K2 SITE RELIABILITY

ENTERPRISE SUPPORT SERVICES

3/27/2020

TABLE OF CONTENTS

1. OVERVIEW

These K2 Site Reliability Policies (“Policies”) apply to service delivery of the K2 Site Reliability Service (“the Service”) by K2 Software, Inc. and its subsidiaries (“K2”).

As used in these policies, “customer”, “you” and “your” refer to the individual or entity that has ordered the K2 Site Reliability Support service from K2 or an authorized distributor, as applicable.

The Service is provided in English, and during regional hours of operations, unless noted otherwise.

2. TERMS

2.1. K2 PLATFORM

The Service relies on K2 software being installed in a customer-provided Azure environment. This K2 Platform-as-a-Service (PaaS) is referred to as “K2 Platform.” With the Service, K2 maintains the K2 Platform, enabling customers to build applications on K2 software without the overhead of setting up, hosting and maintaining K2 environments. The customer does not manage the underlying K2 software components but retains control over the application development cycle and deployed applications.

2.2. UPGRADES AND UPDATES

Major or minor versions of the K2 software, and their installation, are referred to as “Upgrades.” Fix packs, cumulative updates, and other code fixes are known as “Updates.” For more information, see the K2 Product Support and Release Strategy.

2.3. INCIDENT

A “Site Reliability Incident,” or “Incident,” is a single event or set of events which results in downtime.

2.4. DISASTER

For the purposes of this policy, a “Disaster” is defined as an unplanned event or condition that causes a complete loss of access to the primary third-party datacenter used to provide the Service.

2.5. ROLES

	Role	Description
Customer Roles	Customer Azure Administrators	Customer resources who administer the customer Azure tenant.
	Customer Active Directory Administrators	Customer resources who administer the customer’s Active Directory (AD) environment.

	Role	Description
	Customer Network Administrators	Customer resources who maintain the customer’s network and network infrastructure.
	Customer Database Team	Customer resources responsible for the management, administration, backup and DR specific to the databases that are required for the Service.
	Customer SharePoint Administrators	Customer resources who administer the customer’s SharePoint environment. NOTE: SharePoint is not required to operate K2 Platform and this role is only required if the customer requires integration into SharePoint.
	Customer K2 Administrators	Customer resources who maintain the applications and application-specific components on the K2 production and non-production environments.
	Customer K2 Helpdesk	Customer resources who provide first-level application support for the applications deployed on the K2 production and non-production environments.
	Customer K2 Developers	Customer resources who are responsible for building applications that run on or utilize Cloud environment(s). These include no-code developers who may build applications with tools like K2 Designer as well as coding developers who build applications on K2 software.
K2 Roles	Enterprise Service Manager (ESM)	Service resource who serves as the primary contact for delivery of the Service.
	Customer Success Manager	Service resource who acts as the customer’s main contact during customer Onboarding, and for general account topics.
	Service Onboarding	Service resources who assist during the customer Onboarding phase.
	Service Operations	Service resources who maintain the K2 environment and associated infrastructure, and provide support for operational issues.
	Datacenter Operations	Resources provided by the datacenter provider to monitor and control aspects like software and related Service infrastructure.
	Technical Support	K2 Platform technical support services.
	K2 Virtual Services	K2 resources who perform a variety of services for customers, for fee-based credits.

	Role	Description
	Computer Security Incident Management Team (CSMIT)	Team of Service resources that respond to security threats and breaches.
	K2 Service Account	The identity of the K2 Service Account, the account under which the Service runs.

3. PREREQUISITES AND REQUIREMENTS

Prior to onset of the Service, a readiness review will be conducted, to verify the customer’s infrastructure and K2 environment setup is leveraging best practices, and that all integration points are eligible for cloud connectivity.

In addition to the readiness review, the following are required:

- Customer must have a Microsoft Azure tenant
- Customer must be using a supported version of K2 with at least 12 months of standard support remaining
- A supported authentication provider
- Both the K2 SQL database and the K2 server must be hosted in the same MS Azure tenant
- Service Operations requires remote access capability to the K2 Platform hosted instances
- Service Operations requires full administrative access to K2 Platform instances and supporting virtual infrastructure
- Customer must provide a list of named resources and contact details for all relevant existing technical teams and support structures

4. SCOPE OF SERVICE

4.1. SERVICE CATALOG

The following elements make up the Service catalog.

