Omada Identity Cloud Support Specifications

Last Updated: January 8th, 2025

This Omada Identity Cloud Support Specification ("**Omada Support Specifications**") details the standard support and service level agreement for the Omada Identity Cloud services purchased by the Customer, including the Service Level Objective and applicable Service Credits if the objective is not reasonably met. Capitalized terms used herein, but not otherwise defined, have the meaning set forth in the Customer Agreement between Omada and Customer.

1 DEFINITION OF SERVICE

1.1 **Information Security**. Omada operates and maintains the Omada Identity Cloud for the Customer in accordance with Omada's ISO 27001 implementation defined in the Omada internal Information Security Management System (ISMS). Omada Identity Cloud is independently audited annually according to the American Institute of CPAs (AICPA)'s Service Organization Control Program. The SOC 3 Type 2 audit report is made available via Omada's online Trust Center.

1.2 **Omada Service Support**. Omada provides monitoring, scaling and operations of the Omada Identity Cloud in accordance with Service Level Objectives. Omada provides Upgrades and Patches according to the maintenance schedule defined in this document. Omada performs service disaster recovery including backup and restore operations. Backup restore operations due to the Customer's actions are subject to a formal change request process and additional service fees. Omada may access Customers usage data information in aggregated and anonymized form for the limited purpose of the improvement of the product.

1.3 **Service Delivery & Support Center**. Omada provides support for incidents and service request via the Omada Service Delivery & Support center as single point of contact, available according to the below defined schedule and service levels.

1.4 **Environments**. The services provided for the Omada Service Support include Production Environment(s) and Non-Production Environment(s) specified in the Order Forms. The Service Level Objectives apply only to the Production Environment(s). The Non-Production Environment(s) are provided at commercially reasonable best efforts to the Customer with the objective of 24x7x365 availability.

1.5 Definitions:

	Production	Non-Production
High Availability (SLA of 99.5%*)	Yes	Best effort
Multi-Region Disaster Recovery	No/ optional*	No
Regional Redundancy	Yes	Yes
Disaster Recovery	Yes	No
Backup retention	7 days Point in Time Recovery Weekly LTR for 52 Weeks Monthly LTR for 12 Months Yearly LTR Backups for 5 Years	7 days Point in Time Recovery
Scalability/Elasticity	Full	Limited
Deletion prevention	Yes	No
OnPrem Connection	IKEv2	IKEv2
Phase 1 DH Groups	DH1, DH2, DH14, DH2048, ECP256, ECP384, DH24	DH2
Phase 1 Encryption/Hashing Algorithms	GCMAES256, GCMAES192, GCMAES128, AES256, AES192, AES128, DES3, DES, None	AES256, AES128, 3DES SHA256, SHA128, SHA1

	GCMAES256, GCMAES192, GCMAES128, SHA256, SHA1, MD5	
Phase 2 PFS Groups	PFS24, ECP384, ECP256, PFS2048, PFS2, PFS1, None	PFS24, PFS14, PFS2, PFS1, NONE
Phase 2 Encryption/Hashing Algorithms	GCMAES256, GCMAES128, AES256, AES192, AES128 SHA384, SHA256, SHA1, MD5	GCM AES256, AES256, AES128, 3DES GCM AES 256, SHA256, SHA1

*In case Multi-Region Disaster Recovery (DR) is separately purchased the SLA availability increases to 99.9%.

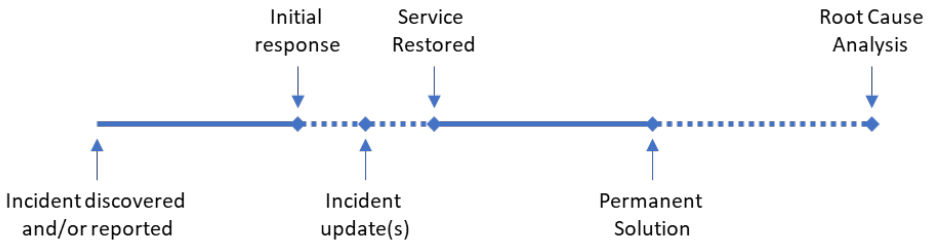
2 INCIDENT MANAGEMENT

2.1 **Objective**. At Omada, our main objective is to deliver flawless services to our customers. Should an event or occurrence occur that disrupts the normal operation and performance of the Omada Identity Cloud, including any service outage, degradation of service quality, security breach, or any failure in the service infrastructure that affects the user's ability to utilize the Omada Identity Cloud as set forth in the Agreement (each an "**Incident**"), we follow the following processes.

2.2 **Service and Support Hours**. The Omada Service Delivery and Support organization operates during the following opening hours:

Service Level Target	Details	SLA
Service Hours	The time period where the Services covered are expected to be available and where Incident Management will be performed	24 hours a day 7 days a week
Support Hours	The time period where the Service Delivery and Support desk is manned and actively monitoring and working on incident tickets.	24 hours a day 7 days a week
Self-service Portal	The time period where the self-service portal for administrators is available.	24 hours a day 7 days a week
General Service Requests	The time period where individual service requests can be logged and fulfilled.	24 hours a day 7 days a week Scheduling of fulfillment of the individual service requests is agreed upon by the parties based on urgency and resource availability. Expected fulfillment within 5 business days.

