# Support and Maintenance for the Monokee Identity and Access Management Platform – SaaS and Dedicated SaaS

Software Defect Correction and Security Vulnerability (CVE) Management

## 1. Introduction and Purpose

This document describes the support and maintenance service that Monokee S.r.l. ("Monokee") provides for the Monokee Identity and Access Management (IAM) platform delivered as a Cloud service, in the following delivery models:

- **SaaS (shared):** a multi-tenant platform in which each Customer has its own logically segregated tenant on infrastructure shared with other customers.
- **Dedicated SaaS:** a single-tenant instance of the platform operated by Monokee on infrastructure reserved exclusively for the Customer.

In both models the service covers the **correction of defects in the Monokee software code** and the **management of security vulnerabilities (CVE)**. Since the platform is operated by Monokee, Monokee is also responsible for applying corrections, security fixes and updates to the production environment. The service is **included in the subscription fee** and does not require any additional purchase.

The availability of the Cloud service, the related service levels and any service credits are governed by the subscription terms and are not covered by this document.

## 2. Scope of the Service

### 2.1 Included in the service

- Diagnosis of reported malfunctions in order to determine whether they are caused by a Defect in the Monokee software.
- Correction of confirmed Defects in the Monokee software code.
- Provision of Workarounds, where available, pending the definitive correction.
- Identification, assessment and remediation of security vulnerabilities (CVE) affecting the Monokee software, the third-party components included in it and the Cloud infrastructure operated by Monokee, as described in Section 8.
- Application of Hotfixes, Patches and new versions to the Customer's tenant or dedicated instance, according to the update policy described in Section 9.
- Publication of release notes and security advisories.

## 2.2 Excluded from the service

- Configuration of the Customer's tenant or instance (for example policies, roles, workflows and connected applications), which remains the responsibility of the Customer.
- Malfunctions caused by systems, applications, identity sources or networks of the Customer or of third parties connected to the platform.
- Installation and updating of any Monokee components installed in the Customer's environment (for example connectors or agents used to integrate on-premises directories or applications). Monokee corrects any Defects in these components and makes the corrected versions available; the Customer is responsible for installing them on its own systems.
- Customizations, integrations or scripts developed by the Customer or by third parties.
- Development of new or custom features, training and consulting activities.

Excluded activities may be requested as separate services and will be quoted separately.

# 3. Definitions

| Term | Definition |
|---|---|
| **Defect** | A reproducible error in the Monokee software code that causes the platform to behave differently from its official documentation. |
| **Workaround** | A temporary procedure or configuration that avoids or mitigates the effects of a Defect or vulnerability pending the definitive correction. |
| **Hotfix** | A targeted correction applied to resolve a specific Defect or vulnerability outside the ordinary release cycle. |
| **Patch** | A software package containing one or more corrections. |
| **Release** | A new version of the platform, including corrections and, where applicable, new features. |
| **Maintenance Window** | A period, communicated in advance, during which Monokee applies updates that may cause a temporary interruption of the service. |
| **Vulnerability / CVE** | A security weakness in the platform or in one of its components. CVE (Common Vulnerabilities and Exposures) is the public identifier assigned to known vulnerabilities. |
| **CVSS** | Common Vulnerability Scoring System, the industry standard used to rate the severity of a vulnerability. |
| **Response Time** | The time between the opening of a request by the Customer and its acknowledgement by a Monokee technician. |
| **Business Hours** | Monday to Friday, 9:00 to 18:00 CET/CEST, excluding Italian public holidays. |

## 4. Delivery Models and Division of Responsibilities

| Activity | SaaS (shared) | Dedicated SaaS |
|---|---|---|
| **Cloud infrastructure, operating systems, databases and runtime** | Monokee | Monokee |
| **Correction of Defects in the code** | Monokee | Monokee |
| **Application of Hotfixes, Patches and Releases** | Monokee, for all tenants at the same time | Monokee, in Maintenance Windows agreed with the Customer |
| **Version of the platform** | Always the current version (N) | Current version (N) or one of the two previous versions (N-1, N-2) |
| **Vulnerability management for infrastructure and software** | Monokee | Monokee |
| **Configuration of the tenant or instance** | Customer | Customer |
| **Systems and applications connected to the platform** | Customer | Customer |
| **Installation of components in the Customer's environment (connectors, agents)** | Customer | Customer |

## 5. Support Channels and Request Management

Requests can be submitted through the following channels:

- **Support portal (self-service):** the Customer contact opens a ticket in the "Support and Assistance" section of the portal.
- **Email to the Service Desk:** the Service Desk registers the request on the ticketing system.
- **Dedicated telephone number:** reserved for Severity 1 requests, which must always be confirmed by opening a ticket.

