NiceLabel Label Cloud

Infrastructure, Security, and Maintenance

Rev-2020-06 ©NiceLabel

Contents

Introduction

Label Cloud is NiceLabel's cloud-based Label Management System.

Cloud management enables you to reap every benefit of digitally transforming your labeling (including lower costs, improved quality assurance, and faster time-to-market) without significant upfront hardware investments. You get secure, scalable, standardized labeling for your suppliers and your entire organization **with an ROI of less than 6 months**.

Label Cloud creates these business benefits by providing you with:

- Reliable IT infrastructure
- Advanced security measures
- Thorough maintenance plans
- Comprehensive disaster recovery processes

Stakeholders in your company, including IT managers, quality assurance managers, security officers, and others all see benefits from the infrastructure, security, and reliability of NiceLabel Label Cloud.

Learn more about Label Cloud here: https://www.nicelabel.com/label-management-system/label-cloud.

Our proven track record

Labels are the glue of our global economy, and NiceLabel knows labeling.

We've been developing labeling software, label management systems, and custom labeling solutions for our partners and customers since 1993. We deliver ongoing support for our clients and make continuous improvements to our products.

NiceLabel has a decade of experience developing cloud infrastructure for labeling. Microsoft introduced the Azure cloud platform as a service in February 2010. We released our first cloud-based print service in July 2011, and haven't stopped innovating since.

We built our completely new labeling platform with cloud-first infrastructure as a priority. Cloud-first principles allow NiceLabel to leverage all the latest thoroughly-tested platforms and tools while maintaining constant security from day one of development.

Our Label Cloud customers securely print millions of labels each month. NiceLabel software is trusted and used by most Fortune 500 companies worldwide. We help a growing number of cloud customers from diverse industries and backgrounds improve their label design, printing, and management, while reducing their costs.

Learn more about NiceLabel here: https://www.nicelabel.com/about.

Infrastructure

Maintaining high availability

NiceLabel develops Label Cloud on Microsoft's reliable Azure platform, ensuring world-class infrastructure and availability.

Your Service Level Agreement **guarantees high service availability** as defined in your Master Software Subscription and Services Agreement.

Label Cloud architecture prioritizes high availability and eliminates single points of failure with multiple redundancies. We work in collaboration with Microsoft architects to build Label Cloud following best practices. Microsoft features Label Cloud in their global catalogue of Azure-based solutions.

You can find Label Cloud on Appsource and the Azure Marketplace.

Label Cloud web availability

NiceLabel builds reliability and redundancy into our cloud-based web architecture.

Label Cloud web sites run on clusters of virtual machines (nodes). Each node runs within different Availability Zones (separate physical locations within Azure data centers). If a node fails, the cluster continues to operate on other nodes.

Label Cloud runs on several clusters. In the event of a large scale whole-cluster failure, we can migrate your Label Cloud accounts to different clusters.

Redundancies and backups

Label Cloud leverages Azure to provide high availability for your applications and data.

Your data is hosted on redundant database servers to ensure no service interruptions. If one database server fails, another database server takes over (seamless service).

Azure performs database backups and stores copies of each backup in multiple physical locations. We can restore your data from any time in the previous 30 days from server backups. Label Cloud creates full backups every week, differential backups every 12 hours, and transaction log backups every 5-10 minutes.

Printing offline

Uninterrupted label printing is Label Cloud's most mission-critical process.

In case of interruptions, Label Cloud allows you to print from applications on your computers without connecting to Label Cloud backend in Azure. With system configuration, you can print in offline mode for up to 5 days. Label Cloud automatically synchronizes your printing records from offline printing.

Note: We recommend running Label Cloud on reliable internet connections. Offline printing requires you to configure your system to rely on your local cache, and is limited to cached labels and locally available data. NiceLabel's professional services team can design or advise you on best practice solution configurations for offline printing.

