Ultimo
an IFS company

Ultimo in the Cloud

Performance Built on Trust.

Reference Guide

Contents

Reasons to Choose the Ultimo Cloud

- In 2024, our uptime was 100%. Applying a so-called container architecture is one of the ways in which we realize a higher availability of the Ultimo application.
- From the cloud, you can safely work anywhere and at any time with the Ultimo software. The same goes for mobile applications and making data available for external parties.
- The cloud fee is predictable and includes the use of the software, continuous updates, and the same high-quality infrastructure.
- By making the Ultimo software architecture suitable for Azure, we took this as an opportunity to start releasing the software more frequently. This means that we strive for a bi-weekly update cadence.

Cloud-based EAM: Grow Fast, Stay in Control

Business moves fast. Your enterprise asset management (EAM) platform shouldn't lag behind. Ultimo is a cloud-native, software-as-a-service (SaaS) EAM solution built to flex and scale as your industry evolves. This way you're always ready for what's next.

Available at all subscription tiers, Ultimo is ready for rapid deployment, complete with the Ultimo Configuration Toolkit tailored to your industry's specific needs. Users consistently report that it's intuitive and easy to use. In today's world, maintenance, reliability, and operations demand speed and precision. Ultimo delivers both–from the cloud.

Subscription Tiers

We offer a subscription plan that meets your needs and budget. With predefined industry solutions, we guarantee a best-practice solution for your industry. Out-of-the-box, yet extremely flexible, Ultimo provides an unmatched time to value through quick implementations, seamless integrations, and self-service application management.

Ultimo Professional

Ultimo Premium

Ultimo Enterprise

When new, important functionalities are added, all end users will be informed when starting the software through a “New in Ultimo“ dialog box. In the Customer Portal, you can consult the release notes of the rolling release.

Are you already hosting Ultimo on a different platform?

We can imagine that when you already host Ultimo externally, you’re wondering what the advantages are when you migrate to the Ultimo cloud. Next to the state-of-the-art platform which we describe in this document, your advantages are:

- Your Ultimo environment is kept up to date automatically.
- Implementing changes or expansions can be done more efficiently.
- You can use the Ultimo Business Intelligence solutions.
- New technologies, such as generative and agentic AI, are automatically made available on the Microsoft Azure platform through frequent updates and can be activated by the customer.

More than 145,000 technicians, managing over 22 million assets, rely on Ultimo to drive maintenance, uptime, safety, cost control, and operational efficiency.

CI/CD from Creation to Release

You do not have time to wait for manual updates. Nor should you be expected to. Legacy technologies were made for another era. Ultimo's modern, cloud-based EAM is built for today.

Your business will benefit from our continuous integration and continuous delivery (CI/CD) which is a best practice for DevOps teams to implement.

In the old days, any software updates could be painfully slow and occurred one at a time. CI/CD is an agile methodology, meaning we update fast, in iterations and sprints. Our software development teams know how vital it is to meet your business requirements, so we ensure that code quality and security are automated for continuous delivery.

We strive for a bi-weekly update cadence.

To maintain the desired quality level, we utilize a process with various reviews and gatekeepers.

Quality Process

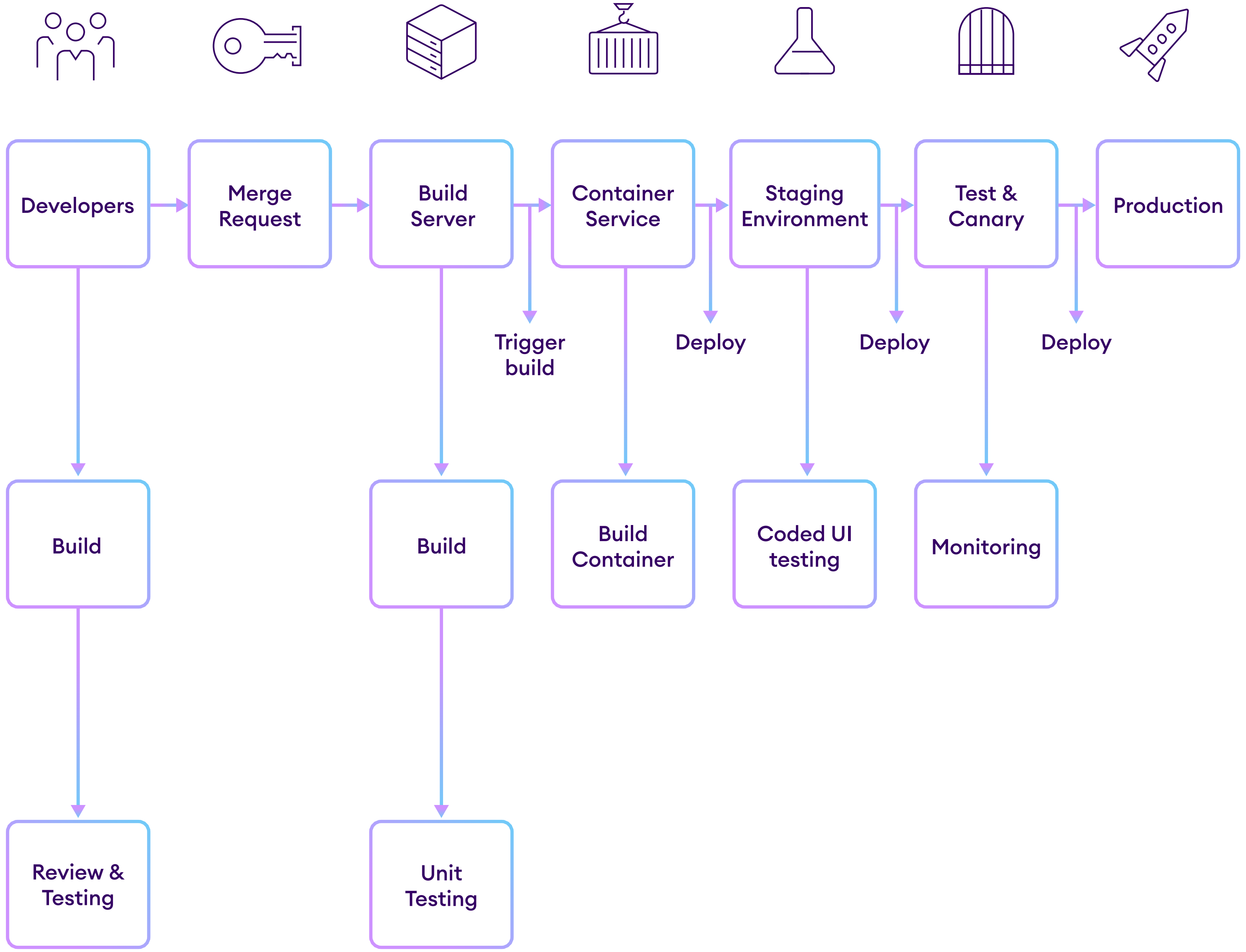
Our developers' work on improving existing functionality as well as expanding additional functionality on a daily basis. The products they deliver are reviewed by experienced peers.

