# Nintex Hosted Cloud Services

Service Policies

# TABLE OF CONTENTS



© 2024 Nintex USA, Inc.

© 2024 Nintex USA, Inc.

# 1 Introduction

Nintex Hosted Cloud Services provide Nintex software and supporting components as a service (the “Service”). This allows Nintex customers who prefer a “cloud first” strategy to license and use Nintex software, without the overhead of setting up, hosting and maintaining the Service's environments. Although Nintex provides the platform that enables customers to use Nintex software, the customer retains control over their Nintex product. For example, with Nintex RPA Cloud, customers continue to manage their robotic process automations and deployed RPA bots, whilst with Nintex K2 Cloud, customers retain control over the application development cycle and deployed applications.

This document describes the Service(s) and policies applicable to the Service(s) and is intended for anyone interested in researching and planning for the Service Offering(s). Note that, in this document, the terms “Service” and “Nintex Hosted Cloud Services” refer to the following (single tenant) offerings *only*:

- Nintex K2 Cloud
- Nintex RPA Cloud

The policies in this document do NOT cover other (multitenant) Nintex Process Platform cloud-based capabilities, such as Nintex Automation Cloud, Nintex Process Manager or Nintex DocGen®.

The Service(s) is provided under the terms of the Nintex Master Subscription Agreement (the “Subscription Agreement”), the applicable Order and the policies described within this document. These policies are subject to change at Nintex’s sole discretion; any material changes directly impacting customers will be communicated accordingly. The Service(s) as ordered by the customer will be governed by the policies in effect at the time the Service(s) was ordered for the period acquired. These policies are reviewed at least annually and may be revised to incorporate issue resolutions and process improvements.

As used in this document, the terms “Customer,” “Subscriber,” "you" and "your" refer to the individual or entity that has ordered the Service(s) from Nintex or an authorized distributor, as applicable.

© 2024 Nintex USA, Inc.

# 2 General Nintex Hosted Cloud Services policy

This section covers policies which are applicable across all Nintex Hosted Cloud Services. Where a policy only applies to some (but not all) of the hosted cloud services, this will be clearly stated.

*Note: Please also refer to the section on additional service policies for Nintex K2 Cloud, which contains policies **in addition** to the general policy covered here.*

## 2.1 Onboarding journey

This section describes the typical onboarding journey for new customers of Nintex Hosted Cloud Services.

1 **Information gathering**
Nintex's Customer Success Management team gather any customer-specific information, needed to start the onboarding journey and provision the Service environments. This may include key customer contacts, preferred service regions, naming conventions, etc.

2 **Service is made available**
The Nintex Hosted Cloud Services environment(s) are provisioned and made available for use by the customer's nominated Administrators, Developers and/or Business Analysts.

3 **Customer onboarding session**
The customer and Customer Success Management team complete an onboarding call that details:

- The specifics of the Service.
- Details of the Technical Support system – specifics on how to file a ticket, check ticket status and how to work with the Support team.
- Details on communication of Service updates from the Service Operations team.
- Typical use of the Service.
- Outline of training and learning & development needs.
- How Nintex and the customer can work together to meet goals and objectives set out in any statement of work (SOW). This only applies where Professional Services have been engaged by the customer and does not include any "custom" configuration of the service (such as using a different database service requested by the customer).

4 **Learning & development**
Where required, training sessions and hands-on workshops will be conducted with the customer to ensure they can leverage the features of the Service. This may incur an additional cost.

5 **Implement and scale**
Features of the Service (e.g., RPA automations or K2 applications) are designed, developed, deployed and optimized by the customer, and then scaled across the customer organization, as defined in the Order.

© 2024 Nintex USA, Inc.

| NOTE | **Onboarding timelines (and the order of events) may vary between products and depend on the scope and complexity of the customer. In general though, the onboarding journey follows the above and is roughly around 1-3 weeks for K2 Cloud and around 2 weeks for RPA.** |
|---|---|

### 2.1.1 Identity Provider and Other System Integrations with Nintex K2 Cloud

As part of the onboarding journey for Nintex K2 Cloud, the following will also be discussed during the "information gathering" stage:

- Integration of K2 Cloud with the customer's identity provider tenant. Details of this will be required prior to making the Service available.
- Integration of K2 Cloud with other line-of-business systems. Where cloud-to-on-premise secure connectivity (OPDA) or VPN tunnel configuration is required for K2 Cloud, these will be priced and quoted for separately.

## 2.2 Customer and Nintex roles

There are various roles involved in a Service subscription (on both the customer and Nintex side). Use the tables below to understand the role definitions for these.

### 2.2.1 Customer roles

All customers using Nintex Hosted Cloud Services will typically have the following roles:

| | |
|---|---|
| Customer Domain Users | Users within the customer's identity provider domain. Consider these the internal end users of the applications. |
| Customer Administrators | Customer resources who maintain the applications and application-specific components on the customer's production and non-production environments. Responsible for security review, environment readiness, architecture and infrastructure, and change management of the customer's own systems.<br><br>In the case of Nintex RPA, customer administrators also assist with hardware setup, software installation and permissions management on the customer's client machines. |
| Customer Network Administrators | Customer resources who maintain the customer's network and network infrastructure. |

In addition to the above, Nintex also recommends that customers have specific roles to assist with the successful operation of Nintex K2 Cloud and Nintex RPA Cloud. See the tables below for more details.

© 2024 Nintex USA, Inc.