	Service	Description
Standard Services	Onboarding	Introduce the customer to the terms of the Service and resources. Introduce customer and K2 points of contact. See Onboarding below.
	Platform configuration	Install and configure monitoring tools. See Onboarding below. By default, the Service includes maintenance of three (3) K2 server instances. See the Data Integration section for more information about included integration types.
	Operations monitoring	Quality-of-service monitoring of operational metrics of infrastructure and K2 to ensure the Service is performing to specification.
	Platform administration	Service administration tasks as necessary to address system instability or reliability issues. Administration of users, permissions, and customer applications are not included in these services.
	Platform troubleshooting	Troubleshooting issues in the core infrastructure and Service environment. Customer application troubleshooting is not included in these services.
	Planned service maintenance	Scheduled core infrastructure maintenance such as hardware, operating system, and application version upgrades.
	Unplanned service maintenance	Unplanned core infrastructure maintenance such as replacement of failed hardware or installation of critical operating systems and application patches.
	Service optimization	K2 aims to continually improve on and optimize the Service through regular reviews of operations and education of the Customer K2 Helpdesk team to improve communication, case triage and deflection.
	Service usage and reporting	Administer and report on licensed usage, Service quality
	K2 API Access	All standard, supported APIs and K2 Cloud web-based APIs are included in the Service. Customers can reference these APIs when building custom applications to connect to the Service.
	Technical Support	Governed by the K2 Software Support Policies.
Subscription Add-ons	Disaster recovery (DR) assistance	Service Operations will work with Customer Database Team to restore the Service in the event of outage.
	Additional Production and/or Non-production environment(s)	Additional instances of production and non-production Service environments are available separately.

	Service	Description
	Global Support	Optional upgrade to standard Technical Support, offering product support in multiple regions and afterhours. For more information, see [K2 Software Support Policies]().
	Enterprise Support	Optional upgrade to standard Technical Support, offering premium services and SLAs.
Fee-based Add-ons	Customer-initiated data recovery (Point-in-Time Service Recovery)	Where such services are contracted, the Service will work with the Customer Database Team to restore the K2 Platform and associated K2 Platform data to a prior point in time. This carries a risk of data loss.
	Data restoration impact investigation	K2 typically acts as middleware and interacts between various systems based on workflow tasks, escalations or other mechanisms. Restoration and re-activation of restored workflows might cause unexpected issues, such as duplicated transactions in other systems or re-escalations. As these issues may be solution-specific, K2 Virtual Services can be engaged to investigate the impact of restoring a K2 database to a specific point in time.
	Installation and configuration of K2 Platform environments	The Service does not include installation and configuration of the K2 software. This requires a separate statement of work and will carry a separate fee.
	Migration of customer K2 Database(s) to Azure	The Service does not include migrating a customer's existing K2 database to customer's Azure tenant. Migration assistance requires a separate statement of work and will carry a separate fee.
	Configuration of additional integration points	K2 Virtual Services can be engaged to assist in the configuration of integration points and functionality that is not part of the standard Onboarding process.

4.2. SERVICE EXCLUSIONS

	Service	Description
Excluded Services	K2 Software installation and data migration	The Service does not include provisioning of K2 Platform environments, nor does it include migrating existing customer K2 databases to the customer's Azure tenant.
	Active Directory configuration and setup	Service Onboarding will provide requirements, instructions and policies for setting up Active Directory (AD) in preparation for Service Onboarding. Such AD changes need to be made by the customer and are not provided as part of the Service.
	Other Authentication Provider configuration and setup	Service Onboarding will provide requirements for setting up supported authentication providers in preparation for Service Onboarding. Such changes need to be made by the customer and are not provided as part of the Service.
	Application testing	Testing of new or updated customer applications and testing of applications against new versions of K2 software is not included in the Service. K2 software upgrades could have both expected and unintended effects on applications. While K2 continues to invest significantly in testing and quality assurance to minimize impact from upgrades to the Service, ultimately it remains the customer's responsibility to test applications against new versions of the Service. See the Change Management section for more information.
	Third-Party product integration	Integration with any third-party system that is not already included in the Data Integration Options section below or as agreed with K2 during Service setup is not available within the Service.
	Network and security configuration	When additional advanced network or security configuration is required (e.g. Kerberos setup and testing), fee-based guidance and troubleshooting service will be available form K2 Virtual Services.

4.3. SERVICE REGIONS

The Service is available to customers that can be accommodated via the following Azure datacenter regions:

- US
- Europe
- United Kingdom
- APAC

NOTE **Customers are responsible for validating they are able to legally operate in the third-party datacenter regions described above.**

4.4. ONBOARDING

4.4.1. CUSTOMER ONBOARDING SESSION

The customer, Enterprise Service Manager and Customer Success Management team complete an onboarding call that details the specifics of the Service, including:

- The roles on the customer and K2 side that will be involved in coordinating and supporting K2 Platform for the customer's Active Directory and Microsoft Azure tenant. Additional integration into a customer's other line-of-business systems can be discussed and coordinated with the K2 Virtual Services team for fee-based assistance as well.
- Details of the Technical Support system – specifics on how to file a ticket, check on ticket status and how to work with the Technical Support team.
- Details on communication of Service updates from the Service Operations team.
- Details on preferred region deployment of the Service. Available regions are listed in the Service Regions section above.
- General use of the Service.

4.4.2. SERVICE TESTING

As part of establishing the Service, baseline testing of K2 Platform will be performed. This will create a benchmark against which operation of the Service will be compared following any Service changes, including Upgrades, outages, and additional configuration of additional integration points.