Following this first review, the developer does a merge request, triggering various checks, including 14,000+ automated unit tests and balances, which lead to deploying the new build through our Container Service.

The build is prepared in a staging environment, where, again, more testing is done by means of over 150 user interface tests. All of which is followed by deployment to a specific set of environments, such as a small subset of users in what is known as a Canary strategy. In the end, the build is integrated into your production environment. From staging to Go-Live, the process takes two weeks and is fitted with various monitoring gaps between the Test, Canary, and Production steps.

Feature Toggles

A Feature Toggles function is built into Ultimo, so you can decide when a feature will be activated in your environment and introduced to users.



Continuous Cloud Availability Worldwide

Ultimo partners with Microsoft to ensure continuous availability of your Ultimo environment. We use multiple primary and secondary Azure data centers as so-called paired regions.

As a customer, you choose a region, and data will be hosted in that region.

Region	Primary	Secondary
Australia	Australia East	Australia Southeast
Europe	West Europe	North Europe
Germany	Germany West Central	Germany North
India	South India	Central India
Sweden	Sweden Central	Sweden South
United Kingdom	UK South	UK West
United States	East US	West US

Infrastructure

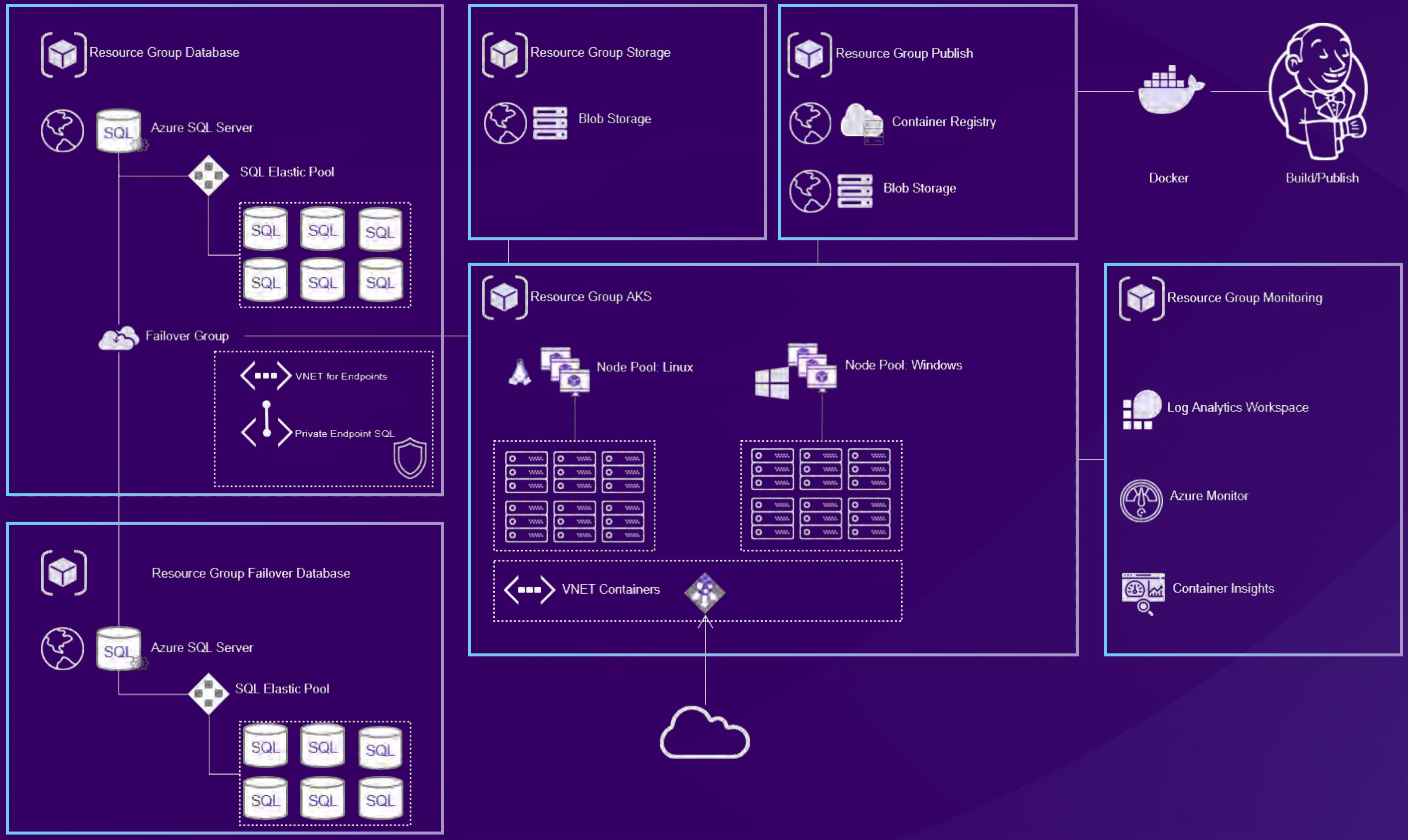
The infrastructure needed to host Ultimo SaaS is entirely created based on Infrastructure as Code. No manual actions are needed to deploy new environments and to maintain current environments, reducing the risk of human error. New environments are rolled out, and updates are performed based on a Desired State Configuration. An automated system continuously verifies that all environments are set to the correct values.