#### 2.2.1.1 Additional customer roles for Nintex K2 Cloud

For Nintex K2 Cloud, customers should also have the following roles:

| | |
|---|---|
| Customer K2 Helpdesk | Customer resources that 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 K2 Cloud environments. These include no-code developers who may build applications with tools like K2 Designer as well as coding-developers who build applications that extend K2 Cloud or interact with K2 Cloud through the available APIs. |
| Customer Identity Provider Administrators | Customer resources who can administer the customer's identity provider environment. |
| Customer SharePoint Online Administrators | Customer resources who administer the customer's SharePoint Online environment. NOTE: SharePoint Online is not required to operate K2 Cloud and this role is only required if the customer requires integration into SharePoint Online. |

#### 2.2.1.2 Additional customer roles for Nintex RPA Cloud

For Nintex RPA Cloud, customers should also have the following roles:

| | |
|---|---|
| Customer RPA Business Analysts | Customer resources who define the RPA workflows to automate, choose the optimal automations to implement and build the automation pipeline for the customer's RPA team. Also provide general project management skills. |
| Customer RPA Developers | Customer resources responsible for creating the RPA workflows, testing them and deploying them into Production. They also adjust the RPA automations as needed, provide general maintenance of the automations and manage the RPA development environment. |
| Customer RPA Manager | Customer resource who produces the automation, assigns automations to Nintex RPA bots, prioritizes discovered processes for automation and manages the RPA operations cycle. |

### 2.2.2 Nintex roles

Nintex has the following roles to support Nintex Hosted Cloud Services:

© 2024 Nintex USA, Inc.

| | |
|---|---|
| Service Operations | Service resources who maintain the Nintex environment and associated infrastructure and provide support for operational issues. |
| Customer Success Manager | Service resource who acts as the customer's main liaison and contact person. |
| Service Onboarding | Service resources who assist during the customer onboarding phase. |
| Technical Support | Technical support services. |
| Professional Services | Consulting services. |
| Learning & Development | Learning and development team responsible for enabling, educating and empowering the customer. |
| Renewals | Renewal and licensing services. |
| Nintex | Refers to other internal Nintex roles and operations. |
| Datacenter Operations | Resources provided by the datacenter provider to maintain aspects like hardware and network infrastructure on the Service infrastructure. |
| Incident Response Team | Team which responds to and resolves security incidents. |
| Service Accounts | The identity of a service account. For example, in the case of K2 Cloud, this is the account under which the K2 service runs. |

## 2.3 Prerequisites and requirements

Prerequisites and requirements must be satisfied to subscribe to the Service(s). However, these vary from service to service:

- For Nintex K2 Cloud, see:
  - K2 Cloud prerequisites and requirements
- For Nintex RPA Cloud, see:
  - Nintex RPA Server Installation Checklist
  - Preinstallation/Upgrade
  - System Requirements – Server
  - System Requirements – Clients

© 2024 Nintex USA, Inc.

## 2.4 Nintex services

A Nintex Hosted Cloud Services subscription includes several services that, when combined, constitute the Service Offering(s). The following sections describe the included services, excluded services and services that will be available separately.

### 2.4.1 Included services

Services included as part of the service fee for all Nintex Hosted Cloud Services:

| Service | Description | Roles involved |
|---|---|---|
| Onboarding services | Nintex provides onboarding services to enroll in the Service.<br><br>Refer to the section called Onboarding Journey for more details. | **Nintex**<br>• Customer Success Manager<br>• Service Onboarding<br>• Service Operations<br><br>**Customer**<br>• Customer identity provider administrator<br>• Customer SharePoint Online Administrators (if integrated)<br>• Customer Administrators |
| Service setup and installation | Core infrastructure provisioning such as application servers, database servers, networking hardware, virtualization, operating systems, and applications needed to support the Nintex Hosted Cloud Services installation. | **Nintex**<br>• Service Onboarding<br>• Service Operations |
| Production Hosted Cloud Services environment | A production environment is made available to all Nintex Hosted Cloud Services customers.<br><br>Customers will access tooling via a web-based URL / smart client applications. K2 Cloud customers can use this tooling, for example, to design, build and deploy K2 applications and RPA customers can create automation content and manage robots. | **Nintex**<br>• Customer Success Manager<br>• Service Onboarding<br>• Service Operations<br><br>**Customer**<br>• Customer Administrators |

© 2024 Nintex USA, Inc.

| Service | Description | Roles involved |
|---|---|---|
| Non-production Hosted Cloud Services environment | Customers that require additional non-production environment/s will work with their Customer Success Manager to coordinate provisioning and accessing additional non-production environment/s.<br><br>Note that some customers may be entitled to a non-production environment based on their Order form, but additional non-production environment/s can also be requested (see Add-on and additional cost services). | **Nintex**<br>• Customer Success Manager<br>• Service Onboarding<br>• Service Operations<br><br>**Customer**<br>• Customer Administrators |
| Service planned maintenance | Scheduled core infrastructure maintenance such as hardware upgrades, operating system, and application version upgrades. | **Nintex**<br>• Service Operations<br>• Datacenter Operations |
| Service unplanned maintenance | Unplanned core infrastructure maintenance such as replacement of failed hardware or installation of critical operating system and application patches. | **Nintex**<br>• Service Operations<br>• Datacenter Operations |
| Nintex Hosted Cloud Services configuration | Configure the Nintex Hosted Cloud Services and supporting Nintex-provided technologies. | **Nintex**<br>• Service Operations |
| Operations monitoring | Quality-of-service monitoring to ensure the Service is performing to specification. | **Nintex**<br>• Service Operations |
| Nintex Service Health Dashboard | Customers have access to a Service<br><br>portal. | **Customer**<br>• Customer Administrators |
| Backup | Configure appropriate infrastructure and configuration-based backups. Where agreed, perform required data backups. | **Nintex**<br>• Service Operations |

© 2024 Nintex USA, Inc.