Every request is registered on the Trouble Ticketing (TT) system with a unique ticket number. The Customer can follow the status of each ticket directly from the portal. Requests are managed through the following phases:

- **Registration:** the ticket is registered and its receipt is acknowledged.
- **Qualification:** Monokee assigns the severity level and checks that the request falls within the scope of the service.
- **Analysis and correction:** the request is assigned to the technical team according to the process described in Section 7.
- **Closure:** the ticket is closed once the correction has been applied to the Customer's tenant or instance, or a Workaround has been provided. Resolutions are recorded in the Monokee Knowledge Base.

# 6. Support Levels and Service Levels

## 6.1 Severity levels

Requests are classified according to the following severity levels, which apply to malfunctions attributable to a Defect in the Monokee software:

| Severity | Definition | Channels |
|---|---|---|
| **Severity 1 – High** | A Defect that prevents the use of a primary function of the platform (for example, authentication or provisioning) and causes the total blocking of the service, with no Workaround available. | Dedicated telephone number, followed by a ticket |
| **Severity 2 – Low** | A Defect that causes the unavailability of a secondary function or a limited, non-permanent disruption that does not significantly affect the service, or a Defect for which a Workaround is available. | Portal, email or telephone |

Security vulnerabilities are classified separately, according to the criteria in Section 8.

## 6.2 Basic Support (included in the subscription)

Coverage during Business Hours, with the following Response Times:

| Severity | Response Time (Business Hours) |
|---|---|
| **Severity 1 – High** | Within 2 business hours |
| **Severity 2 – Low** | Within 4 business hours |

## 6.3 Premium Support (optional)

Quoted separately. In addition to Basic Support, Premium Support extends coverage outside Business Hours (24/7, including weekends and public holidays) with the following Response Times:

| Severity | Response Time (24/7) |
|---|---|
| **Severity 1 – High** | Within 1 hour in 95% of cases; the remaining 5% within 2 hours |
| **Severity 2 – Low** | Within 4 hours in 95% of cases; the remaining 5% within 8 hours |

Service levels refer to Response Times. Since the correction of a Defect depends on its complexity, Monokee does not guarantee a resolution time but will provide a Workaround or correction with priority proportional to the severity.

## 7. Corrective Maintenance – Defect Management

Corrective maintenance aims to diagnose and remove the causes of Defects in the Monokee software code. The process includes the following steps:

- **Qualification:** the Service Desk checks that the request is complete and assigns the severity level.
- **Analysis (Second Level):** the technical team analyzes the information provided by the Customer and the platform logs, reproduces the malfunction where possible and determines whether it is caused by a Defect in the Monokee software or by factors outside the scope of the service. In the latter case the ticket is closed with an explanation.
- **Workaround:** where available, Monokee applies a Workaround on the platform or indicates to the Customer the configuration to be applied on its side.
- **Escalation:** Defects that require changes to the code are escalated to the Monokee development team (Problem Management).
- **Correction and release:** the correction is developed, tested and applied by Monokee to the production environment through its own change and release management process, according to the update policy in Section 9.
- **Closure:** the ticket is closed once the correction has been applied and the Customer has been informed.

## 8. Security Vulnerability (CVE) Management

### 8.1 Scope

The vulnerability management service covers:

- the source code of the Monokee IAM platform;
- the third-party libraries, frameworks and runtimes used by the platform;
- the Cloud infrastructure operated by Monokee, including operating systems, container images, databases and network components;
- the Monokee components installed in the Customer's environment (connectors, agents), limited to the release of corrected versions.

The Customer's systems, applications and networks connected to the platform are excluded.

### 8.2 Identification

Monokee identifies vulnerabilities through:

- continuous monitoring of public sources, including the NVD (National Vulnerability Database), vendor security advisories and the CISA Known Exploited Vulnerabilities (KEV) catalog;
- Software Composition Analysis (SCA) of third-party dependencies, based on the Software Bill of Materials (SBOM) of each release;

- static analysis of the code and security testing performed during the development cycle;
- vulnerability scanning of the Cloud infrastructure and of the container images;
- reports from Customers, partners and independent researchers, received through the coordinated vulnerability disclosure process (Section 8.6).

## 8.3 Assessment and classification

Each identified vulnerability is analyzed to determine whether it actually affects the platform, taking into account whether the vulnerable component or function is used, how it is exposed and whether it can be exploited. Applicable vulnerabilities are classified according to the CVSS base score, adjusted where appropriate to the context of the platform. Vulnerabilities that are being actively exploited (for example, those listed in the CISA KEV catalog) are treated with the highest priority, regardless of their score.