Infrastructure as Code

- Patches and operating system (OS) updates are performed on a ‘zero-downtime’ basis. Only Kubernetes updates require downtime. These are announced two weeks in advance and, based on experience, take about 2 hours approximately 4 times a year. These updates are carried out outside office hours in the respective regions where possible.
- Disaster Recovery is tested at least every 6 months. Since almost all Resource Groups are replicated to a Failover region, only the Kubernetes Cluster needs to be rolled out. This is done on an Infrastructure-as-Code basis and requires no manual actions besides starting the process.
- Access to the platform is based on Privileged Account Management. Every engineer needs to log in using Azure Active Directory (AD) with multifactor authentication (MFA). Only then can they give themselves access to Resource Groups. The reason and timeslot are logged, and all other managed privileged accounts are notified about it instantly. This process is managed through our proprietary system. We provide you with access to these logs through the Customer Portal.
- In Ultimo, all customers databases are stored separately creating additional security. Most of our resources (especially the resources containing customer data) is single tenant and therefore separate from all other customers; One tenant’s code cannot directly interfere with another’s. Some small parts (such as the report service) are made multi-tenant in Ultimo.

Azure

🌐 = Geo-Redundant



Resource Group Database

Azure SQL Server

SQL Elastic Pool

Failover Group

VNET for Endpoints

Private Endpoint SQL

Resource Group Failover Database

Azure SQL Server

SQL Elastic Pool

Resource Group Storage

Blob Storage

Resource Group Publish

Container Registry

Blob Storage

Docker

Build/Publish

Resource Group AKS

Node Pool: Linux

Node Pool: Windows

VNET Containers

Resource Group Monitoring

Log Analytics Workspace

Azure Monitor

Container Insights

Availability

We do our utmost to keep all SaaS environments online 24-7. Our target uptime in the service level agreement (SLA) for Ultimo SaaS environments is 99.7%.

Steps Taken for Availability

We take the following measures to meet high expectations on uptime:

- Ultimo is running on an Azure Kubernetes Service (AKS). By default, AKS provides high availability by using multiple nodes in a virtual machine scale set. This means that all the nodes (every customer has their own node) are running on multiple underlaying virtual machines. Should a virtual machine fail, you won't even notice.
- The Ultimo database is running on an SQL Elastic Pool on Azure with automatic failover in case of a disturbance.
- Storage is Geo-Redundant and has automatic failover in case of a disturbance.

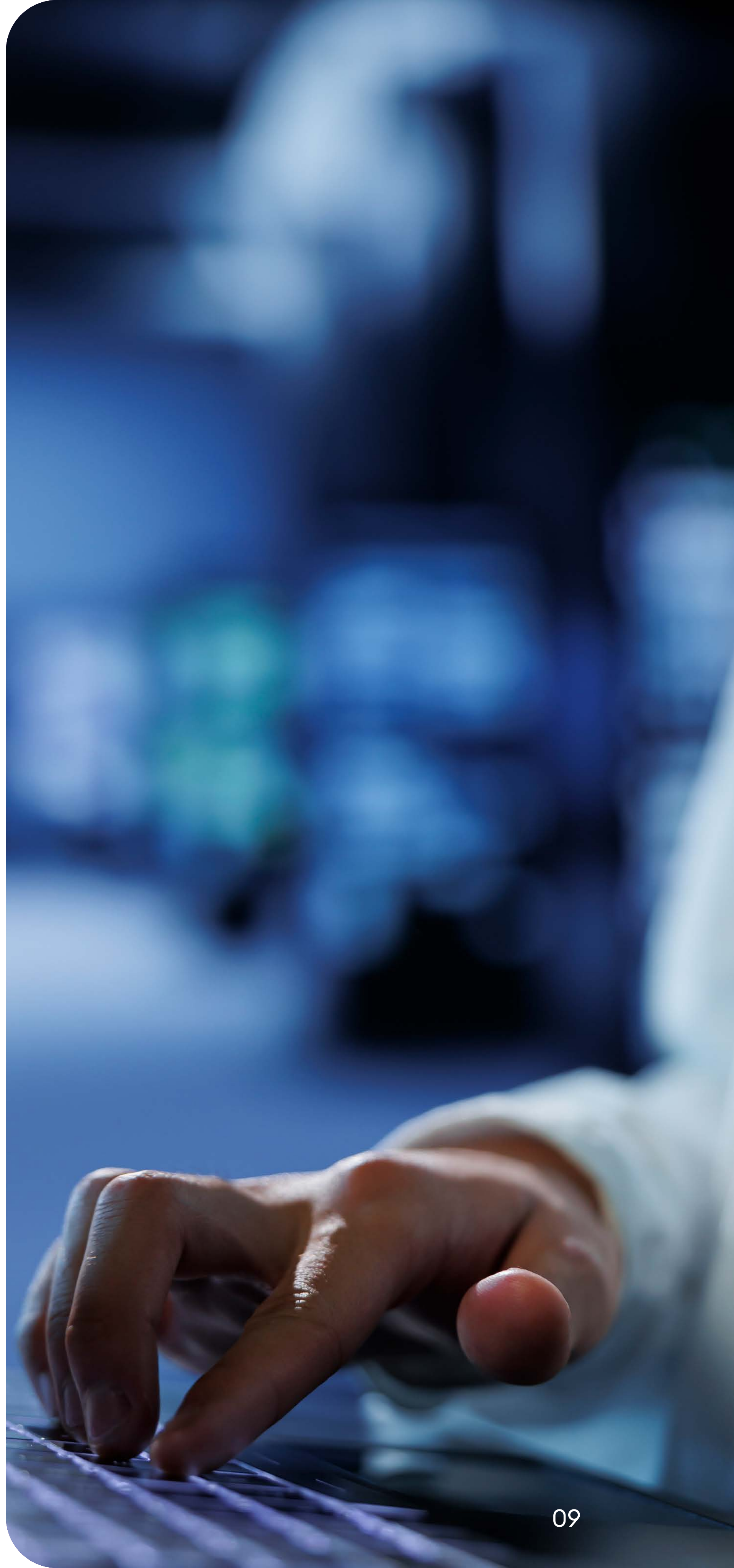
Ultimo's uptime historical data:

2024	100%
2023	99.97%
2022	99.98%

- Within the Azure data center, many measures are taken to prevent hardware failures.
- For Backup Retention, we provide 3 levels of availability for all databases and files:
  1. Hourly restore point for the last 7 days.
  2. Weekly restore point for the last 4 weeks.
  3. Monthly restore point of the last 3 months

Monitoring and Support

- The infrastructure is monitored using Azure Monitoring on relevant metrics like Memory Pressure, CPU Pressure, performance monitoring, and available disk space. Engineers are notified by email, SMS, or PagerDuty escalation to prevent downtime in environments.
- In addition to overall infrastructure monitoring, there are health probes for each environment in place. Should an environment fail, the engineers are alerted instantly.
- There is 24/7 monitoring for platform instability, downtime, regional, and multi- or single-tenant issues.
- In case of a Priority 1 incident, which includes a certain site error, Ultimo will make commercially reasonable efforts to a maximum recovery point objective (RPO) of 1 hour and recovery time objective (RTO) of four 4 hours. In case of the unlikely event of total site error Ultimo will take commercially reasonable efforts to a maximum RPO of 24 hours and RTO of 5 business days.