| Service | Description | Roles involved |
|---|---|---|
| High availability | Configuration of the Service's ability to operate continuously even with partial loss or failure of separate components. | **Nintex**<br>• Service Operations<br>• Datacenter Operations |
| Recovery | Restore available data via a customer request (see additional cost services) or due to an overall disruption in Service. | **Nintex**<br>• Technical Support<br>• Service Operations<br>**Customer**<br>• Customer Administrators |
| Disaster Recovery (DR) and Failover testing | Run failover and DR tests to verify backups are configured correctly and operational. | **Nintex**<br>• Service Operations<br>• Datacenter Operations |
| Infrastructure and Service environment troubleshooting | Troubleshooting issues in the core infrastructure and Service environment. Customer Application troubleshooting is not included in these services.<br><br>Troubleshooting integrations with customer environments (such as with their SharePoint or Azure tenants in the case of K2 Cloud) may require assistance from customer administrators (e.g. to grant consent). | **Nintex**<br>• Technical Support<br>• Service Operations<br>**Customer**<br>• Customer Administrators<br>• Customer Network Administrators |
| Service usage | Administer and report on licensed usage. | **Nintex**<br>• Renewals<br>**Customer**<br>• Customer Administrators |
| Requests and tickets | Online system to log requests and support issues. | **Nintex**<br>• Technical Support<br>**Customer**<br>• Customer Administrators |
| Technical Support | See the Technical Support section. | **Nintex**<br>• Technical Support |

© 2024 Nintex USA, Inc.

| Service | Description | Roles involved |
|---|---|---|
| Licensing costs | Service subscriptions will include specified licenses. Additional charges may apply for additional components and/or services.<br><br>Customers may acquire additional licenses as user counts or usage increase. | **Nintex**<br>• Service Operations<br>• Customer Success Manager<br>**Customer**<br>• Customer Administrators |

#### 2.4.1.1 Included services for Nintex K2 Cloud

In addition to the above, the following services are also included specifically for Nintex K2 Cloud:

| Service | Description | Roles involved |
|---|---|---|
| Promotion of applications | Ability for the customer to promote Service application elements (SmartForms, Workflows, SmartObjects, Services Definitions) between environments using K2 Package and Deployment tools. | **Customer**<br>• Customer Administrators<br>• Customer K2 Developers |
| Service security administration | Administer users and permissions for Forms, Workflows and SmartObjects. | **Customer**<br>• Customer Administrators<br>• Customer K2 Developers |
| K2 API Access | SmartObject OData API and Workflow REST API capabilities to interact with SmartObject data and expose that data to developers and third-party tools, and to manage workflows, workflow instances, events, and tasks<br><br>See: API Configuration. | **Customer**<br>• Customer K2 Developers |

#### 2.4.1.2 Included services for Nintex RPA

The following service is also included specifically for Nintex RPA:

© 2024 Nintex USA, Inc.

| Service | Description | Roles involved |
|---|---|---|
| Nintex Public API Access | The Public API for Nintex RPA allows customers / other applications to invoke / monitor the work of a Nintex RPA solution. It is used, for example, by customers of Nintex Automation Cloud to invoke Nintex RPA bots within a workflow.<br><br>For more details on the Public API, see here. | **Customer**<br>• Customer RPA Developers |

### 2.4.2 Add-on and additional cost services

Some services may incur additional costs. The costs of these "add-ons" will be defined in the customer's Order. Examples include (but are not limited to) the following:

| Service | Notes |
|---|---|
| Troubleshooting | Nintex provides reasonable scope for assisted troubleshooting. Issues deemed beyond reasonable scope may require paid assistance through Nintex professional services. |
| Customer-initiated data recovery | Customer-initiated requests (via a Technical Support ticket) to restore (where possible) data from a Nintex managed backup. Data is only available within 14 days of the current date for K2 Cloud, and within 8 days for RPA. |
| Investigation of impact of data restoration | Some Nintex Hosted Cloud Services act as middleware and interact between various systems based on workflow tasks, escalations or other mechanisms. Restoration and re-activation of restored workflows, for example, might cause unexpected issues, such as duplicated transactions in other systems or re-escalations. As these issues may be solution-specific, Nintex professional services can be engaged to investigate the impact of restoring a Nintex Hosted Cloud Services database to a specific point in time. |
| Configuration of additional integration points | Nintex professional services can help configure integration points and functionality not part of the standard onboarding process. |
| Additional production and non-production instances | Additional production and non-production instances can be provisioned within the current environment. Please speak with Nintex Sales. |

© 2024 Nintex USA, Inc.

| Service | Notes |
|---|---|
| Configuration of additional network infrastructure | Customers that desire to connect Service environments to on-premises systems via special network infrastructure (such as VPN, in the case of K2 Cloud) are responsible for obtaining all related network infrastructure and configuration. The Service Operations team will assist in “last mile” connection to the Service.<br><br>Customers will be responsible for the external network infrastructure costs and any additions to the base Service infrastructure. |
| Implementation of customer use cases | Customers will be responsible for the actual development and implementation of their use cases (e.g. development of RPA automations or K2 Cloud applications). Nintex professional services can be engaged to assist. |

### 2.4.3 Excluded services

Services which are not provided include (but are not limited to) the following:

| Service | Notes |
|---|---|
| Identity provider configuration and setup | Service Onboarding will provide Nintex Hosted Cloud Services requirements, instructions and policies for setting up integration with the customer’s identity provider. The customer is responsible for connecting and liaising with their identity provider. |
| Application testing | Nintex undertakes new feature and upgrade testing through a range of scenarios. The nature and flexibility of the services provided necessitates that the customer takes responsibility for acceptance testing for new features and upgrades within their unique environment. |
| Third Party product integration | Integration with any third-party system not included in the Data Integration Options section is the customer's responsibility. |

### 2.4.4 Service regions

The table below shows a list of regions in which Nintex Hosted Cloud Services operate:

| | United States of America | Ireland | United Kingdom | Netherlands | Canada | Singapore | Australia | South Africa | United Arab Emirates |
|---|---|---|---|---|---|---|---|---|---|

© 2024 Nintex USA, Inc.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Nintex K2 Cloud** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **Nintex RPA** | ✓ | ✓ | | | ✓ | ✓ | | ✓ | |

**NOTE** **Customers are responsible for validating that they can legally operate in the available third-party datacenter regions. Customers should also be aware that both Datacenter Operations and Technical Support may operate in a country other than the datacenter location.**

## 2.5 Service availability

All Nintex Hosted Cloud Services are 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.

