileged access may be required to remediate password issues which could incur additional charges.
- Customers are responsible for customer user credentials and passwords.
- Bulk and/or reoccurring password changes would be considered a project and would incur T & M charges.

Certificate Management:

- Certificate Management and Renewal is the responsibility of the customer if the certificate audit and implementation are not managed by STEP.
- Alarms related to certificate expiration events will be forwarded to the customer and will be held by Managed Services until certificates are renewed if the customer is responsible for certificate audit and installation.
- Third party certificates are the responsibility of the customer to provide in the event certificates are required.
- Customer will provide access and assume financial responsibility for certificates issued from an external Trusted Root Authority as required for the operation of the service.
- Certificate Renewals completed by STEP will be billed at the rate of the resource doing the work through T & M or will be scoped as a project.

Best Effort:

The following products have been identified as best effort support. Best effort applies to customer systems that meet the following criteria:

- Customer does not have an active manufacturer support contract, or the system is beyond End of Manufacturer Support (EOS) or End of Life (EOL)
- Systems that contain legacy hardware parts that are hard to acquire
- Software and updates are no longer available.
- Require a specialized skillset to support
- STEP will provide best effort support for the legacy systems that are no longer supported by the manufacturer. The customer understands that due to the above circumstances not all events may be recoverable, which may lead to down time or unconventional workarounds. Systems that are unpatched may be at risk to security vulnerabilities. STEP is released from liability for all impacts from legacy equipment. STEP reserves the right to discontinue support on renewal if a product is found to be unsupported. Customer understands that investment in the latest technology is the only way to ensure both manufacturer support and access to patches. The customer also acknowledges that due to the limited parts available that not all parts acquired may work and that multiple parts may need to be sourced. Sourcing

STEP

of parts may take extended periods of time to acquire. If parts cannot be acquired, customers may need to look at alternative solutions.

Product Coverage

STEP reserves the right to discontinue support of product platforms based on factors such as product demand, manufacturer support, manufacturer road maps, certification requirements and tools support.

Third Party Tools Monitoring and Potential Conflicts:

If STEP is the services incumbent providing managed and monitoring services, its tools will supersede any third-party monitoring solutions on the supported systems as originally proposed. Through discovery, STEP can assist the customer in identifying conflicts and provide a solution to remediate. This will be completed on a Time and Material basis. SLO and SLA adherence may be impacted by the implementation of the third-party tool or processes. Scope of Service modifications will require review. Individual site and/or location monitoring may not be excluded from monitoring and/or support when registered to a supported core system.

Customization:

STEP catalogs and scope of service documents define the features that we have proposed and provided. Customers may require customizations to meet specific requirements. STEP services are predefined and configured based on STEP's offer, best practices and tools. Customization of services, tools and processes are subject to a mutual collaboration approach that includes defining customization requirements, exploration of the enhancement request with appropriate parties, understanding additional costs, and establishing a timeline for deliverables. Deviation from the current offer may impact deliverables, service, cost and may require project collaboration between STEP and the customer. After onboarding, in-service additional customization may be required to obtain the service level objectives agreed upon.

STEP

Contract Dates & Billing

This contract is valid for 1 year, beginning at the service start date, with upfront billing.

Pricing Summary

Please see the provided Proposal for pricing breakdown of all Support Contracts.

Additional Services

There are no additional services included in the contract.

Payment

This quote is subject to the STEP payment terms and conditions.

Scope

This Scope of Service identifies the purchasable services available under the STEP Apex Service offer. The price reflects the services selected by the customer. Additional services can be priced and scoped as required. Additional notes can be found on pg. 3 of this Scope of Service.

STEP

Proposal Acceptance

By signing this agreement, the parties agree to the terms and conditions as stated in this document. IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date written below. This Document is governed by the STEP Terms and Conditions Agreement between STEP.

DeKalb County Schools:

Signature

Printed Name

Title

Date

STEP:

Signature

Printed Name

Title

Date

STEP

Appendix A: Quoted Details

The Support Contract will include the following equipment, which will be considered “In Scope” for the duration of this contract:

SCG-MediumFW-Apex-1Y – QTY: 2

- Palo Alto Firewalls

SCG-Switch-Apex-1Y – QTY: 160

- Ruckus/Brocade
- Juniper/Mist

SCG-Controller-Apex-1Y – QTY: 16

- Aruba WLAN Controllers

SCG-AP-Apex-1Y – QTY: 10

- Aruba APs