Security

The security of your data and processes is very important. We take various measures to set your mind at ease.

Penetration Tests

Penetration tests are performed by an external party on a yearly basis. These tests focus on the software as well as the platform. A management summary can be provided upon request.

Secure Sockets Layer (SSL)

We only allow secure HTTPS connections to Ultimo environments. HSTS preloading on NGINX is used to ensure all supported browsers force users to a secure connection.

Web Application Security

To safeguard customer environments against web-based threats, our cloud platform integrates ModSecurity, a powerful open-source Web Application Firewall (WAF) engine, with NGINX. This WAF delivers advanced traffic inspection, and customizable security rules tailored to specific application needs.

Private Endpoints

Most resources are only accessible through private endpoints. This means traffic isn't flowing over publicly routable networks, so the risk of the network traffic being eavesdropped on is reduced.

DDoS Protection

We use Azure Distributed Denial of Service (DDoS) protection.

Virus Scanning

We use Azure Defender Protection. In addition, there is also a scanner active in the Container Registry, which scans, for instance, whether the OS used on images is secure. This provides both virus and vulnerability scanning.

Encryption

All your customer files are stored using Azure Storage. The data on Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

For the database, Transparent Data Encryption (TDE) helps protect Azure SQL Database against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files.

Security for Ultimo Mobile Solution

Ultimo takes security very seriously. Of course this extends to our mobile solutions as well. What actions are taken to keep your data and processes safe?

The mobile application runs with the minimum privileges required on the OS. No part of the code is executed with root privilege. In this way, malware attacks are unable to use elevated privileges to gain access.

Connection to the Corporate Network

Ultimo Go+ is listed in the Apple App Store and Google Play Store with only default features; any corporate customization lives in your cloud environment and stays private.

For connection to your corporate network, it is possible to authenticate using two-factor authentication (2FA) via your own IDM solution. With two-factor authentication it is harder for attackers to gain access to sensitive content on devices or online accounts. The additional authentication check that is performed ensures that a password alone is not enough to gain access.

All data between the app and the network is end-to-end encrypted (e.g., HTTPS with header-based authorization).

Data Storage

All data entered or opened in the app, and all data saved for offline use, is stored within the app. As a result, all sensitive data is not stored or cached on mobile devices where it may be accessible for third parties. Passwords and keys are not stored in caches or logs. All sensitive data is stored encrypted.

Mobile App Offline Capability

All data can be stored offline in a local SQLite database. If the user wants to update locally stored data, they can synchronize their offline data when they are online. When a user is offline, an action on stored data (such as reporting progress on a job) is saved. When the user is online, they can manually synchronize their offline actions with the server-stored data.

Authentications

Identifiers of a specific mobile device shared by us with other applications are encrypted. The same principle applies for application sessions and to HTTP(S) sessions and cookies. This way, device information stays anonymous.

When using Internet services, data sent as part of the HTTP header is kept at a minimum. No user or device-specific related data (e.g., MSISDN, IMEI, IMSI, subscriber number) is sent. If device-specific related data is needed, we will ask the user specifically to give their consent and all data sent shall be subject to the Ultimo Master Agreement.

When periodic authorization from the device is required, authorization tokens are used instead of static passwords. These tokens are encrypted while stored on the device and encrypted in transit (using HTTPS). Tokens can only be issued by the backend service after verifying the user credentials initially and are time-bound as well as revocable.

The latest versions of the authorization standards are used.

Connections sending sensitive data are only established after verifying the identity of the remote endpoint. It is ensured that SSL is only established with end points that have trusted certificates in the key chains.

Software Development

Of course, the security measures for software development, as described elsewhere in this document, are also applied to our mobile solution. Our app is built with MAUI and communicates with an Ultimo server using HTTP or (even better) HTTPS calls. The app is compatible with Android and iOS phones and tablets. More information about compatibility can be found in our system requirements.

To view our system requirements, visit:
www.ultimo.com/system-requirements

Single Sign-On Possibilities

Ultimo offers solutions for Single Sign-On, namely:

User Authentication

Ultimo offers a free Single Sign On (SSO) solution with Microsoft Entra ID. Only users with an account can use this standard SSO option. The authentication is done at your Identity Provider (Entra ID). You can control additional security measures like multifactor authentication (MFA) or 2-step verification as a customer in your Identity Provider.

User Provisioning

User accounts can be created manually (in batch) or automatically via an optional System for Cross-domain Identity Management (SCIM) module. To implement SCIM, your IT department should be involved. User provisioning ensures an accurate list of users is always available in your system. When a user leaves your organization, the account is disabled.

Customer-specific SSO Options

Maybe you don't use Entra ID, or you want to use additional certificates. In that case, Ultimo also offers customer-specific SSO options. We support SAML2 and OIDC as protocols to communicate with different Identity Providers, like Okta.

Form Authentication

If an SSO solution isn't an option, form authentication can be enabled in the environment so that users can log in with a username and password. Because this is single-factor authentication, we don't recommend this option.

For more information, request our Identity and Access Management (IAM) white paper.

Active Directory Federation Services (ADFS)

ADFS, a software component developed by Microsoft, can run on Windows Server OS to provide users with Single Sign-On access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and to implement federated identity. Claims-based authentication involves authenticating a user based on a set of claims about that user's identity, contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means and that is trusted by the entity doing the claims-based authentication. It is part of the Active Directory Services.