### 2.5.1 Overall service availability

A Service is available when the customer is able to access the production environment which hosts the Service.

**NOTE** **Nintex Hosted Cloud Services offer customers a 99.6% Overall Service Availability within a billing month. This includes Nintex K2 Cloud and the *high availability* version of Nintex RPA ONLY.**

**This high availability RPA environment is optional and incurs additional cost. Customers who wish to have a highly available RPA environment should contact Nintex Sales.**

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

$$\frac{Total\ available\ minutes - Downtime\ minutes}{Total\ available\ minutes} \times \frac{100}{1} \quad X \quad 100$$

© 2024 Nintex USA, Inc.

### 2.5.2 Total available minutes per month

Total available minutes per month is the total minutes in the applicable billing month less Scheduled Maintenance.

### 2.5.3 Downtime minutes

Downtime minutes are 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.

### 2.5.4 Maintenance notifications

Scheduled maintenance events are *planned* updates or fixes to the Service environment. Unscheduled maintenance events are *unplanned*, ad-hoc updates or fixes, typically to address time-critical issues. Although most of these maintenance tasks are performed without impact on Service availability, some may affect availability for a brief period.

Notifications for maintenance tasks will be posted via the Service Status page. Customers should subscribe to updates on this page to be kept informed. Note that:

- The target notification window for scheduled maintenance is 3 calendar days for minor updates and 10 calendar days (about 1 and a half weeks) for major updates (such as major Service version upgrades).
- Unscheduled or emergency maintenance updates, which will result in downtime, will be notified whenever reasonable.
- For isolated incidents within customer-specific tenants, Service Operations will make all reasonable efforts to communicate the downtime directly to affected customers.

### 2.5.5 Service level remedy policy

When Overall Service Availability of 99.6% is not met in a given subscription month, Nintex, after confirming the nature and accuracy of the availability issue, may credit the customer's account up to 10% of the monthly portion of the annual Subscription fee amount ("Service Credit"). This only applies to Nintex K2 Cloud and the *high availability version* of Nintex RPA.

To receive a Service Credit, the customer must have opened a Technical Support Ticket for the availability issue, and the customer must notify the Customer Success Manager associated with the customer's Service within thirty (30) days of the Overall Service Availability not being met to provide the following:

- The support case 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

© 2024 Nintex USA, Inc.

Nintex 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 comply with the Subscription Agreement to be eligible for Service Credits. Customers in breach of the Subscription Agreement, including payment obligations, are not entitled.

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.

### 2.5.6 Service level exclusions

The Overall Service Availability applies only to a customer's Service production environment.

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.
- Outages caused by third-party services, such as a customer's identity provider.
- Planned outages, scheduled maintenance, or outages initiated by Service Operations at the request or direction of customer for maintenance, activation of configurations, backups or other purposes that require the Service to be temporarily taken offline.
- Interruption or shut down of the Service due to circumstances 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 are 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.
- 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 Nintex 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 Service Operations' or Nintex 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.

### 2.5.7 Network bandwidth and latency

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

© 2024 Nintex USA, Inc.

Service environment and will address any networking issues within the Service environment that may impact availability or latency.

## 2.6 Technical support

Standard Technical Support is provided as part of Nintex Hosted Cloud Services. Additional premium support is available for separate fees. The Technical Support Policy for Nintex Hosted Cloud Services is available for review here: https://www.nintex.com/customer-success/nintex-customer-support/.

## 2.7 High-level architecture

Refer to the following links for an overview of the high-level architecture for:

- Nintex K2 Cloud
- Nintex RPA

## 2.8 Security

Security of customer data and applications is of utmost importance to Nintex. Service subscriptions leverage the security features provided by the underlying infrastructure and system architecture. In addition, Nintex Hosted Cloud Services constantly look to improve security by applying new security features as they become available.

All Nintex Hosted Cloud Services have in place various procedural, administrative, technical, and physical safeguards to help protect subscriber accounts, Nintex environments and data from loss, theft, misuse, abuse and unauthorized access, disclosure, alteration, and destruction.

### 2.8.1 Access control

#### 2.8.1.1 System hardening

As part of the onboarding process and ongoing maintenance, all Nintex Hosted Cloud Services employ standardized system-hardening practices such as restricting access, removing or disabling unnecessary software and services, removing unnecessary user accounts, setting up network security, patch management, and logging.

#### 2.8.1.2 System and application access control

Access to underlying Service environments by Services Operations is restricted to authorized personnel only. Service Operations' access to Service infrastructure is limited to remote connectivity only, secured with accounts controlled by Service Operations. Nintex Hosted Cloud Services employ strong password policies and restrict access to authorized users only. Service Operations staff will be able to access and manage the Nintex infrastructure with role-specific permissions, limited to the requirements of managing the Service(s).

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

© 2024 Nintex USA, Inc.

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(s) by the customer will use the standard administration interfaces provided by Nintex within the Service(s), and only when authorization is in place.

The customer is responsible for all end user and application administration within the Service environment. Nintex does not own, control or manage the customer's end user accounts or applications in the Service environment. 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.

### 2.8.2 Infrastructure security

Nintex utilizes the Microsoft Azure and AWS platforms to deliver its services. Access is restricted to authorized members of the Service Operations team via the Azure/ AWS Management portal and its associated security mechanisms. Authorized Service Operations team members utilize secure account credentials including multifactor authentication to log into Azure / AWS Management Portals.

### 2.8.3 Authentication

The following sections detail the authentication aspects of specific Nintex Hosted Cloud Services.