4.5. PLATFORM CONFIGURATION

To ensure platform reliability we will as part of the service install and configure monitoring tools.
By default, the Service includes maintenance of three (3) K2 server instances. See the Data Integration section for more information about included integration types.

4.6. OPERATIONS MONITORING

The Service includes automatic measurement and monitoring of the underlying infrastructure and network communication for the Service environment. Any monitoring outside of the Service infrastructure (such as network connectivity to the customer site, or availability of customer systems that integrate with the Service) is not included in the Service. Measurement and monitoring of application-specific performance metrics is not included.

Service Operations monitors system availability and will communicate any availability issues as soon as possible. System status, availability, performance and security notifications and issues will be posted via a Service status webpage.

4.7. PLATFORM ADMINISTRATION

Service administration tasks as necessary to address system instability or reliability issues. Administration of users, permissions, and customer applications are not included in these services.

4.8. PLATFORM TROUBLESHOOTING

We will work with customer and 3rd-parties, if needed, to identify issues affecting the K2 Platform. Where a problem is found in the K2 software, Service Operations will work with K2 Technical Support. Where a problem is found in the Service infrastructure, Service Operations will work with resources provided by the datacenter provider (“Datacenter Operations”) as appropriate. Where a problem is identified in the customer’s infrastructure – including network and integration points – Service Operations will notify customer of the findings, and provide suggested next steps, where possible.

Customer application troubleshooting is not included in these Services.

4.9. MAINTENANCE

The Service performs a variety of both scheduled and unscheduled maintenance tasks on the K2 Platform (See Service Availability below for more information). This includes Upgrades and Updates to the K2 Platform software, service restarts, K2 Platform configuration changes, etc.

In alignment with the K2 Product Support and Release Policy, Service Operations will perform one Upgrade per year, to keep the K2 Platform running on a fully supported software version. The Service includes application of Updates on a Quarterly basis, including cumulative updates and fix packs. If the customer encounters a critical issue resolved in a fix pack or codefix, Service Operations will install this fix according to a schedule agreed upon with the customer.

The Service does not maintain the underlying VM hosting the K2 Platform. Operating system patches, etc., are the responsibility of the customer.

4.10. SERVICE OPTIMIZATION

K2 aims to continually improve on and optimize the Service through regular reviews of operations and education of the Customer K2 Helpdesk team to improve communication, case triage and deflection.

4.11. SERVICE USAGE & REPORTING

The Service will provide regular reporting to the customer, through a combination of review meetings and self-service. This will ensure that you have full visibility into delivery of the Service.

4.11.1. WEEKLY

On a weekly basis, the ESM will provide you with a status report that gives an overall summary of the following:

- Platform health
- On-going activities
- Completed tasks
- Upcoming milestones and releases
- Bug fixes
- Risk identification and mitigation plan

4.11.2. MONTHLY

On a monthly basis, the ESM will meet with the customer’s business and/or technical contacts to review service delivery. This activity includes the following:

- Tracking unresolved issues from maintenance projects which impact service levels
- Updating maintenance project progress and resolving critical issues
- Capturing agreements and disagreements and items needing escalation

4.11.3. QUARTERLY

A quarterly review meeting will be through teleconference meeting session which will be booked in advance. This quarterly meeting will provide:

- Overall project status
- Issues list
- Service level review, including metrics reporting, supporting reasons for metrics deviation, and items needing adjustment within service levels (e.g., scope, metrics)

4.12. K2 API ACCESS

All standard supported APIs and K2 Cloud web-based APIs are included in the Service. Customers can reference these APIs when building custom applications to connect to the Service

4.13. TECHNICAL SUPPORT

Governed by the K2 Software Support Policies.

4.14. LIMITATIONS

You must have an active software and support subscription to be eligible for Site Reliability services.

Delivery of the Service is via remote/virtual access. The Service does not include any on-site visits or personnel.

The Service is not responsible for a customer’s network connections or for conditions or problems arising from, or related to, a customer’s network connections (e.g., bandwidth issues, excessive latency, network outages), or caused by the Internet. This includes any connectivity between the Service environment and any resources managed by the customer. Service Operations monitors network performance within the Service environment and will address any networking issues within the Service environment that may impact availability or latency.

K2 has no support obligations for issues resulting from: (I) your equipment, network connections or other infrastructure; (ii) your use of the K2 software in a manner not consistent with the K2 software documentation or in violation of the license agreement; (iii) modifications to K2 software by any party other than K2; or (iv) failures or downtime of the K2 software due to any factors beyond K2’s reasonable control or due to any force majeure event as described in your license agreement.

5. ADDITIONAL ADD-ON SERVICES

In addition to the standard scope of the Service defined above, the following optional add-ons can be purchased.

5.1. DISASTER RECOVERY ASSISTANCE

A Service subscription can include disaster recovery (DR) for the production environment. In the event of a disaster, the Service will restore availability of the K2 Platform. Depending on the level of service acquired, and the nature of the disaster, DR may take place in the same or a different geographic region from the customer's primary K2 Platform datacenter. The DR service operates in a cold standby model, where application server(s) are not available during normal operation. During recovery, the cold standby servers are brought online with a restored backup of the K2 application database.