Security Assertion Markup Language (SAML)

SAML 2.0 is a version of the SAML standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between an SAML authority, called an Identity Provider and an SAML consumer, called a Service Provider. SAML 2.0 enable web-based, cross-domain Single Sign-On (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user.

> "The infrastructure and the web application of Ultimo have excellent security levels."

Software Development

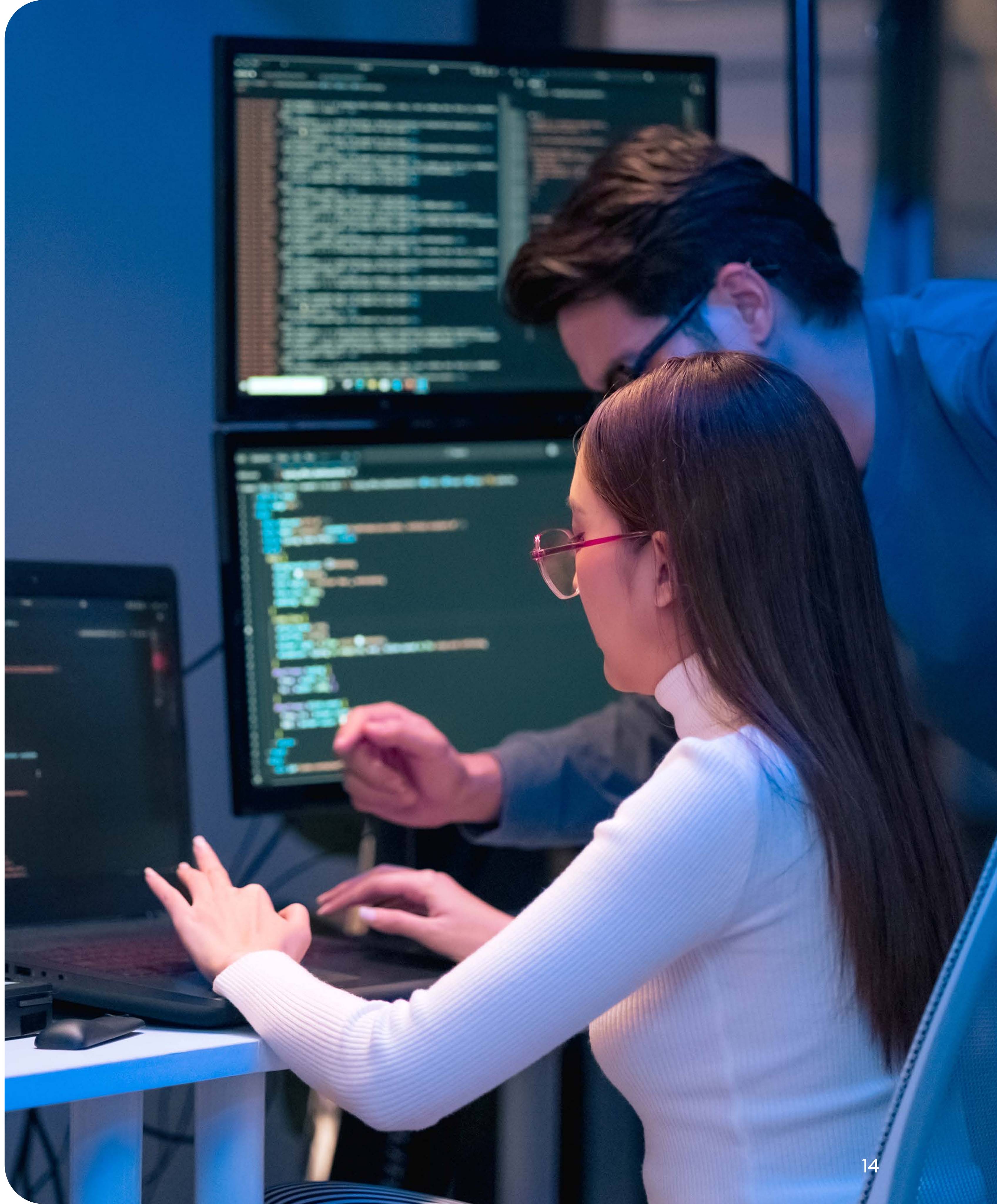
Several measures regarding security and quality are part of the agile software development process at Ultimo.

Security-related Measures

- Development and code reviews are done according to the OWASP list. Peer developers and gatekeepers do the code reviews.
- The code is continuously scanned for security vulnerabilities by specialized external tools, like WhiteSource.
- Penetration testing of the hosting platform and software security reviews are done yearly by a specialized external party called Mend.

Software Quality-related Measures

- Performing tens of thousands of automated tests before every software release. This combined with periodical manual tests.
- Static source code analysis tools checking code complexity, code duplication, static violations, agreements concerning style and consistency, and code coverage that is reached through unit testing.
- Agile scrum process that contains clear process steps regarding quality, for example, code reviews.



Unified Support

Application Manager

Your experience with Unified Support at Ultimo begins with designating an application manager from your organization to manage your Ultimo application. They can grant access, roll out, and supervise new functionality; inform your team about changes, maintain the application, etc.

At Ultimo, we need to know who the Ultimo application manager at your organization is, so we can inform them well in advance about upcoming changes. They would be the one to determine whether an Ultimo (test) environment can be overwritten.

Within your Ultimo Production environment, you can mark users as application manager. This gives them access to extra content relating to application management in the Academy knowledge system from the Ultimo environment. This information is also important to access the Ultimo portal, for example, to report a service request. To be clear, this makes application managers the only contact for customer support.

In the future, we expect a further roll-out of functionality that will give application managers a significant role. It is, therefore, important to mark application managers in Ultimo and keep this up to date.

Customer Support

Ultimo Customer Support is a dedicated, global team of highly skilled and professional Support Engineers, committed to delivering exceptional service. For our customers, Ultimo Customer Support serves as the primary point of contact for any questions, issues, or minor configurations encountered during daily use of Ultimo. English is the primary language used to ensure clear and efficient communication. If support requests are submitted or updated in any other language, Ultimo cannot guarantee response times as outlined in the support policy.

Ultimo Customer Support is available during business hours, from 08:30 to 17:00 CET on weekdays. For customers based in continental America, support is available from 08:00 to 16:00 CST.