#### 2.8.3.1 Nintex K2 Cloud authentication

The K2 Cloud Service environment will leverage one of the following provider types:

- Microsoft Azure Active Directory (AAD)
- Other OpenID Connect and SCIM providers, such as Google, Okta, PingFed and OneLogin

The Service also permits Anonymous Access for its K2 SmartForms.

| NOTE | **In certain cases, non-AAD credentials such as Basic, Static or OAuth Authentication Modes could be used, for example leveraging K2 Cloud SmartObjects integrating with external systems. Configuration and management of non-AAD credentials is the responsibility of the customer.** |
|---|---|

#### 2.8.3.2 Nintex RPA authentication

Nintex RPA leverages the Aerobase Identity Provider and Multi-Factor Authentication (based on RedHat Keycloak). Refer to the following for more details:

- Aerobase Identity Provider
- Authentication and Authorization Policy

© 2024 Nintex USA, Inc.

### 2.8.4 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 / temporary authorization may be required to address issues in the environment. Nintex will not make any authorization changes without prior notification, and subject to the customer raising a Technical Support ticket.

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

#### 2.8.4.1 System access and application authorization

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 to Nintex Hosted Cloud Services.

| **Securable Component** | **Access** | **Roles** | **Notes** |
|---|---|---|---|
| Service underlying infrastructure and components | Access through Service administration interfaces | Service Operations<br><br>Technical Support | Service Operations staff will have remote access to the Service environment and be able to perform administrative operations to the infrastructure.<br><br>Technical Support may be allowed read-only, temporary database access to the customer environment for the express purpose of attempting to resolve a customer issue.<br><br>Technical Support may enable/disable logging and export logs for review.<br><br>All access requests by Service Operations or Technical Support are logged for auditing purposes.<br><br>Customer users will not be allowed to access the Service infrastructure. |
| | Access through customer's cloud | Service Operations | For customers utilizing a cloud provider (e.g., Microsoft Azure or |

© 2024 Nintex USA, Inc.

| | | | |
|---|---|---|---|
| Customer's cloud provider | provider administration interfaces | | Amazon Web Services), Service Operations will not have any access to the customer's cloud environment through any of the cloud provider's administration interfaces. |
| | Microsoft Azure Active Directory API access *(Nintex K2 Cloud only)* | K2 Service Account | For Nintex K2 Cloud customers utilizing the native Azure AD integration, K2 Cloud utilizes a service account to allow it to integrate with the customer's Microsoft Azure AD (AAD) store and utilize these AAD identities for authentication.<br><br>Consent for K2 Cloud to access a customer's Microsoft Azure AD tenant will be granted by the customer's Microsoft Azure AD Tenant Administrator during the Service onboarding. |
| Identity provider services *(Nintex K2 Cloud only)* | Identity provider access | K2 Service Account | In the case of Nintex K2 Cloud, the Service can utilize SCIM to push identities from the customer's identity provider into the Service; however, via this setup the Service does not have the ability to pull identities into 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. |

© 2024 Nintex USA, Inc.

| | | | |
|---|---|---|---|
| Nintex databases | Database administration and ownership | Service Operations<br><br>Technical Support<br><br>Nintex Service Accounts | Service Operations will have administrative access to Nintex databases.<br><br>Technical Support will have read-only access to Nintex databases.<br><br>Nintex Service Accounts have the ability to interact with Nintex databases as well. |

#### 2.8.4.2 Integration-specific authorization

Integration with third-party applications (such as the customer's other cloud-based data providers or on-premises data sources) will be subject to the particular requirements of each application. As such, Nintex cannot provide any authorization details about these third-party integrations. Customers should consult their third-party application vendors for more information.

### 2.8.5 Network traffic security

For details on network traffic security for specific Nintex Hosted Cloud Services, refer to:

- K2 Cloud network traffic security3.3.1 for Nintex K2 Cloud.
- Network Security for Nintex RPA.

### 2.8.6 Data security

For details on data security for specific Nintex Hosted Cloud Services, refer to:

- K2 Cloud data security for Nintex K2 Cloud.
- Data Privacy & Segregation, Encryption and Data Retention for Nintex RPA.

The sections below cover general policies around backup data and customer data ownership.

#### 2.8.6.1 Backup data

Customer application data, system configuration data and underlying Service database and database backups are securely stored as part of the Service High Availability capabilities.

#### 2.8.6.2 Customer data ownership

Customers retain ownership of, and responsibility for, the data and other content they enter while using Nintex Hosted Cloud Services. Where a customer requires a copy of any of their production data held by the Service(s), Nintex requires a written request (via a Technical Support ticket). Nintex will work in good faith to arrange a copy of the data which may require the customer to arrange specialized data storage and additional fees.

© 2024 Nintex USA, Inc.

### 2.8.7 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. Nintex has teams, policies and procedures in place to respond appropriately to security incidents.

Any security incidents detected by the customer can be reported to Nintex via Nintex Technical Support.

#### 2.8.7.1 Incident Response Team (IRT)

Nintex establishes an IRT to resolve Service security incidents. All IRT members shall attend security training at least annually. The table below describes the roles and responsibilities of the IRT:

| Role | Responsibility |
|---|---|
| **Incident Response Lead** | Responsible for coordinating the overall response and recovery activities performed by the IRT. |
| **Technical Incident Manager** | Responsible for coordinating the Technical Incident Resolution Team and managing the technical aspects of the incident. |
| **Incident Communications Manager** | Responsible for coordinating overall communications within IRT and to other affected parties. |
| **Incident Technical Resolution Team** | Responsible for coordinating the technical troubleshooting efforts and engagement with any technical vendors or external providers. |
| **Compliance Team** | Responsible for activating the IRT for Severity 1/2 incidents and ensuring that relevant regulatory and legal requirements are considered during the resolution of incidents. |
| **Legal Representative/Team** | Responsible for ensuring that the IRT acts in compliance with federal and state laws and regulations for responding to incidents that shall expose Nintex to legal liability. |
| **Communications Team** | Responsible for working with the Incident Communications Manager and Technical Incident Manager to manage customer communications during the incident if there is an impact to the customer. |

© 2024 Nintex USA, Inc.