Where such a service is provided, K2 will be responsible for the compute layer / application servers and the Customer Database team will take responsibility for the database.

NOTE	**The disaster recovery datacenter may not be geographically near a customer site, resulting in different latency responses from normal Service operations.**

After the primary datacenter has recovered from the outage, the cold-standby roles will be reversed (fail-back) and the customer can request a switch back to the original primary datacenter. Fail-back operations may involve backup and restore operations and could result in longer downtime compared to the fail-over downtime.

5.1.1. DATA BACKUP AND RESTORE STRATEGY

Data pertaining to the customer's configuration of the Service resides solely in the K2 database. This data can be backed up and should be stored remotely. This is the responsibility of the customer.

5.2. ADDITIONAL ENVIRONMENTS

Standard Service subscription includes three K2 instances, where a K2 instance is defined as a server running a K2 service instance that can be utilized at the client's discretion. Additional K2 instances can be added to the overall subscription.

5.3. CUSTOMER-INITIATED DATA RECOVERY

In the absence of a disruptive incident, the customer may request a point-in-time restoration of the K2 database. This is primarily used in the event of accidental modifications to applications or data running on the Service, which adversely affect customer operations. The customer's backup and recovery strategy (including backup frequency and retention policies) will dictate the maximum timeframe for such point-in-time restoration.

This customer-initiated data recovery is a fee-based (credit-based) service, and will require the Customer Database Administrator to work with Service Operations to complete.

5.4. DATA RESTORATION IMPACT INVESTIGATION

Restoring your Service database to an earlier point in time will likely result in some loss of data, including progress on workflow processing, development changes made to applications, and SmartBox data. K2 Virtual Services can be engaged to determine the impact of such a point-in-time data restoration.

This investigation is an hourly, fee-based service.

5.5. INSTALLATION AND CONFIGURATION OF K2 PLATFORM

The Service does not include installation and configuration of the K2 software. This requires a separate statement of work and will carry a separate fee. Included in the installation and configuration (if purchased) is a review of readiness for migration to private cloud architecture, network infrastructure preparedness and data integration compatibility. The K2 Platform software will be installed and configured on virtual servers provisioned by the customer according to best practices.

5.6. MIGRATION OF CUSTOMER K2 DATABASE TO AZURE

The Service does not include migrating a customer's existing K2 database to their Azure tenant. For customers with existing K2 on-premises environments, K2 Virtual Services can be engaged to migrate the existing K2 database to the customer's private Azure cloud tenant, and configure their K2 Platform environment to use this migrated database. This requires a separate statement of work and will carry a separate fee.

5.7. CONFIGURATION OF ADDITIONAL INTEGRATION POINTS

After initial Onboarding, the customer can configure additional integration points themselves, or can engage K2 Virtual Services to assist.

6. MEASUREMENT OF SERVICE DELIVERY

6.1. K2 PLATFORM AVAILABILITY

The Service is designed to be available to the customer 24 hours a day, 7 days a week, 365 days a year, except during system maintenance windows, unplanned downtime and as otherwise detailed below.

The Service offers customers 99% overall Service Availability within a calendar month. The Service is available when the customer is able to access the Service production environment.

6.1.1. K2 PLATFORM AVAILABILITY

Service Availability is measured as a "Monthly Uptime Percentage" and is calculated via the following formula:

$$\frac{[Total\ available\ minutes\ per\ month] - [Downtime\ minutes]}{[Total\ available\ minutes\ per\ month]} \times 100$$

6.1.2. TOTAL AVAILABLE MINUTES PER MONTH

Total available minutes per month is the total minutes during regional business hours in the applicable billing month less Scheduled Maintenance.

6.1.3. DOWNTIME MINUTES

Downtime minutes is defined as the total minutes in a billing month in which the Service is unavailable, excluding (i) Scheduled Maintenance or (ii) unavailability of the Service due to issues described in the Service Level Exclusions below.

6.1.4. SCHEDULED MAINTENANCE

Scheduled Maintenance events are planned, periodic updates, fixes or changes made by the Service to the K2 Platform environment. The majority of these maintenance tasks are performed without any impact on Service availability, but some maintenance tasks may require planned downtime. Service Operations will communicate any planned downtime to customers as per this Service Level Policy.

6.1.5. UNSCHEDULED MAINTENANCE

Unscheduled Maintenance events are considered unplanned, ad-hoc updates, fixes or changes made by Service Operations to address time-critical issues, and which require downtime. Additionally, any outages of the underlying third-party datacenter which may affect the quality of the Service generally or a customer's Service environment specifically may result in unplanned downtime.

In case of emergency maintenance or downtime, Service staff will make reasonable efforts to communicate the downtime to affected customers.