2.3 **Resolution Process**. The resolution process for incidents will be managed by Omada in accordance with the following process and timescales:



Incident Report Severity Level	Time to Initial Response as of the Incident Report	Incident Updates	Time to Restore as of the Incident Report	Permanent Solution available for Customer
Critical	Within 1 (one) hour as of the report of the Incident made by telephone (*) and Omada Service Delivery and Support portal, 24x7x365.	Every 30 (thirty) minutes	2 (two) hours	Omada shall undertake to work continuously until permanent solution has been delivered, delivery to be made at the latest 10 business days as of the day of the incident report.
Major	2 (two) hours, during Business Hours, as of the report of the Incident made by telephone and Omada Service Delivery and Support portal.	Every hour, during Business Hours	4 (four) hours, during Business Hours	One calendar month
Minor	4 (four) hours, during Business Hours, as of the report of the Incident made by telephone and Omada Service Delivery and Support portal.	-	12 (twelve) hours, during Business Hours	Next update of the Service, but no later than 3 (three) calendar months
Low & Service Request:	5 (five) business days	-	To be agreed case by case	To be agreed case by case

(*) The Customer shall provide Omada with phone number(s) that Omada can use to contact the Customer 24 hours per day, 7 days a week, for updates and further troubleshooting.

A Root Cause Analysis (RCA) is to be delivered no later than 10 business days after a permanent solution has been made available to the Customer for Critical incidents. RCAs for Major incidents can be requested by the Customer and will be delivered no later than 20 business days after permanent solutions has been made available. RCAs are only provided for Production Environments.

3 INCIDENT CLASSIFICATION

3.1 **Definition**. Incidents are classified using the following definition:

Severity	Description
1 – Critical	Critical Incidents affect the entire Omada Identity Cloud. No users and customers can access the Omada Identity Cloud. Business is impacted. Incidents classified as security related are categorized as Critical if loss of data, information disclosure, etc. is realistically possible. Critical incidents can only be raised for Production Environments
2 - Major	Major Incidents affect a large number of users and/or customers, interrupt business, and affect service delivery. These incidents almost always have a financial impact.
3 - Minor	Medium-priority Incidents affect a few staff and interrupt work to some degree. Customers may be slightly affected or inconvenienced.

Severity	Description
4 - Low	Low-priority incidents are those that do not interrupt users or the business and can be worked around. Services to users and customers can be maintained.

3.2 **Service Boundaries (Out-of-Scope)**. Omada is not obliged to manage and remedy incidents that are related to data quality, system connectivity or any other elements of the customer specific use of the Omada Identity Cloud.

3.3 **General Service Activity Matrix**. The service activities to maintain the Omada Identity Cloud for all Omada customers:

Activities/ process	Descriptions	Frequency
Incident Management	Re-establishment of normal service as quickly as possible and with minimization of adverse effects to the utility delivered by the Services. Incidents are solved based on workarounds and solutions. If no workaround or solution exists, Omada takes full responsibility for solving the incident with engagement of their cloud service provider(s) if needed.	Continuously
Cloud Upgrades	Cloud Upgrades (CUs) are released on a regular cadence as defined from time to time in the published release calendar. The dates for CUs are communicated in Omada's Know-How Platform (the HUB). It is the Customer's responsibility to ensure that the configuration of the Service as deployed is prepared to support the new version.	Deployed version on Non-Prod and Prod environments must not be older than two CUs back from the recent CU
Service Upgrade	Major releases are evaluated and implemented. It is the Customer's responsibility to ensure that the customization of the Omada Identity Cloud as deployed is prepared to support the new version. Release management is coordinated with Customer. Major releases are defined as new generations e.g. version 14 update 3 to version 15	Not later than 90 days after release for Production Environment Not later than 30 days for Non-Production Environments
Reporting	Reporting on relevant application-specific measures such as usage, potential bottlenecks, resource load, capacity usage etc. with recommendations for future improvements. Reporting of Managed Identities in the Service.	On Request

3.4 **Business Continuity Obligations**. Omada is responsible for backing up the Omada Identity Cloud and having the ability to restore the Omada Identity Cloud to a Recovery Point Objective (RPO) that is no older than 15 minutes. The Recovery Time Objective (RTO) of full service recovery is 240 minutes. Yearly DR test reports are available on request.

3.5 **Backup and Retention Obligations**. Databases are backed up using the following schedule:

Full Backups

- Every Day - Retained for 30 days
- Every Week - Retained for 5 weeks
- Every Month - Retained for 12 months

Delta Backups

- Every 15 Minutes - Retained for 30 days

The Backups are performed at the end of the period (i.e. 23:59 (every day), Sunday 23:59 (every week), etc.) in the leading time zone of the delivery region (as agreed in the Order Form).