#### 2.8.7.2 Incident Response Plan (IRP)

Nintex has an IRP in place for all Nintex Hosted Cloud Services. The plan describes team structure, roles and responsibilities, activation criteria, communication expectations and the overall process, which involves:

- Discovery
- Containment
- Investigation
- Communication
- Mitigation
- Review

### 2.8.8 Security certificates and details

Nintex is committed to maintaining the security of our hosted cloud services. Below are the relevant compliance and certification programs in place.

#### 2.8.8.1 ISO 27001:2013

ISO 27001:2013 is a widely accepted set of international standards relating to the secure management of information, particularly in a cloud-based environment. Nintex Hosted Cloud Services have been independently verified to meet all ISO 27001:2013 standards for cloud security and information management.

#### 2.8.8.2 ISO 27701:2019

ISO 27701:2019 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). Nintex RPA Cloud has been independently verified to meet all ISO 27701:2019 standards for privacy information management.

#### 2.8.8.3 SOC 2 Type 2

Nintex's System and Organization Controls (SOC) 2 report provides assurances that there are controls in place that protect your data. Nintex has SOC2 Type 2 and SOC3 reports that support Nintex K2 Cloud and Nintex RPA Cloud. A copy of our latest SOC2 Type 2 report can be obtained by raising a Technical Support ticket.

## 2.9 Business continuity

The following section details disaster recovery capabilities of Nintex Hosted Cloud Services.

### 2.9.1 Definitions

#### 2.9.1.1 Incident

An incident refers to any single event or any set of events that result in downtime.

© 2024 Nintex USA, Inc.

#### 2.9.1.2 Disaster

For this policy's purposes, a disaster is defined as an unplanned event or condition that causes a complete loss of access to the customer's production Service environment.

#### 2.9.1.3 Recovery Point Objective (RPO)

RPO is commonly defined as the maximum amount of data (measured in time), which can be lost after a disruptive event occurs, which an organization deems to be acceptable. This is typically the time between a data backup and when a disruptive event has happened.

#### 2.9.1.4 Recovery Time Objective (RTO)

RTO is the maximum loss of availability following a disruptive event measured by the maximum amount of time before the application fully recovers.


*Figure 1* -1 *Visual representation of RPO and RTO*

### 2.9.2 High availability and redundant infrastructure

The Nintex K2 Cloud environment is built on redundant and resilient infrastructure, designed to maintain high levels of availability and provides the ability to recover the Service in the event of a significant disaster or disruption.

K2 Cloud production environments feature high availability architectures to ensure that failure of a single node will not affect production availability. These same capabilities are optionally available for non-production environments for separate fees.

#### 2.9.2.1 Network

Network infrastructure is duplicated where possible (e.g., duplicate NICs) as per the third-party datacenter provider's policies, or otherwise virtualized for rapid replacement.

#### 2.9.2.2 Application servers

Application servers are load-balanced and redundant, so that a failure of all but one application server will not result in system downtime.

#### 2.9.2.3 Database servers

Database storage is continuously backed-up and can be restored to a point-in-time.

© 2024 Nintex USA, Inc.

**NOTE** **In the case of Nintex RPA, a high availability environment is optional and incurs additional cost. Customers who wish to have a highly available RPA environment should contact Nintex Sales.**

### 2.9.3 Disaster recovery and data restoration strategy

The Service maintains internal business continuity plan (BCP) and disaster recovery (DR) policies in support of certifications such as ISO27001:2013.

A Service subscription includes disaster recovery (DR) for the production environment which is intended to provide Service restoration in the event of a major disaster, as declared by the Service.

Data restoration is available in the event of a DR event or upon customer request.

**NOTE** **The disaster recovery datacenter may not be geographically close to a customer site and may incur different latency responses from the Service.**

#### 2.9.3.1 Service level – failover and disaster recovery

| Item | Target Response Objective | Notes |
|---|---|---|
| Recovery Time Objective (RTO) | Within 48 hours after DR event | This refers to the time necessary to restore a Service following a disruption event. |

#### 2.9.3.2 Data backup and restore strategy

Data pertaining to the customer's configuration of a Service resides solely in the Nintex Hosted Cloud Services databases and is natively backed-up.

Should a database restore be required (either due to a DR event or following customer-initiated request for restoration), the restore operation can be initiated by submitting a Technical Support request. Details about the impact of a database restore within a customer's tenant can be discussed with the Customer Success Manager and/or Technical Support Engineer as needed.

#### 2.9.3.3 Service level – data backup

| Item | Target Response Objective | Notes |
|---|---|---|

© 2024 Nintex USA, Inc.

| | | |
|---|---|---|
| Recovery Point Objective (RPO) | 1 hour or less | Nintex Hosted Cloud Services databases, which contain Nintex configuration data as well as any data stored by the customer, can be restored to any restore point within 14 days for K2 Cloud and 8 days for RPA Cloud.<br><br>Restoration of data is also subject to the Database RTO Service Level detailed above. |
| Data backup restoration period | K2 Cloud: 14 days of backup data<br><br>RPA Cloud: 8 days of backup data | For Nintex K2 Cloud, retention of last 14 days of the underlying database backups. Database restores can revert backups to any restore point within 14 days.<br><br>For Nintex RPA Cloud, retention of last 8 days of the underlying database backups. Database restores can revert backups to any restore point within 8 days.<br><br>Restoration of data is subject to the Database RTO and RPO Service Levels. |

### 2.9.4 Measurement and monitoring

The Service(s) include 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 constantly and will communicate any availability issues as soon as possible. System status, availability and performance notifications and issues will be posted via a Service status webpage.

Service Operations also internally monitors various environmental performance, usage and stability metrics. While these metrics are not shared with customers, they do provide monitoring and fault identification capabilities to Service Operations and are a key tool utilized to make sure that a customer's environment is stable, available and performant.

## 2.10 Change management

Change control policies are in place to ensure that only approved and audited changes are applied to each Service environment. There are two main categories of change management.

© 2024 Nintex USA, Inc.