Assessing and mitigating risk

RISK	MITIGATION
SERVICE OVERLOAD	We monitor performance data. In the event of poor performance, we scale out resources or move you to another web server.
SYSTEM DATABASE FAILURE	We geo-replicate your database in another location. In the event of system database failure, your system automatically switches to a geo-replicated copy after 1 hour. Your database also has point-in-time backups for the previous 30 days, so in the event of data corruption, we can restore your data.
USER DATABASE FAILURE	Your database has geo-replicated point-in-time backups for the previous 30 days. In the event of data corruption or loss, we can restore your data.
AUTHENTICATION FAILURE	Your providers (Microsoft, Google) are responsible for service availability. In the event of authentication not working properly (i.e. bugs) NiceLabel cooperates with providers to resolve issues.
WEB SERVER FAILURE	All websites run on multiple nodes (clusters). If one node fails, another takes over.
DATA CENTER FAILURE	Handled by PaaS provider (Microsoft Azure). In the event of data center failures, NiceLabel contacts Microsoft (support request) to resolve issues. If Microsoft doesn't resolve issues or promptly provide estimated restoration times, NiceLabel restores services in another data center.
DNS FAILURE	Microsoft guarantees 100% DNS services availability.

Security

NiceLabel makes significant efforts to ensure Label Cloud security.

We implement the latest security standards and perform automatic and manual Label Cloud security checks. We're committed to providing you trustworthy service while applying policies, technologies, and controls to protect data you entrust to Label Cloud.

Layered security

NiceLabel keeps your systems and data secure in multiple ways.

Most security breaches don't occur from someone breaking into cloud data centers. Instead, attackers typically exploit cloud application vulnerabilities. To prevent attacks, we combine multiple mitigation strategies and security controls to protect your resources and data.

Our layered security includes:

- Employee education
- Physical security
- Network security
- Web security
- API-based cloud security
- Data encryption

By running on Microsoft Azure, Label Cloud inherits many platform and infrastructure security approaches and best-practice implementations. Microsoft handles core data center security and inspects dataflows from the internet to help secure your network against intrusions and malware attacks.

We design cloud applications following modern security-conscious programming practices. We use encryption techniques and execute testing procedures to develop code and launch products.

Our development teams complete IT security-related training on software development to strengthen their information security awareness and experience.

Role-based access

Label Cloud authenticates with Microsoft and Google (Oauth2/OpenID Connect).

We integrate trusted providers into Label Cloud security to authenticate your user identities and protect your users from attacks. This allows NiceLabel to focus on core features and leaves identification to experts you know.

You can define your users with LDAP directory services or use your Microsoft Office 365 or Active Directory (AD) accounts (available as Azure Active Directory for cloud applications). Label Cloud does not include authentication mechanisms or custom authentication logic.

Database security

Database separation is essential and ensures you get additional layers of security.

You can only access your own assigned application database. You cannot access application databases directly with management applications or via API. Database ownership prevents other customers from accessing or reading any of your data.

Dependent on your Label Cloud subscription, you can access user-based cloud databases to store printing data and for daily intermediate master data exports from ERP systems. You don't need user-based cloud database access to run Label Cloud web applications.

User database access is entirely customer specific. When you claim your user database, we create your first administrative account so you can manage your database and grant user access yourself.

Data encryption

NiceLabel encrypts your data to keep your business safe.

Your data can occupy two states in Label Cloud-- **data in transit** and **data at rest**. Your data can be exposed to risks in both states. Label Cloud uses encryption to protect data in transit and at rest from unauthorized access or theft.

Data actively moving between devices or networks across the internet is data **in transit**.

We protect your data in transit from local storage to Label Cloud storage. We encrypt your data in transit on one end and decrypt it on the other to prevent eavesdropping from unauthorized clients. Label Cloud uses modern data encryption communication protocols (TLS and HTTPS) for privacy and data integrity.

We encrypt your data when you connect to Label Cloud with:

- **Browsers.** You can use any modern web browser to interact with our web applications.
- **NiceLabel clients.** All our clients, including Designer, Print, Automation, and Web Client, use secure encrypted channels to request Label Cloud data and to send back logs and updates.