The backup integrity is tested monthly, and the backup restoration test is performed annually. Omada is obligated to validate that the backup integrity is tested as described.

Omada will perform a full backup of the Omada Identity Cloud before carrying out platform Upgrades, in order to be able to roll-back the changes if and as necessary.

4 PREREQUISITES AND RESTRICTIONS

4.1 **Prerequisites**. The prerequisites required in terms of information from the Customer, or other Customer input of any form (e.g. processes, data, personnel, expertise), and any restrictions that may apply to the Omada Identity Cloud:

Prerequisite & Restriction	Description
Administrative access to application	The installation and configuration of the Omada Identity Cloud are done by Omada, and only Omada personnel are granted administrative privileges on application environments, where Omada has KPIs to meet.
Patches and Upgrades	The term "**Patches**" refers to minor releases such as bug fixes and security updates provided to fix minor issues for an application or application component. A Patch can be applied without customizations/adjustments of the application and with no special considerations regarding data transformation. The term "**Upgrade**" refers to a new version of the Omada Identity Cloud that requires considerations with regards to either other application components, related infrastructure or underlying data. In case any customer-specific configurations or changes are made to the Omada Identity Cloud only Patches are included in the subscription fee. In this case Upgrades are not included in the subscription fee, as changes will be required that require the conclusion of a separate Statement of Work between the Customer and Omada.

5 SERVICE LEVEL OBJECTIVE

5.1 **Objective**. Omada will use commercially reasonable efforts to make the Omada Identity Cloud available 24x7x365 to Customer. The Service Level Objective of Omada Identity Cloud is to achieve System Availability of Production Environments of at least 99.5% during all calendar months of the Order Term. In case Multi-Region Disaster Recovery (DR) is separately purchased this increases to 99.9%.

5.2 **System Availability**. "**System Availability**" means the percentage of minutes in a calendar month that the Omada portal in a Production Environment is operational, excluding Service Interruptions.

The System Availability is calculated as:

$$System\ Availability = \frac{Total\ minutes\ in\ period - Total\ minutes\ of\ Service\ Interruption}{Total\ minutes\ in\ period}$$

"**Service Interruptions**" are all times (in minutes) during which the Omada portal is not operational for the Customer, provided, however, that the following occasions of non-operability are not counted as Service Interruptions:

a) planned major Upgrades as agreed between the Parties,
b) planned downtime,
c) events of Force Majeure,
d) malicious attacks on the system, and
e) issues related to the Customer's environment outside of Omada's control.

Example:

- Minutes in period: June 2018 had 30 days x 24 hours x 60 minutes = 43.200 minutes in total
- Service Interruption: 100 minutes
- System Availability = (43.200 – 100) / 43.200 = 99.8%

Operational state is monitored and reported on a continued basis based on probes set on the Omada Portal website.

5.3 **Planned Downtime**. Omada reserves the right to take the Omada Identity Cloud offline for scheduled maintenance for which Customer has been provided reasonable notice. Notice is given at least one calendar week in advance unless impossible due to the criticality of the maintenance (patching for security reasons or the like). In the latter case, the notice period may be shorter and, in urgent cases, not apply. The Omada Identity Cloud can be taken offline for up to a total of 8 hours a month for planned maintenance work. Such maintenance work is scheduled outside of Customer's business hours where possible. No downtime can be longer than 4 hours in duration, and only one downtime can be planned in a calendar week. Omada can perform non-interrupting maintenance as needed without notifying the Customer.

5.4 **Monthly Planned Downtime**. A monthly preventive scheduled downtime window, included in the above allotment, is reserved on the 3rd Saturday of the month from 21:00 to 23:59 CET/CEST. Omada strives to make the duration if this window as short as possible and/or non-disruptive.

5.5 **Service Credits**. If Omada fails to meet the System Availability, for any month during the applicable Order Term, the Customer is entitled to receive a Service Credit, upon written request by Customer within 30 days after the end of the month. A credit will be applied to the Customer's next invoice equal to 5% of the monthly fee for the affected Services for each 1% loss of System Availability below stated. Such credit is capped at 50% of the Customer's monthly fee for the affected Omada Identity Cloud in the applicable Order Form.

5.6 **Termination**. In the event Omada fails to achieve 98.9% Service Availability for 3 consecutive months during any 12-month period or 5 months during a calendar year period, the Customer will have the option, in its sole discretion, to terminate the applicable Order Form in accordance with Section 7.2 of the Agreement.

5.7 **Exclusive Remedy**. The remedies set forth in Sections 5.5 and 5.6 of these Omada Support Specifications shall be the Customer's sole and exclusive remedies for any failure by Omada to meet the Service Level Objectives under the Agreement. These exclusive remedies replace and supersede all other remedies, whether statutory, contractual, in tort, or otherwise, available to the Customer under any law or equity.