### 2.10.1 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 changes without notice, but in all cases, will retain history of changes applied for auditing purposes.

#### 2.10.1.1 Nintex software updates

Nintex will periodically release product updates to its hosted cloud services. For more information, please refer to:

- Nintex K2 Cloud Product Support and Release Strategy
- Nintex RPA Support and Release Strategy

#### 2.10.1.2 Staggering Nintex software updates

Customers can request a delay in scheduled service-initiated changes of a production environment to allow for testing in associated non-production environments prior to the update of their corresponding production environment by coordinating with their Customer Success Manager. A production environment service-initiated change can be delayed by a maximum of five business days.

For customers that have both a production and development environment, both environments must be updated to the same version within a given Service update period.

**NOTE** **It is important to note that, for K2 Cloud, the migration of solutions between non-production and production environments via the K2 Package and Deployment (P&D) tool will not be possible during the duration of this delay.**

A production Nintex Hosted Cloud Services environment can only be delayed further in cases where an issue is discovered during regression testing of a customer non-production environment that would introduce the same issue within production.

**NOTE** **There are certain circumstances in which delaying the upgrade of an environment cannot be scheduled – for K2 Cloud, specifically, when multiple environments share either a Microsoft Azure Active Directory tenant and/or a Microsoft SharePoint Online tenant. A change to either of the K2 apps associated with these types of tenants will render other connected tenants potentially problematic; all tenants that share resources such as these should be upgraded at the same time.**

### 2.10.2 Customer-initiated changes for Nintex K2 Cloud

Nintex K2 Cloud will not allow customers to make changes to a standard Service environment through custom code or other unique customizations that would alter the standard functions of the Service.

© 2024 Nintex USA, Inc.

The non-production environment within K2 Cloud 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.

## 2.11 Acceptable use policy

Use of Nintex Hosted Cloud Services is conditioned on Nintex's Customer Use Policy. Refer to this policy for more information.

## 2.12 Suspension and termination policy

### 2.12.1 Termination of service

Nintex will retain customer production and non-production data including back-ups (if any) up to thirty-five (35) calendar days after termination or expiration, after which the data will be deleted and is not recoverable. Data will not be made recoverable for customer non-production environments. A customer (via a Technical Support ticket) can request deletion prior to the 35-day limit.

Please also see the "Customer data ownership" section for information on obtaining a copy of production data.

### 2.12.2 Suspension of service

Nintex may temporarily suspend customer access to, or use of the Service(s) if the customer or users acting on behalf of the customer violate any provision of the Subscription Agreement or these policies, or if in Nintex's reasonable judgment, the Service(s) or any component thereof have or, are about to suffer a significant threat to security or functionality. Service Operations will make reasonable efforts to provide advance notice to customers of any such suspension and to promptly re-establish the affected Service(s) once the issue has been remedied.

### 2.12.3 Customer data ownership rights

Each customer retains ownership of its data residing in the Service databases. Nintex has no ownership rights to such customer data.

One exception is that Nintex shall retain the right to collect usage telemetry data, such as the number of attended vs unattended bots, number of scripts built, or the average number of wizards run by a robot per day. This will be used for diagnostic, operational, performance, analytics, and product improvement purposes only.

© 2024 Nintex USA, Inc.

# 3 Additional Nintex K2 Cloud service policies

This section covers policies which are specific to the Nintex K2 Cloud offering. These policies are *in addition to* those described in the General Nintex Hosted Cloud Services policy.

## 3.1 K2 Cloud prerequisites and requirements

The following prerequisites and requirements must be satisfied to subscribe to the K2 Cloud Service.

- The Service requires the customer provide one of the following to provide authentication of users:
  - A supported identity provider (IdP) that conforms to the following identity specifications:
    - OpenID Connect
    - System for Cross-domain Identity Management (SCIM) 2.0
  - One of the following Microsoft Azure Active Directory editions:
    - Free
    - Basic
    - Premium P1
    - Premium P2

  It is important for the customer to validate the edition of the identity provider they provide will work for their authentication needs and to plan for it to be incorporated with the Service.

- For customers integrating K2 Cloud with an Azure AD tenant:
  - If a customer is utilizing both on-premises Active Directory (AD) and Azure Active Directory (AAD); the customer's AAD environment must be synchronized with the organization's on-premises AD domain.
  - Customers will be required to deploy the "K2 for Office 365" app into their AAD tenant to facilitate the authentication of users within the Service. The "K2 for Office 365" app requires read-only permissions within a customer's AAD environment.
  - Using a dedicated AAD service account for the K2 integration into AAD is highly recommended.
    - This account should be assigned Global Administration permissions.
    - The Service account must have an allocated mailbox through the appropriate O365 license plan. K2 Cloud administrative notifications, including service status updates and consent expirations, will be sent to this email account. Email forwarding from this account to the K2 Administrators role is highly recommended so that critical notifications are not missed.
  - For customers requiring the ability for the Service to create/update/delete information within AAD, an additional "AAD for K2 Management" app must be installed and configured within the AAD tenant; this will require the customer to consent to granting K2 "write" capability within the customer AAD tenant.

- For customers integrating K2 Cloud with a SharePoint Online tenant:
  - An O365 subscription that supports third-party developed apps being deployed into the customer's tenant is required.
  - An O365 subscription, which contains SharePoint Online within the SKU, is required.

© 2024 Nintex USA, Inc.

- The account used during the registration of K2 and SharePoint Online must have Global Administrator rights in Office 365, to grant consent between the “K2 for SharePoint” app and SharePoint Online.
- Site Collection Administrator rights in SharePoint Online are required to add the “K2 for SharePoint” app to the SharePoint Online App Catalog and SharePoint Site Collections.

**NOTE** **Customers are required to utilize a valid identity provider for authentication and authorization within a K2 Cloud Service subscription. On-premises-based Microsoft Active Directory will not meet the requirements of the Service and can only be utilized if serving as a source for user credentials to be synchronized with given identity providers.**

## 3.2 K2 Cloud data integration

Nintex K2 Cloud provides the ability for customers to connect to data systems external to K2 Cloud. These connections known as SmartObjects can be configured either as standalone read / write or bi-directional read-write connections.