To view our support policy, please visit:
www.ultimo.com/system-requirements

Cloud Support

The Cloud team is responsible for all SaaS/Cloud environments' performance and reliability. That means our daily activities always have the uptime and performance of the customer environments in mind.

The cloud team operates for 16 hours per weekday, from 08:00 until 00:00 CET. In addition, a 24/7 shift is active for any issues outside office hours. There is a dedicated team monitoring and managing the system 24/7. We have automated alerts tied into our ticketing system to immediately notify the team of any service degradation. We assist and collaborate also with internal teams such as R&D and QA teams, which results in better quality releases and faster issue resolution.

On our developer page **(developer.ultimo.net)** we provide extensive information about our connectivity capabilities and Azure documentation. The cloud team communicates directly to all stakeholders through our status page **(status.ultimo.com)** for any planned maintenance activities or unplanned downtime.

What Customers Say About Ultimo

We did make the choice to migrate to the cloud because we also want to keep up with the latest developments in software. We understand that this is the future. I also participated in Ultimo customer panels a number of times. While it's nice to talk about new applications, you also want to actually start using them at some point. Ultimately, it's important to keep up with the evolution of a system.”

Gregory Ketel

Manager IT Application Management

AVR.

We chose Ultimo as our maintenance management solution because the cloud-based Enterprise Asset Management software offers the most capabilities and aligns with our best-in-class standards.”

Martin Lorefice

Corporate Technical Project Manager

Dr Schär

Working smarter with Ultimo Premium saves us at least 1 FTE in time, because all asset data are recorded, and we no longer have to search for missing maintenance and service or quality data.”

Frits ten Brinke

Maintenance Manager

BROSHUIS HOLLAND

We wanted to move to a new, consistent and up-to-date environment and an application that supports our work processes. And because Ultimo continuously develops their cloud application, it contributes to our continuous improvement program.”

Erik Bakker

Advisor Information Management, Antonius

antonius zorggroep

General Information

We, at Ultimo, strive for the highest possible quality at a fair price and with continuous availability. Obviously, we also expect this from our partners. Ultimo is ISO 27001 and ISO 9001 certified. Ultimo also obtained the SOC2 Type II independent service auditor Assurance Statement.

Overall Compliance

Ultimo in the Cloud is built on a strong foundation of trust, transparency, and compliance. We adhere to globally recognized standards like ISO 9001 to ensure consistent quality and operational excellence. Our platform aligns with key privacy frameworks including GDPR and CCPA, safeguarding customer data across regions and industries.

Security

Protecting customer data is a top priority. Ultimo operates within a security-by-design and by-default framework, backed by certifications like ISO 27001, Cyber Essentials, and SOC 2. These standards reflect our commitment to managing risk, securing availability, confidentiality and integrity, and continuously monitoring for potential vulnerabilities across our ecosystem.

You can request a copy of our SOC2 Assurance Statement Report via our website: **www.ultimo.com/soc-2-type-ii**

Ethical AI Policies

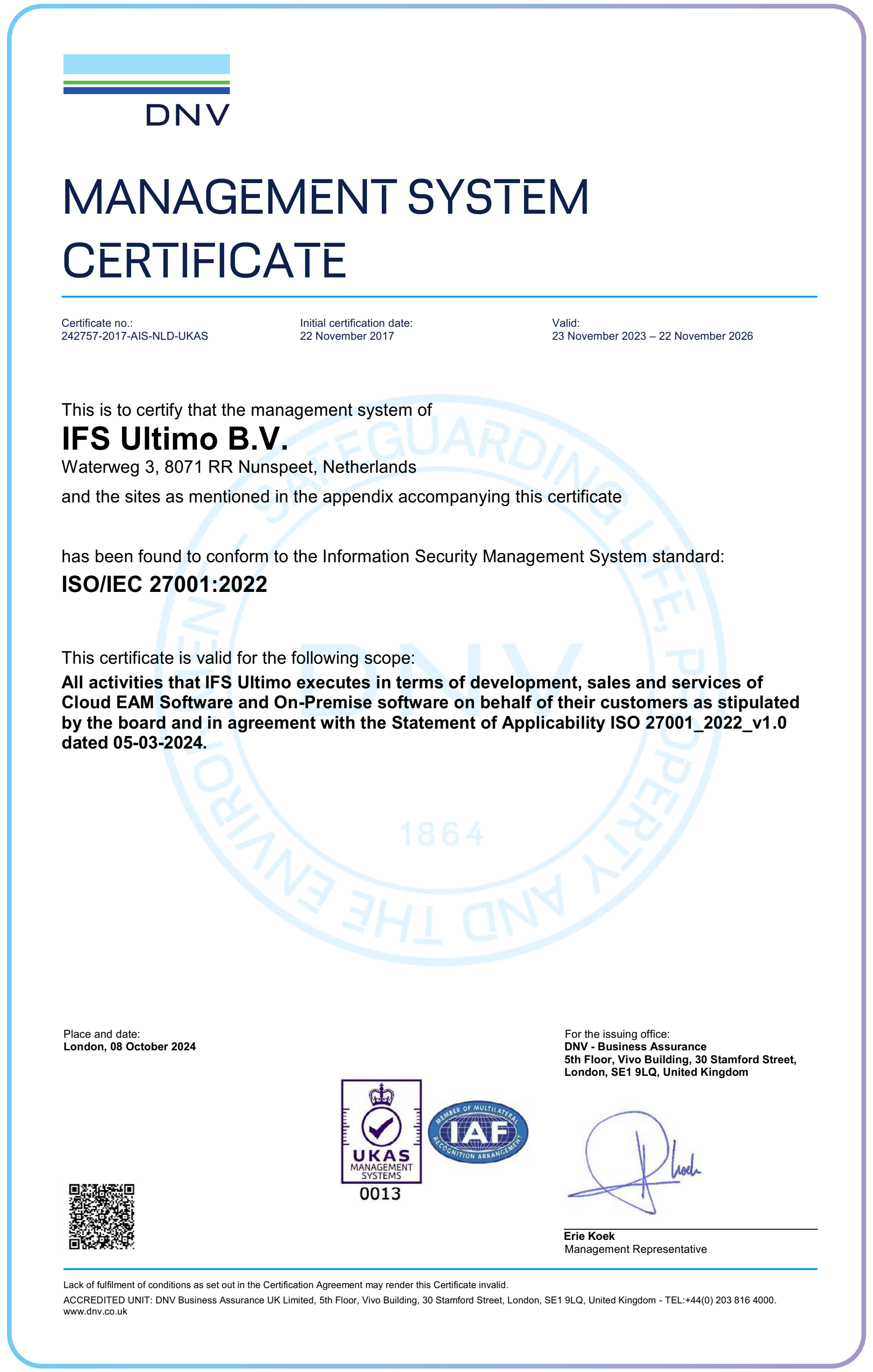
We believe in the power of AI to support smarter, more efficient maintenance and asset management. That's why all AI-driven features are developed and deployed in line with our internal ethical AI policies. These guardrails ensure our use of AI remains transparent, responsible, and low risk, always enhancing the user experience without compromising security or control.