## 8.4 Remediation timelines

Starting from the confirmation that a vulnerability affects the platform, Monokee commits to the following target timelines for applying the correction to the production environment or, where a correction is not yet available, a mitigation:

| Severity | CVSS score | Target timeline |
|---|---|---|
| **Zero-Day** | Any (actively exploited or publicly disclosed, no fix available) | Mitigation applied within 24 hours; correction applied within 2 calendar days of the availability of a fix. |
| **Critical** | 9.0 – 10.0 | Mitigation as soon as possible; correction applied within 30 calendar days |
| **High** | 7.0 – 8.9 | Mitigation as soon as possible; correction applied within 30 calendar days |
| **Medium** | 4.0 – 6.9 | Within 90 calendar days or in the next Release |
| **Low** | 0.1 – 3.9 | In the next scheduled Release |

If a correction depends on a fix released by the supplier of a third-party component, the timelines start from the availability of that fix. In the meantime Monokee will apply, where possible, a mitigation.

Critical and High vulnerabilities may be corrected through emergency Maintenance Windows, including in the Dedicated SaaS model, with the shortest possible advance notice. For components installed in the Customer's environment, the timelines refer to the availability of the corrected version; its installation is the Customer's responsibility.

## 8.5 Zero-day and actively exploited vulnerabilities

A Zero-Day is a vulnerability affecting the platform that is publicly disclosed or actively exploited and for which no correction is yet available from Monokee or from the supplier of the affected component. Zero-Day vulnerabilities are handled through an emergency process, regardless of their CVSS score, and the timelines run from the moment Monokee becomes aware of them. Where the correction depends on a third-party supplier, the two-day timeline runs from the availability of that supplier's fix; in the meantime Monokee applies a mitigation. Where there is evidence that the vulnerability has been exploited against the platform, Monokee also activates its security incident management process and, where Personal Data are affected, notifies the Customer in accordance with Section 7 of Part A of the DPA.

## 8.6 Communication to the Customer

For vulnerabilities rated Critical or High, Monokee will send a security advisory to the Customer's designated security contacts. For vulnerabilities rated Medium or Low, the information will be included in the release notes. Security advisories contain, where applicable:

- the CVE identifier and a description of the vulnerability;
- the affected components;
- the severity and the CVSS score;
- the mitigation and correction applied, or the actions required from the Customer, if any.

On request, Monokee will also confirm whether a specific public CVE affects the platform, including when the vulnerable component is present but cannot be exploited ("not affected" statement).

## 8.7 Coordinated vulnerability disclosure

Suspected vulnerabilities must be reported through the Monokee security contact channel and not through public channels. Monokee will acknowledge receipt of the report, keep the reporter informed of progress and agree with them on the timing of any public disclosure. Details that could facilitate exploitation will not be disclosed until a correction or mitigation is in place.

## 8.8 Customer responsibilities for vulnerabilities

- Designate and keep up to date at least one security contact to receive advisories.
- Promptly install the corrected versions of the Monokee components installed in its environment.
- Manage vulnerabilities in its own systems connected to the platform.
- Report suspected vulnerabilities to Monokee confidentially.

This process supports the Customer in meeting supply chain security requirements, including those set out in the NIS2 Directive.

# 9. Update Policy

## 9.1 SaaS (shared)

All tenants run the current version of the platform. Monokee applies Hotfixes, Patches and Releases to all tenants, in scheduled Maintenance Windows communicated in advance. Updates that do not cause interruptions may be applied without a Maintenance Window. Release notes are published for each Release.

## 9.2 Dedicated SaaS

Monokee agrees with the Customer the schedule of Maintenance Windows for Releases. The Customer may postpone the adoption of a new Release, provided that its instance remains on one of the supported versions (N, N-1 or N-2). Where an instance reaches a version no longer supported, Monokee will agree with the Customer the update to a supported version.

Security corrections for Critical and High vulnerabilities are not subject to postponement and are applied according to the timelines in Section 8.4.

# 10. Customer Responsibilities

In order to receive the service, the Customer agrees to:

- designate qualified contact persons authorized to open requests;
- provide a description of the malfunction and the information needed for the analysis, such as screenshots, the steps needed to reproduce the issue, the users and the time at which the issue occurred;
- collaborate in the reproduction and verification of the malfunction;
- in the Dedicated SaaS model, agree on the Maintenance Windows within a reasonable time;
- install the updated versions of the Monokee components installed in its environment.

Monokee is not responsible for any delays caused by the Customer not fulfilling the above obligations.