Notification Type	Notice Window	Notes
Scheduled Maintenance for Service version upgrades	10 Days	Customers will be notified in advance of planned Service version upgrades to allow for application testing against the new platform. Notifications will be sent to the primary customer contact for the Service.
Scheduled Maintenance (minor Service updates, not Service version upgrades)	3 Days	Service Operations will provide three days' notice of Scheduled Maintenance. Notifications will be posted via the Service Status page.
Unscheduled Maintenance	N/A	For broader Service outages that require unscheduled maintenance, the Service Status page will be updated. Customers should subscribe to updates via the Service Status page.

6.1.6. SERVICE LEVEL EXCLUSIONS

Unless specified otherwise, Service Availability applies only to a customer's Service production environment. Service Credits for overall Service Availability of non-Production environments are not offered.

Overall Service Availability does not include the following:

- A failure, degradation of performance or malfunction resulting from scripts, data, applications, infrastructure, software, penetration testing and/or performance testing directed, provided or performed by customer.
- Planned outages, scheduled maintenance, or outages initiated by Service Operations at the request or direction of customer for maintenance, deployment, configurations, backups or other purposes that require the Service to be temporarily taken offline.
- Interruption or shut down of the Service due to circumstances reasonably believed by Service Operations to be a significant threat to the normal operation of the Service, the operating infrastructure, the facility from which the Service is provided, and/or access to, or the integrity of customer data (e.g., a hacker or malware attack).
- Outages due to unsupported system administration, commands or changes performed by customer users or representatives.
- Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and other K2 vendors), and other force majeure events.

- Inability to access the Service or outages caused by the customer's conduct, including negligence or breach of the customer's material obligations under the Service, or by other circumstances outside of the Service's or K2 control.
- Lack of availability or untimely response time of the customer to respond to incidents that require customer participation for source identification and/or resolution.
- Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to customer conduct or circumstances outside of Service Operations' control.

6.2. SERVICE LEVEL REMEDY POLICY

Where the Service has not achieved the required 99% Service Availability service levels within a calendar month (as set out in Section 6.1), the customer will be entitled to a Service Credit of 10% of the monthly rate of the Service fee.

To receive a Service Credit, the customer must have opened a Technical Support Ticket for the availability issue, and the customer must notify the K2 Enterprise Service Manager within thirty (30) days of the end of the month in which the overall Service Availability was not met to provide the following:

- The Technical Support Ticket number
- A detailed description of when the Service was not available including duration of the downtime
- How the customer was affected
- Description of the steps the customer initially took to attempt to resolve the issue

K2 reserves the right to withhold a Service Credit if it cannot verify the downtime or if the customer cannot provide evidence that they were adversely affected as a result of the downtime.

A customer must be in compliance with all Policies in order to be eligible for a Service Credit. Customers in breach of the Policies, including payment obligations, are not entitled to a Service Credit.

Verified Service Credits will be added to the customer's Service account balance for use upon subsequent renewal. No refunds or cash value will be provided.

The total Service Credits payable to the customer in any month will not exceed thirty percent (30%) of the monthly Service fee.

7. DATA INTEGRATION

The Service natively provides the ability for customers to connect to data systems external to the Service as a means to integrate critical line-of-business systems into the applications that are being built utilizing K2 Platform. These connections – called SmartObjects – can be configured as standalone read, standalone write or bi-directional read-write connections and allow a customer to interact with data in the systems of record without importing data into and out of the Service for transient use within K2 Cloud applications. The data that is integrated via SmartObjects is not cached within the Service nor is it permanently stored in internal K2 Cloud data stores to ensure that customer data is always the most relevant version available.

K2 Platform offers integration with a wide variety of service types. For a list of available integration types, please see K2 Service Types in the product documentation.

8. SECURITY

K2 Platform is provisioned on customer infrastructure and will have a direct dependency on customer network security. It is critical that customers have reviewed and specifically locked down their on-premise to Azure tenant access in line with corporate standards and policies for data security.

Service subscriptions leverage the security features provided by the underlying infrastructure and system architecture. In addition, the Service constantly looks to improve security by applying new K2-based security features as they become available.

The Service has in place various procedural, administrative, technical, and physical safeguards to help protect subscriber accounts, K2 environments and data from loss, theft, misuse, abuse and unauthorized access, disclosure, alteration, and destruction.

NOTE	**K2 is providing a managed service on customer's infrastructure and customer's underlying security posture. As a result, K2 will not be held responsible for security breaches resulting from the use of K2 Platform.**

8.1. ACCESS CONTROL

8.1.1. SYSTEM AND APPLICATION ACCESS CONTROL, USER AND PASSWORD MANAGEMENT

Management access to underlying Service environments by Service Operations is restricted to authorized personnel only. Service Operations' access to customer's infrastructure is limited to remote connectivity only, secured with accounts controlled by Service Operations. The Service employs strong password policies wherever possible, including restricted access to authorized usernames and passwords. Service Operations staff will be able to access and manage the K2 infrastructure with role-specific permissions, limited to the requirements of managing the Service.

In the event Technical Support needs access to a Service environment for troubleshooting, read-only, time-limited database access may be granted for the explicit purpose of attempting to resolve an issue. Such access may include the ability to enable or disable logging and extract those logs for further review.