Data not actively moving between devices or networks across the internet is data **at rest**.

Label Cloud receives and stores your data in Azure SQL databases unique to you. We follow protective security measures to prevent anyone from accessing, modifying, or stealing your at-rest data:

- Only you have access to product databases you own.
- Your Azure SQL databases use transparent data encryption (TDE). TDE gives you real-time database encryption and decryption using AES 256 encryption algorithms.

API security

NiceLabel software uses Azure APIs for secure data exchanges and inter-application communication.

- **Service Bus:** the communication system between mutually interacting software applications in service-oriented architecture. We use Service Bus to communicate with your on-premise infrastructure, either through cloud-connected IoT printers or cloud triggers (running in NiceLabel

Automation). Service Bus creates outbound connections from your backend to Label Cloud and makes it possible to call your backend from the cloud.

- **Azure functions.** Our published APIs for Label Cloud (Cloud Print API and Cloud Trigger API) call Azure functions for additional processing, which in return call the correct Service Bus endpoints. For example, when you execute "print" in Cloud Print API, Label Cloud generates a print job, knows where your IoT cloud printer is, and delivers your print job to your printer. We have traffic limits in place to prevent the abuse of APIs.

Health monitoring

NiceLabel continuously monitors your hosted system health with Azure Insight.

Insight automatically detects performance anomalies and includes powerful analytics tools to help us diagnose issues and improve products by understanding how our customers use Label Cloud.

We use Insight to:

- Monitor abnormal traffic and respond quickly to possible threats.
- Detect and respond to higher demands for services.
- Continuously improve performance and stability

Testing

NiceLabel tests all code extensively to ensure safety and high quality.

Commonly exploited software vulnerabilities include defects, bugs, and logic flaws. Our development team strives to produce quality code through best practice techniques, including:

- Pair programming
- Recurring code reviews
- Adhering to secure code standards
- Running multiple tests

Our general policy is to automatically test everything we can. We perform continuous regression testing for each release throughout the lifecycle of our software to ensure industry-grade quality standards.

In addition to our experienced internal testing teams, we continuously contract third-party security assessment specialists to make sure our software is safe, secure, and ready for you to use.

Internal testing

NiceLabel development teams design and execute an expansive array of manual and automated tests for each new software build.

We increase the number of tests and the number of test team members for final testing before releases. Any security flaws we detect results in writing new automated tests to prevent problems from appearing again.

Third-party security assessments and penetration testing

NiceLabel contracts third-party IT security specialists for major and minor releases.

Our security experts access our software like our customers, but use their expertise to assess our web and desktop applications to identify exploitable vulnerabilities. Testing involves building custom threat profiles to uncover security vulnerabilities specific to our applications and web technology.

Our third-party security testers use the OWASP Testing Guide for test execution and verification. The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software.

Acceptance in regulated environments

NiceLabel testing is compliant and trusted by customers in regulated industries.

Label Cloud customers in regulated industries including healthcare, pharmaceuticals, medical device manufacturing, food & beverage, and others rely on test results we provide.

We will also work with you to perform tests with your own testing tools and procedures.

Maintenance and Updates

NiceLabel keeps you up to date.

Our controlled process updates Label Cloud automatically, providing you seamless hassle-free updates with **no platform downtime**.

We update with major product releases every two years, minor releases twice per year, and service releases in between (as needed):

RELEASE TYPE	EXAMPLE	DESCRIPTION
MAJOR	NiceLabel **2019**	Major product releases include significant feature updates, performance improvements, and bug fixes.
MINOR	NiceLabel 2019.**1**	Minor releases include feature updates, performance improvements, and bug fixes.
SERVICE	NiceLabel 2019.1.**1**	Service releases include bug fixes.

For full update schedules and more details, read our Product Lifecycle Policy.

Updating Label Cloud

NiceLabel provides new Label Cloud deployments for every software release.

We prepare and test each new deployment before we update your subscription, allowing you to upgrade seamlessly without downtime. We update your subscription by simply moving you from your previous deployment version to your new one. If you experience any unexpected problems, we return you to your previous version while we solve any problems.