Ultimo Cloud Platform

Best-in-class **features**

- Microsoft Azure Platform
- SOC 2 compliant
- Continuous delivery
- Standard API's
- ON
- OFF
- Feature toggles
- ISO/IEC 27001
- E-learning
- Ultimo an IFS company
- 120K Monthly active users
- Global network
- Single tenant
- 24/7 Availability & monitoring
- Multifactor authentication integration
- Geo-redundant
- 256-bit AES encryption
- 100% SaaS Only internet required
- Infrastructure as Code

Ultimo Certifications



DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate no.:
242757-2017-AIS-NLD-UKAS

Initial certification date:
22 November 2017

Valid:
23 November 2023 – 22 November 2026

This is to certify that the management system of

IFS Ultimo B.V.

Waterweg 3, 8071 RR Nunspeet, Netherlands

and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Information Security Management System standard:

ISO/IEC 27001:2022

This certificate is valid for the following scope:

All activities that IFS Ultimo executes in terms of development, sales and services of Cloud EAM Software and On-Premise software on behalf of their customers as stipulated by the board and in agreement with the Statement of Applicability ISO 27001_2022_v1.0 dated 05-03-2024.

Place and date:
London, 08 October 2024

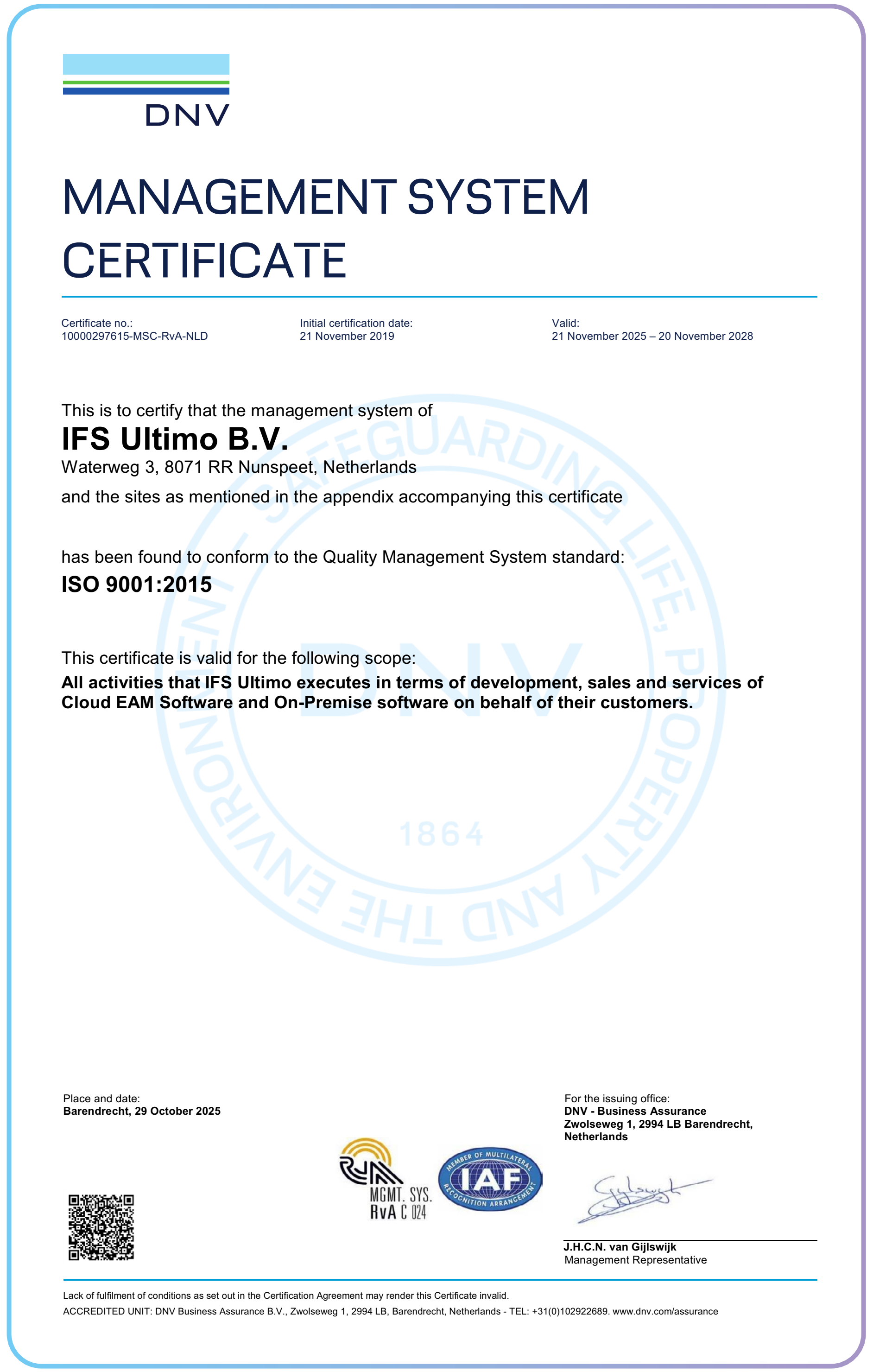
For the issuing office:
DNV - Business Assurance
5th Floor, Vivo Building, 30 Stamford Street,
London, SE1 9LQ, United Kingdom

UKAS MANAGEMENT SYSTEMS
0013

Erie Koek
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

ACCREDITED UNIT: DNV Business Assurance UK Limited, 5th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom - TEL:+44(0) 203 816 4000.
www.dnv.co.uk



DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate no.:
10000297615-MSC-RvA-NLD

Initial certification date:
21 November 2019

Valid:
21 November 2025 – 20 November 2028

This is to certify that the management system of

IFS Ultimo B.V.