All access requests by either Service Operations or Technical Support will be logged for auditing purposes.

Customer resources will not be allowed to access the Service infrastructure. Administrative access to the Service by the customer will use the standard administration interfaces provided by K2 within the Service, and only when authorization is in place.

As the Service can integrate with third-party applications and data (such as Salesforce, Azure SQL, private and public web services, Microsoft SQL Server and others), integrating with these services may require additional, ad-hoc security and communication configuration based on the technology being integrated and the specific use case of the integration.

The customer is responsible for all end user and application administration within the Service environment. K2 does not own, control or manage the customer's end user accounts or applications in the Service environment. Customers may configure the environment and applications on the Service environment using K2's built-in security features, authorization protocols and administration tools. Customers are responsible for managing and reviewing access for their own employee accounts.

For details on specific authorization for Service environments, please refer to the Authorization section of these policies.

8.2. AUTHENTICATION

A Service environment will leverage the customer's Microsoft Active Directory infrastructure or other approved identity provider for authentication to ensure that only valid, authenticated users have access to the K2 environment. The Service does permit SmartForms Anonymous Access if desired. This access may be configured on request per the standard Anonymous Access configuration supported by K2 SmartForms.

NOTE	**In certain cases, non-AD credentials could be used to integrate with systems, such as when Basic, Static or OAuth Authentication Modes are used by SmartObjects to integrate with external systems. Such integration is the responsibility of the customer and not provided as a core feature of the overall Service.**

8.3. AUTHORIZATION

Authorization policies are applied to ensure that appropriate rights and permissions are in place to restrict access to Service resources and allow only the access that is required to achieve specific tasks. It is possible that certain application requirements may require additional permissions, or that ad-hoc authorization may be required to address issues in the environment.

The tables below describe the base-level authorizations that are applied in the Service.

8.3.1. SYSTEM ACCESS AND APPLICATION AUTHORIZATION

Virtual access to machines and access to supporting applications will be restricted to minimum permissions that will allow the infrastructure and applications to operate. The table below describes some machine and software authorizations that apply in a Service implementation.

Component	Permissions	Roles	Notes
Service underlying infrastructure and components	Access through Service administration interfaces	Service Operations Technical Support	Service Operations staff will have remote access to the Service environment and be able to perform administrative operations to the infrastructure. Technical Support may be allowed read-only database access to the customer environment for the express purpose of attempting to resolve a customer issue.

Component	Permissions	Roles	Notes
			Technical Support may enable/disable logging and export logs for review. All access requests by Service Operations or Technical Support are logged for auditing purposes. End users will not be allowed to access the Service infrastructure.
Customer's Microsoft Azure subscription and Microsoft Azure Services	Access through Microsoft Azure administration interfaces	Service Operations	Where required (K2) Service Operations will work with Customer Azure Administrators on customer's Microsoft Azure environment through Microsoft Azure administration interfaces.
	Microsoft Active Directory API access	K2 Platform	The Service utilizes a K2 Service Account to allow the Service to integrate with the customer's Microsoft Active Directory (AD) store and utilize these AD identities for authentication within the Service.
Customer servers	Administrative access	Service Operations	For customers that have established a direct connection between the Service and on-premises systems, Service Operations staff will not have access to customer servers or machines in the customer environment.
*K2 database**	Database administration and ownership	Service Operations Technical Support K2 Service Account	Service Operations will have administrative access to the K2 databases. Secure password management to enable shared credentials between K2 Service Operations and Customer Database Team will be required. Technical Support will have read-only access to the K2 databases. The K2 Service Account has the ability to interact with the K2 database as well.

*Core database administration is provided by the Customer Database Team.

8.3.2. INTEGRATION-SPECIFIC AUTHORIZATION

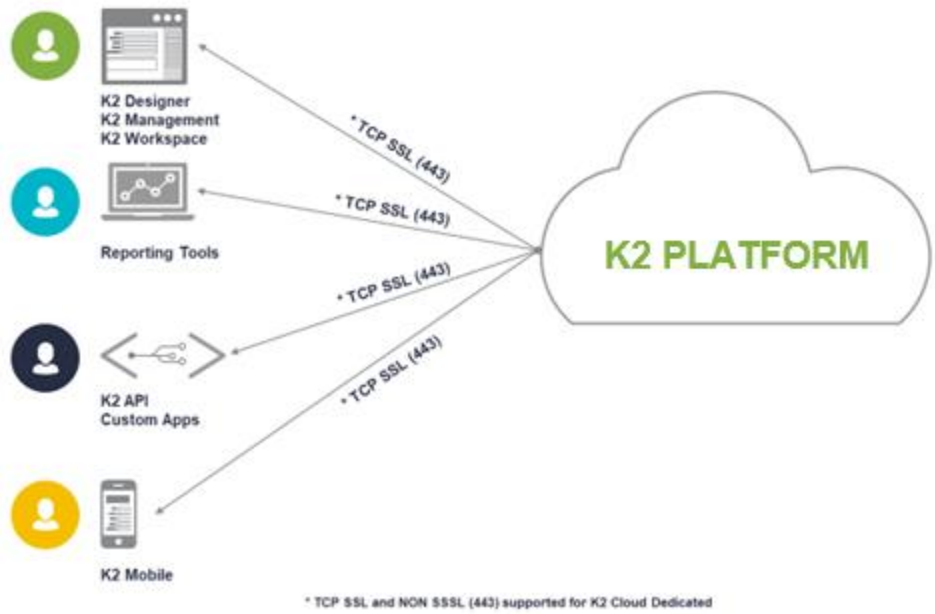
Integration with applications outside of the Service environment (such as interacting with cloud-based data providers or on-premises data sources) will be application-specific and subject to the particular requirements of the application. For example, some integration may leverage OAuth token flow. The target system can then apply authorization based on the credential used by K2 for integration. In all cases, the specific authentication mode and authorization applied will be established based on the application requirements and the infrastructure support. As such, it is not possible to provide integration-specific authorization information because the authorization necessary will depend on the integration.