We have transparent update plans and clearly-defined procedures in place for all release types (major, minor, and service). You receive email notifications before any Label Cloud version updates, allowing you to prepare for, test, and track every upgrade.

Update timeline for Label Cloud releases

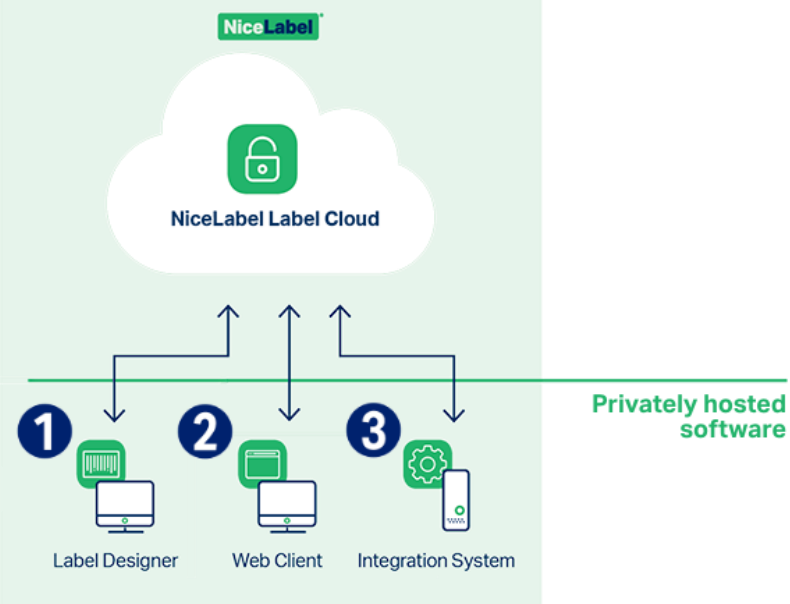
Note: Release days are when major, minor, or service releases become publicly available.

TIME	ACTIVITY	DESCRIPTION
RELEASE DAY	First email notification	You get an email notification saying your sandbox (testing) environment will update in seven days, giving you a 3-week testing period before your production environment updates.
RELEASE DAY + 7 DAYS	Second email notification	You get a second email notification saying your sandbox (testing) environment is updated to the latest version, giving you a 3-week testing period before your production environment updates.
RELEASE DAY + 7	Sandbox	We update your sandbox environment to the latest version. You

DAYS	environment upgraded	have no sandbox environment downtime, we simply move your account. This procedure allows you to see how your production environment will handle the upgrade.
RELEASE DAY + 28 DAYS	Third email notification	You get a third and final email notification saying your production environment is updated to the latest version.
RELEASE DAY + 28 DAYS	Production environment upgraded	We upgrade your production environment to the latest version. You have no production environment downtime, we simply move your account.

Updating privately hosted software

You can host Label Cloud modules on your private infrastructure with your subscription:



1. Your **Label Designer** designs labels and configures your printing application.
2. Your **Web Printing Client** runs your printing application through the web.
3. Your **Integration System** integrates your printing (Label Cloud Business only).

Your privately hosted software always links seamlessly with your Label Cloud subscription.

We regularly update Label Cloud, but your **privately hosted software does not update automatically**. Our up-to-date Label Cloud backend still runs older versions of your privately hosted software.

Until you update your privately hosted software, you may not be able to use some new Label Cloud features and functionality. To get every benefit from your Label Cloud subscription, periodically update your privately hosted software as we release newer versions of Label Cloud. Schedule your updates to fit your maintenance and production requirements.