Waterweg 3, 8071 RR Nunspeet, Netherlands

and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Quality Management System standard:

ISO 9001:2015

This certificate is valid for the following scope:

All activities that IFS Ultimo executes in terms of development, sales and services of Cloud EAM Software and On-Premise software on behalf of their customers.

Place and date:
Barendrecht, 29 October 2025

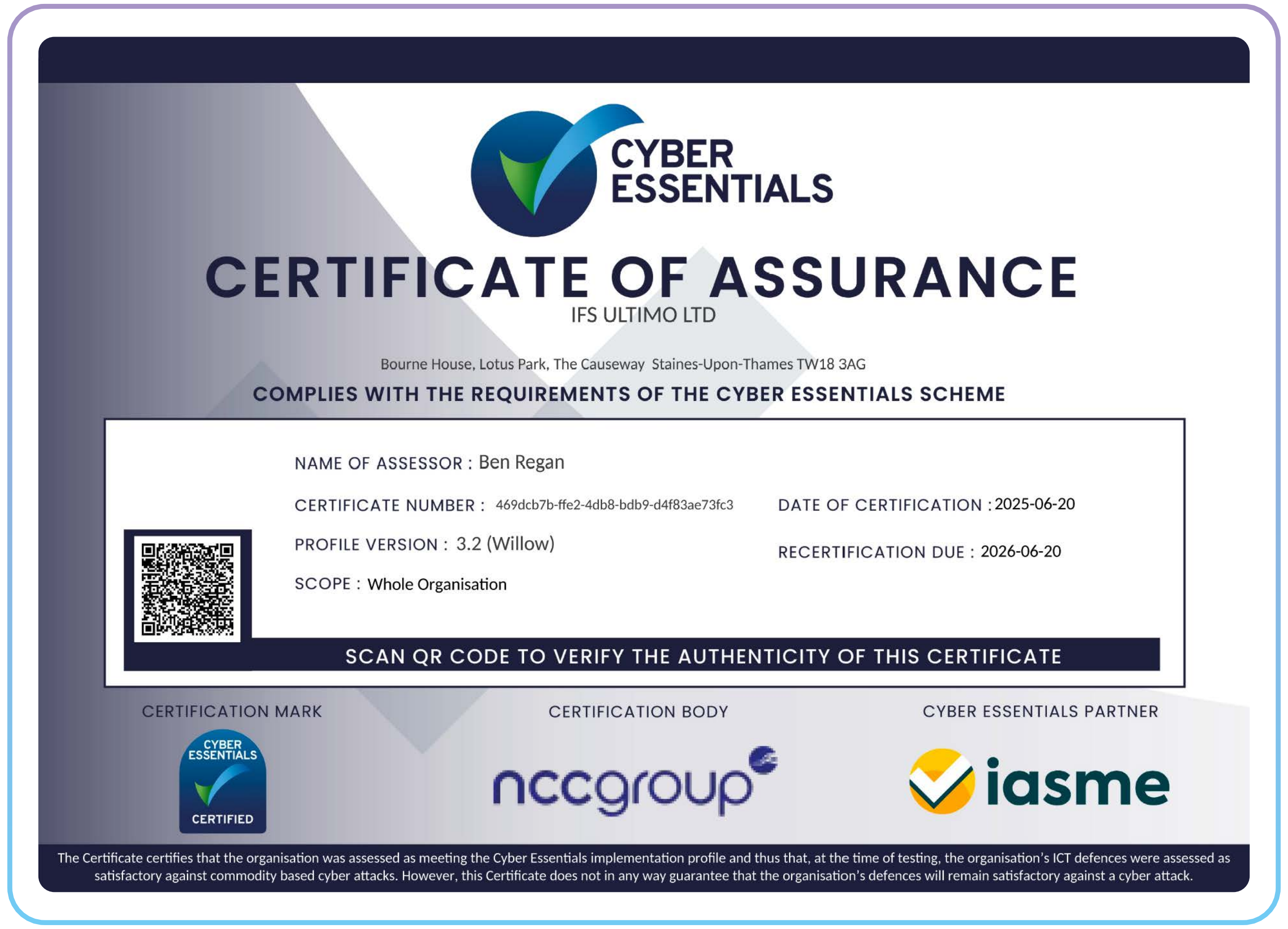
For the issuing office:
DNV - Business Assurance
Zwolseweg 1, 2994 LB Barendrecht,
Netherlands

MGMT. SYS.
RvA C 024

J.H.C.N. van Gijlswijk
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

ACCREDITED UNIT: DNV Business Assurance B.V., Zwolseweg 1, 2994 LB, Barendrecht, Netherlands - TEL: +31(0)102922689. www.dnv.com/assurance



CYBER ESSENTIALS

CERTIFICATE OF ASSURANCE

IFS ULTIMO LTD

Bourne House, Lotus Park, The Causeway Staines-Upon-Thames TW18 3AG

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Ben Regan

CERTIFICATE NUMBER : 469dcb7b-ffe2-4db8-bdb9-d4f83ae73fc3

DATE OF CERTIFICATION : 2025-06-20

PROFILE VERSION : 3.2 (Willow)

RECERTIFICATION DUE : 2026-06-20

SCOPE : Whole Organisation

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK: CYBER ESSENTIALS CERTIFIED

CERTIFICATION BODY: nccgroup

CYBER ESSENTIALS PARTNER: iasme

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attacks. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.

About Ultimo

Ultimo, an IFS company, energizes the financial resilience, regulatory compliance and operational excellence for manufacturing, logistics and healthcare organizations through its AI-augmented software-as-a-service (SaaS) enterprise asset management (EAM) solutions.

Focused on maintenance, uptime, safety, cost control, and efficiency, the Company is known for rapid deployment, ease of use and an unparalleled time to value. Ultimo supports over 145,000 technicians who manage more than 22 million assets for 2500+ customers worldwide. For further information, see Ultimo.com.

© 2025 Ultimo. All rights reserved.

Ultimo and the Ultimo logo are registered wordmarks and logos. Other trademarks used are (non) registered trademarks of the relevant statutory owners.

ultimo.com

Ultimo
an IFS company