8.4. NETWORK TRAFFIC SECURITY

Customers will connect to the Service via the following different primary mechanisms:

- Directly to Service tooling via a web browser
- By utilizing third party reporting tools
- Via customer-managed, custom applications
- Via a device-specific K2 mobile application (“K2 Mobile App”)

In each of these scenarios, traffic between the Service and the customer will travel over secure and encrypted TLS/SSL channels, except where connectivity occurs within a virtual or real customer network and such networks are protected from external access.



* TCP SSL and NON SSSL (443) supported for K2 Cloud Dedicated

Figure 1 - Network Security of connections to K2 Platform

8.4.1. DATA TRANSPORT ENCRYPTION

For customers that are connecting to systems external to the Service via SmartObjects, secured communication channels should be utilized whenever possible.

8.4.2. NETWORK AND FIREWALLS

All data communication within the Service environment (for example, communication between the K2 application servers and the K2 database) occurs within the underlying customer-protected network and does not touch the public Internet.

8.5. DATA SECURITY

The data stored in the Service itself is protected from unauthorized access with underlying data infrastructure security applied to logins and roles, based on the standard minimum-permission model applied by the Service. In addition, certain sensitive data such as cached credentials are stored in encrypted format in the K2 database for additional security.

8.5.1. PERSISTENT AND TRANSIENT DATA

The Service architecture is designed to securely retrieve or update data in real time from external systems. When communicating directly with an external system, SSL configuration is recommended for every connection between the Service and an external system; however, this is ultimately at the discretion of the customer when establishing connections. See Network Traffic Security section for additional details.

Although data flows directly from the external system through the Service to the client and is never permanently stored, the Service does make use of Microsoft SQL Server Common Table Expressions (CTEs) for internal operations such as SmartObject disparate data joins and normalization. A CTE is similar to a derived table in that it is not stored as an object and lasts only for the duration of the query.

NOTE

Customers should be aware that the database roles required for maintaining a K2 database means that Service Operations may have access to the data stored in the K2 SmartBox data stores. Service Operations is restricted from altering, deleting or extracting that data from the Service.

Any interaction Service Operations has with customer data stored within the Service is only initiated after a customer logs a Technical Support ticket to address a particular issue, and never without direct customer request and notification.

8.5.2. CUSTOMER DATA OWNERSHIP

K2 does not claim ownership of customer data in the K2 database. To obtain such stored data from the Service, a customer must initiate a request via the Technical Support ticket system indicating they would like to obtain such data. Technical Support will work with Service Operations to provide an extract of the data in a timely manner. More details are available in the Customer Data Ownership Rights section.

8.6. MOBILE DEVICE SECURITY

Communication between devices operating the K2 Mobile App and the Service environment will occur via the HTTPS-secured connection to the public-facing K2 web-service endpoints and websites.

Data for the K2 Mobile App is stored in a device-specific local database on the device and locally encrypted. Additionally, user credentials are encrypted using device-specific encryption capabilities. For specific details on K2 Mobile App Security, please refer to the K2 Mobile App Security page on help.k2.com.

8.7. SECURITY INCIDENT RESPONSE

While reasonable precautions are taken to secure Service environments from security threats and breaches, in any connected environment there is always a risk of security incidents that might originate from external or internal threats. The Service has in place certain teams, policies and procedures to deal with security incidents.

Security incidents that are not automatically detected by Service Operations can be reported through the normal support channels, or in case of emergency, contact security@k2.com.

8.7.1. COMPUTER SECURITY INCIDENT MANAGEMENT TEAM (CSIMT)

K2 has established a Computer Security Incident Management Team (CSIMT) to resolve Service security incidents. The table below describes the roles and responsibilities of the CSIMT:

Role	Responsibility
Technical Support Engineer	The Technical Support Engineer is the first line of support when reporting any security incidents and will initiate CSIMT responses.
Service Operations Manager	The Operations Manager will begin to isolate the incident and preserve any forensic evidence.
Service Chief Engineer	The Chief Engineer will work with the Operations Manager to determine the scope of the incident.
Service Security Analyst	Security Analysts will assist the Chief Engineer to better understand the nature and root cause of the incident.
Service Engineering Director	The Engineering Director owns the CSIMT process and works with all other team members to ensure the proper steps are followed and the incident is addressed and documented with appropriate action towards resolution.
General Counsel (GC)	This role is primarily responsible for overseeing legal and liability matters, including liaising with local, state and federal authorities.