Disaster recovery

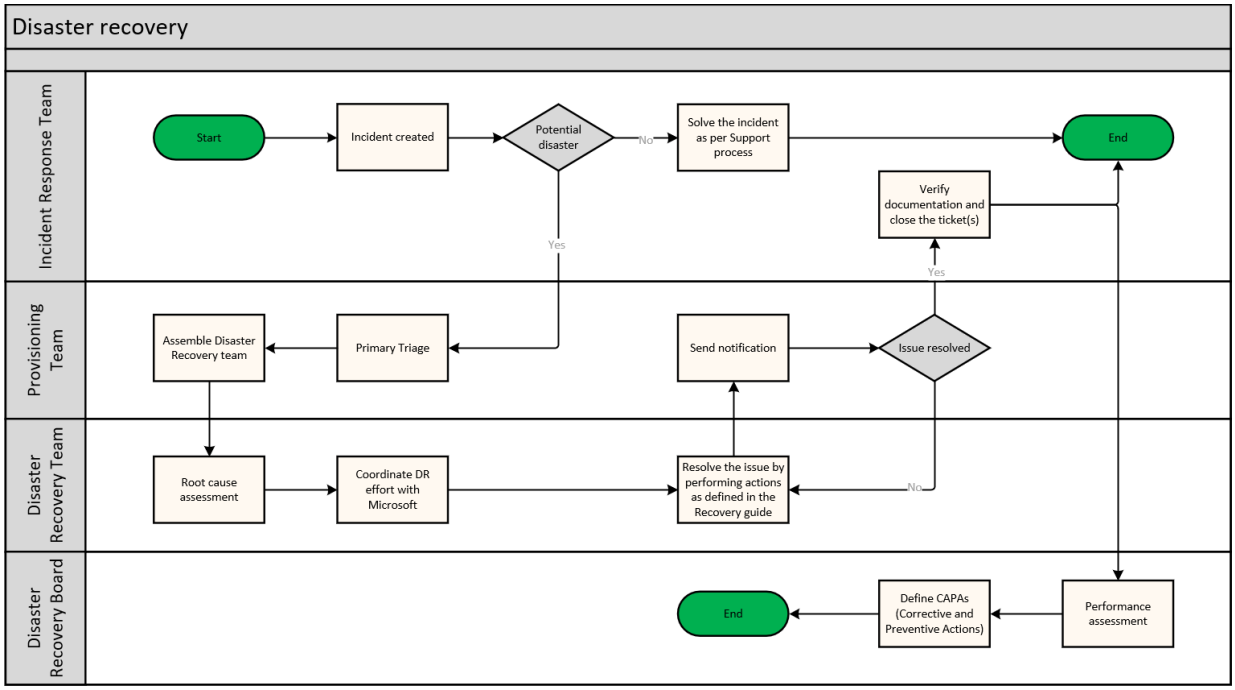
Label Cloud is stable and secure.

But if things go wrong, NiceLabel has comprehensive disaster recovery plans in place. Our teams work hard to minimize your downtime and help you get back to business as usual as quickly as possible.

Terms and definitions

NAME	DEFINITION
INCIDENT	A situation that might be, or could lead to, a disruption, loss, or disaster.
DISASTER	Any condition that results in a prolonged inability to access or use Label Cloud. A disaster requires recovery action to restore normal operation.
INCIDENT RESPONSE TEAM	Includes members of our support and application development teams who respond to incident support requests from customers. Incident response team members receive alerts from our monitoring system. Incident response teams resolve incidents or escalate incidents to disasters.
PROVISIONING TEAM	Application development team members responsible for managing Label Cloud. Besides regular management, our provisioning team supports our incident response team resolving incidents.
DISASTER RECOVERY TEAM	Assembles in the event of a disaster scenario to recover the service from the disaster. Includes provisioning team members.
DISASTER RECOVERY PROCESS MANAGEMENT TEAM	Monitors, reviews, and makes changes to disaster recovery processes to ensure effectiveness. This team is not directly involved in disaster response, but reviews each disaster scenario to improve processes.

Flow chart



Workflows

Incident start

Incidents begin when our incident response team receives information about issues affecting Label Cloud. This information may come from:

- Monitoring system alerts
- Customer support requests (phone or email)
- Other events indicating potential Label Cloud problems

We track incidents with support tickets following standard support procedures.