A list of out-of-the-box SmartObject integrations can be found here. Additional external data sources can also be configured. If this is required, please contact Nintex professional services.

## 3.3 K2 Cloud security

This section covers security-related policies specific to Nintex K2 Cloud. Note that these are *in addition to* the security policies covered in the general Security section.

### 3.3.1 Network traffic security

Customers will connect to the Nintex K2 Cloud Service:

- 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

In each of these scenarios, traffic between the Service and the customer will travel over secure and encrypted TLS/SSL channels.

© 2024 Nintex USA, Inc.

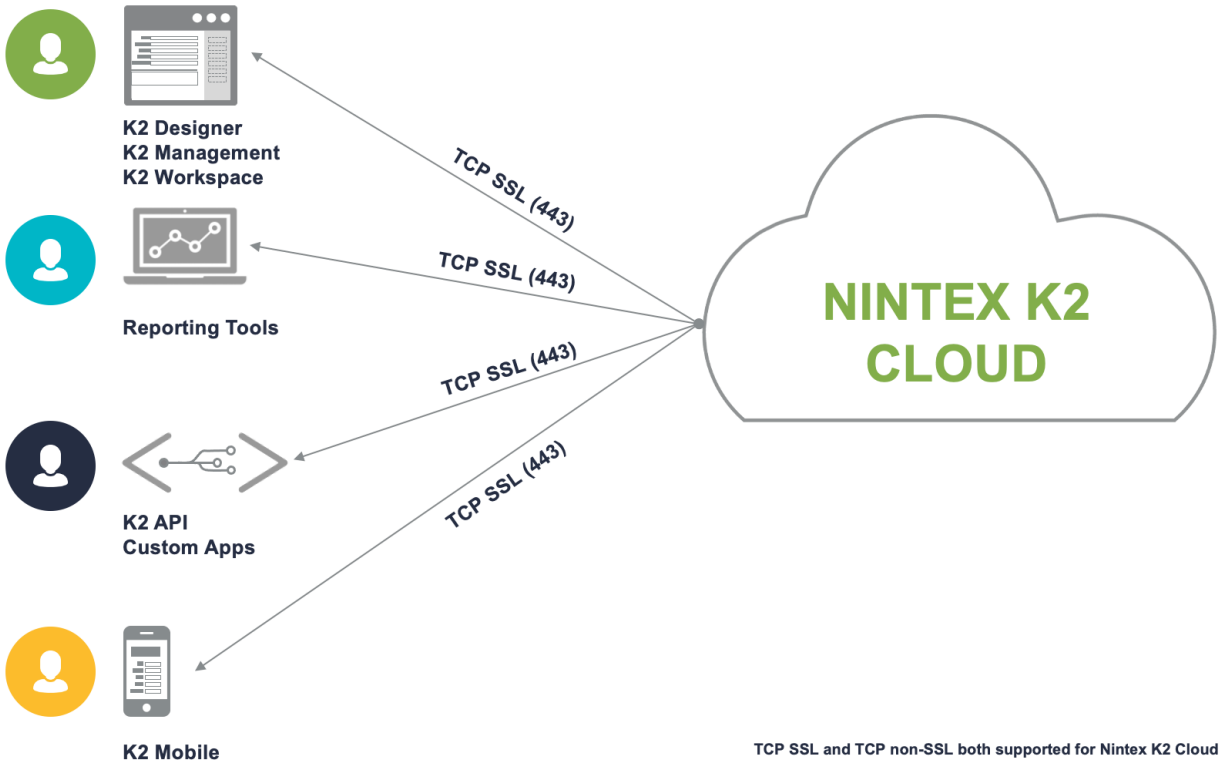


*Diagram showing network security of connections to Nintex K2 Cloud*

#### 3.3.1.1 Data transport encryption

As data is either retrieved or generated from within the Service, it is secured during transport to the client. Internal network traffic within the Service environment is secured using network subnets utilizing Access Control Lists (ACLs) to restrict network communication to resources within the Service environment only. All communication is made over secure and encrypted channels.

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

#### 3.3.1.2 Network and firewalls

All data communication within the Service environment (for example, communication between Nintex application servers and Nintex databases) occurs within the underlying protected network and does not touch the public Internet until data is returned to the calling client via secured TLS/SSL channels.

#### 3.3.1.3 Isolation and segregation

Each Service subscription, along with the resources within that subscription (including the Nintex environments, servers, data storage and network communication), is logically separated per customer.

### 3.3.2 Data security

Data stored within the Nintex K2 Cloud Service is kept separate in individual environment databases and is isolated from neighboring environments.

© 2024 Nintex USA, Inc.

The data stored in the Service is protected from unauthorized access with underlying data infrastructure security applied to logins and roles. Any data that is stored by a customer as the result of building applications on the Service is encrypted at rest within the Service via Transparent Data Encryption (TDE); more details about TDE are available here: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption.

#### 3.3.2.1 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.

**NOTE** **Customers should be aware that the database roles required for maintaining a K2 Cloud database means that Service Operations may have read-only access to the data stored in the K2 SmartBox data stores.**

**Any interaction that 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.**

### 3.3.3 K2 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 and is encrypted. Additionally, user credentials are encrypted using device-specific encryption capabilities. For specific details on K2 Mobile App Security, please refer to K2 Workspace App Security.

© 2024 Nintex USA, Inc.

© 2024 Nintex USA, Inc. All rights reserved. Nintex and K2 software products are protected by one or more U.S. and international patents. Other patents pending. SourceCode, Nintex RPA Cloud, K2, the four squares logo, the Nintex logo, K2 Five, K2 Cloud, K2 blackpearl, and K2 smartforms are registered trademarks or trademarks of Nintex in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.