8.7.2. INCIDENT RESPONSE PLAN

In the unlikely event of a security-related incident or breach, K2 has a system to report, contain, analyze, communicate and resolve security related incidents. This incident response plan outlines the roles and procedures in place for responding to security incidents involving the Service, infrastructure and systems. The plan does not cover security breaches within a customer's internal environment or other third-party environments connected or integrated into the Service.

1. Monitoring
   a. Service Operations actively monitors automated metrics for system level events and will investigate and report incidents accordingly.
   b. Service penetration tests are performed periodically and identified issues are addressed.

   c. Customers are encouraged to monitor for any unusual activity or behavior and report any suspicious or malicious events immediately by contacting Technical Support.
2. Incident Reporting and Escalation
   a. All security related incidents must be reported to Technical Support Engineers who will log the incident and begin primary investigation.
   b. If the primary investigation warrants escalation, the Technical Support Engineer will escalate to the Service Operations Manager, Service Chief Engineer and Service Engineering Director.
   c. Following investigation, if the incident is a valid security incident, the Security Team is notified and assists in the incident response.
3. Containment
   a. The Technical Support Engineer, Service Operations Manager and Service Chief Engineer will initiate an immediate lock-down procedure to contain the incident and preserve any forensic evidence.
   b. if additional help is required, outside forensic assistance may be utilized to assist in the investigation.
4. Analysis
   a. The Service Engineering Director will coordinate with all involved parties to analyze the extent of the incident.
5. Resolution
   a. The Engineering Director will determine next steps to resolution and if any Service change requests are needed.

9. CHANGE MANAGEMENT

Change control policies are in place to ensure that only approved and audited changes are applied to the Service environment. There are two main categories of change management, each with specific policies that are described further in this section.

9.1. SERVICE-INITIATED CHANGES

Service-initiated changes include those applied during Scheduled or Unscheduled Maintenance, and will be communicated as per the defined Service Level. For changes that will not affect Service availability or application stability, Service Operations will apply such changes without notice, but in all cases will retain history of changes applied for auditing purposes.

Service environments are subject to standard product updates provided by K2. For more information on K2 releases, please refer to K2 Product Release Strategy.

9.2. CUSTOMER-INITIATED CHANGES

9.2.1. CUSTOMER-INITIATED INFRASTRUCTURE CHANGES

Customer-initiated infrastructure changes may include:

- Changes to the Windows Operating Systems that run the K2 Platform
- Changes to the Microsoft SQL Server databases, licenses, patch levels or database upgrades.
- Changes to infrastructure that impact the K2 Platform including, but not limited to:
    - Security
    - Active Directory

- IIS
- Patches and updates
- Load balancing
- Microsoft Azure related components and infrastructure

These changes are done by customer resources responsible for these services and should be coordinated with Service provider staff to ensure that such changes are managed, well tested and implemented in a way to ensure minimum disruption to the service. K2 will not be held responsible for service disruption caused by customer-initiated changes to these components.

9.2.2. CUSTOMER-INITIATED PLATFORM CHANGES

Customer-initiated platform changes may include:

- Packaging applications from within a non-production environment
- Deploying applications into a production environment
- Configuring the Service

The Service will not allow customers to make changes to the standard Service environment through custom code or other unique customizations that would alter the standard functions of the Service.

The non-prod environment within the Service duplicates the production environment so that testing of applications in the non-prod environment is representative of the production environment (outside of applications developed and deployed within the production environment) and to facilitate easy migration between non-production and production environments.

10. ESCALATION

In case of Service interruptions, the escalation process will follow the standard incident management process. In case of any other issues not related to incidents or urgent situations (e.g. related to the delivery of the service in general, changing business requirements or others), the ESM should be contacted. Any escalation related to the service or service delivery should be escalated as follows:

UK, EMEA and APAC*

Title	Contact Details
K2 Site Reliability Incident logging	https://portal.k2.com/ticket/default
Enterprise Service Manager (ESM)	<Details to be provided, varies by customer>
Manager of K2 Enterprise Services	Theo Roos, Theo@k2.com
K2 Professional Services Director	Kevin Bryant Kevin.B@k2.com

*These contact details are subject to change.

North America*

Title	Contact Details

K2 Site Reliability Incident logging	https://portal.k2.com/ticket/default
Enterprise Service Manager (ESM)	<Details to be provided, varies by customer>
Manager of K2 Enterprise Services	Steve Barnard SteveB@k2.com
K2 Professional Services Director	Cesar Fernandez Cesar@k2.com

*These contact details are subject to change.