Incident response

Incident response teams handle incidents. Response includes:

1. Incident assessment (reviewing alerts, customer reports).
2. Decision point. After investigation, teams decide whether or not to escalate incidents to disasters.
    a. Incident response teams consult with the provisioning team as needed.
    b. If incidents do not require disaster responses, teams resolve incidents according to standard support processes.

Incident handling and response times follow standard support procedures determined by your SLA level.

Escalation to disaster

Incident response teams contact the provisioning team to trigger disaster recovery responses. Our provisioning team assembles a disaster recovery team to oversee disaster recovery processes.

Disaster recovery

Teams log all status updates in our internal system to ensure visibility for all teams involved. Teams add the [Disaster] keyword to all related support requests to organize disaster logs.

Our disaster recovery team analyzes problems and determines next steps by following our established disaster recovery procedures:

1. Identify the scale, impact, and root cause of the problem.
2. If the problem is due to underlying Azure cloud infrastructure, make sure Microsoft is solving the problem:
    a. Check Microsoft notifications in the Service Health section.
    b. Open support tickets as needed.
    c. Monitor Microsoft's progress.

    If Microsoft resolves the problem in a timely manner, no additional recovery action is required.
3. If Microsoft does not solve the problem, begin recovery procedures following our recovery guide.

While the disaster recovery team progresses through disaster recovery, we provide affected users with status updates and estimated resolution times.

Following recovery, the disaster recovery team analyses root causes of outages and recommends improvements you can make to prevent future incidents. Your affected users receive reports including service credit notes when applicable.

Recovery times

We're committed to restoring service as soon as possible. Recovery times may vary according to the nature and the scale of the problem. NiceLabel works with Microsoft to resolve issues related to underlying services provided by Microsoft Azure.

Management

Periodic tests

Our disaster recovery process management team periodically tests our disaster recovery processes to ensure correct execution and measure effectiveness. Our teams schedule and perform periodic tests at least once per year following established plans. Teams analyze test results during process reviews.

Process reviews

Our disaster recovery process management team reviews our recovery processes:

- After each disaster scenario

- Periodically (at least once per year)
- As needed (during planned enhancements, or if deficiencies are found outside the scope of periodic testing)

Our disaster recovery process management team determines if our processes require changes and may delegate implementation to our provisioning team. We notify affected teams about all changes.

Additional resources

NiceLabel delivers the following documentation on request.
Note: Some documents are subject to signed non-disclosure or software maintenance agreements.

1. **Consensus Assessment Initiative Questionnaire (CAIQ).** Shows compliance with CSA® (Cloud Security Alliance) best practices. CSA STAR™ (CSA Security, Trust, Assurance and Risk) is the industry's most powerful program for security assurance in the cloud. STAR™ encompasses key principles of transparency, rigorous auditing, and standards harmonization.
2. **Microsoft CAIQ document.** NiceLabel Label Cloud runs on Microsoft Azure and automatically inherits Azure security specifications: https://cloudsecurityalliance.org/star/registry/microsoft/.
3. **Traceability matrixes. Features lists including test cases.** NiceLabel Control Center feature specifications. Automated Label Cloud product testing ensures there are no software flaws or bugs in released software.
4. **Internal team testing reports.** Showing tests we performed and total numbers of tests ran for each software release.
5. **Penetration testing reports.** Assessments from our third-party security company showing tests performed for NiceLabel Label Cloud, test time intervals, any vulnerabilities, and their conclusions on software security.
6. **ISO 9001:2015 certificate.** Our parent company, Euro Plus d.o.o., has implemented and maintains a management system which meets the requirements of ISO 9001:2015 standards: https://www.nicelabel.com/resources/files/doc/resources/ISO9001-certificate.pdf.

Americas
+1 262 784 2456
sales.americas@nicelabel.com

EMEA
+386 4280 5000
sales@nicelabel.com

Germany
+49 6104 68 99 80
sales@nicelabel.de

China
+86 21 6249 0371
sales@nicelabel.cn