Service Level Agreement

(Service Description)

Inventory as a Service

Code: FS-KIE
Version: 3.0
Valid from 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com
HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219
Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797
www.cancom.at

Service of the contractor

This document describes the services of the service module, which are provided as part of the contract concluded between the client (CL) and the contractor (CO). The responsibilities of the services described are based on a RACI model. Explanations of terms and contact information for the Customer Service Center can be found under the following link.

Unless otherwise agreed, the following service goals apply as standard: Service time "SNAZ" (NWH) with a response time of 4 hours.

Inventory as a Service

By using the Inventory Engine, the most important questions and problem areas surrounding a network infrastructure can be answered.

Initial Services	CO	CL
Imaging of the appliance: latest operating system incl. patches, latest CANCOM application	R/A	C/I
Pre-configuration of the CANCOM Inventory Engine (hardware appliance, mini industrial server) with regard to customer data (IP address, DNS/NTP etc.), then sent to the customer	R/A	C/I
Remote commissioning and adjustment regarding customer setup (mail relay, LDAP connection, etc.)	R/A	C/I
Definition of the management networks or hosts to be managed	R/A	C/I
Connection tests to the infrastructure devices (switches, routers, access points, etc.)	R/A	C/I
Setting up users and authorization structure including notifications	R/A	C/I
Initial configuration of the discovery job	R/A	C/I
Connection test (HTTPS) to the CANCOM data center in Vienna for data enrichment regarding EoX, security vulnerabilities, licensing, etc.	R/A	C/I
Local or remote backup control	R/A	C/I
Creation and test VPN setup (Site2Site or Client-VPN) for CANCOM to regularly patch system"	R/A	C/I

Recurring Services	CO	CL
Deployment of Linux Appliance / Inventory Engine		
The contractor provides the client with a hardened Linux appliance (hardware form: mini industrial server) on site. The Inventors Engine runs on this system and provides the client with a modern user and administration interface via a web interface (HTTPS).	R/A	C/I

The system is initially configured for the client's environment as part of the installation fee (IP address, subnet mask, def gateway, DNS/NTP, mail relay, LDAP/MS-AD connection, etc.). Depending on the settings, the system scans the client's entire network infrastructure once a day and thus detects changes and deviations, which are documented in so-called snapshots. The client thus has a daily updated "live CMDB" of its Cisco network landscape.		
System Security		
The highest security standards apply to the Inventory as a Service service. Only encrypted protocols (HTTPS, SSH) are used, the data partition of the Linux system is natively encrypted (two-stage process), and no unencrypted passwords (login data encrypted with "salted hash values", discovery credentials and API tokens) are stored in the database. Communication with the contractor's Vienna data center for data enrichment (end-of-X, security vulnerabilities, etc.) takes place via HTTP/TLS (TCP port 443) to a single official owned public IP address of the contractor in Vienna. No personal data, configurations, settings or backups are transferred to the contractor's data center. Due to the security design and architecture, there is NO push function, the contractor cannot establish or initiate a connection to the client's system. The Inventory Engine retrieves information from the contractor's data center via HTTPS, such as new security vulnerabilities or End-of-X (sales, service, software) information that has been published, and correlates this with the client's installed base. In the interests of maximum security and 100% transparency, the client can specify the data fields transmitted to the contractor in the web GUI. Selecting or deselecting the data fields can slightly limit the range of functions of the IE, depending on the choice. The contractor's Vienna data center is certified according to internationally recognized information security standards such as ISO/IEC 27001.	R/A	C/I
Troubleshooting		
The faults reported by the client or identified by the contractor regarding the Linux appliance (operating system) or inventory web application are analyzed, processed and resolved by the contractor. Examples are: errors, bugs in the web interface, system crashes, unplanned reloads, incomplete data records, data loss, problems recognizing special or new device types, etc. If it is not possible to resolve errors and faults immediately, or there are dependencies on third parties (e.g. Cisco IOS software), the contractor will endeavor to minimize the effects of the fault using a workaround. The resolution of third-party faults is NOT part of the service and must be handled via other existing processes. If there is a hardware defect in the Linux appliance provided by the contractor, a replacement (RMA exchange) will be offered with a maximum response time of next business week. The client's last saved configuration status (backup) will be used. For data protection reasons and with regard to confidential information or configurations, none of this data will be transferred to the contractor or backed up. The responsibility for a "current" backup lies with the client. In the Inventory Engine, there are manual (web GUI download) or professional backup options (automated, daily SFTP backup) so that a current backup is stored on site at the client's premises. In the event of a hardware failure, the client provides the contractor's technicians with an IE backup for the restore, the system recovery.	R/A	C/I

If the client does not have a backup, the new installation, setup or configuration will be invoiced depending on the scope and requirements.		
Patches, hotfixes and security updates		
The contractor carries out patch management for the operating system (Rocky Linux) every six months in coordination with the client, unless there is an urgent need for action (e.g. serious security gap with CVSS 10) that requires immediate intervention. The prerequisite is functioning, tested remote access (Citrix, VPN solution, etc.) between the contractor and the client, and at least a temporary HTTPS connection to the Internet in order to update the operating system packages (RPMs). The contractor's own web application can be updated and patched by the client himself via the web interface. Product improvements, new functions and hotfixes are constantly being added, which the client can download and install independently by confirming. When the appliance or the web application is restarted, there is NO impact on the client's services! The system is a valuable helper in the network infrastructure, but is in no way involved in data transport. Read-only SSH access (various show commands) also ensures 100% that our inventory as a service does not cause any changes in the client's environment. Restarting or stopping the services on the inventory engine has no service impact for the client!	R/A	C/I

Obligation of the client to cooperate	CO	CL
Provision of users and permissions		
The client ensures that there is a read-only SSH user for the inventory engine on all devices to be integrated (switches, routers, WLAN controllers, etc.). The read-only rights can also be restricted to dedicated "show commands" using the TACACS protocol. Existing users can of course be used, but for better separation and traceability, a separate user for "inventory as a service" is recommended. In large environments, a central directory service is usually used (e.g. Microsoft Active Directory), which is available for authentication via a RADIUS server (e.g. Cisco ISE, MS NPS, etc.) of the network infrastructure. In these cases, the client creates a central user for the inventory engine that works on all devices. The creation of the read-only SSH user is an important requirement on the client side. Write rights, i.e. write commands or configuration changes, are never required using the inventory engine. It is a passive system for lifecycle and asset information, not a management or monitoring tool etc. The client ensures a functioning connection, IP communication between the inventory engine and the network devices to be managed (routers, switches, etc.). All adjustments such as routing tables, access lists, firewall rules, NAT rules, VPN tunnel extensions, provider adjustments, WAN adjustments (MPLS/SD-WAN), etc., or extensive troubleshooting, are not included in the scope of services with regard to these points and must be carried out by the client.	C/I	R/A
Requirement: Secure Shell		
Devices that do not offer or have activated Secure Shell (SSH) by default, e.g. wireless LAN controllers, Cisco ISE, etc., must be prepared by the client if they are to be managed using the Inventory Engine.	C/I	R/A

Framework conditions for service

At the end of the contractual relationship, the client's data will be deleted by the contractor within one month. If requested, the client's existing data can be copied to media and handed over for a fee before deletion.

Services not included

Configuration of the SSH user for the inventory engine on the devices to be managed, or the central directory service (RADIUS)
Enabling or activating SSH on devices to be managed
Configuration adjustments & intensive troubleshooting of communication problems between Inventory Engine and the client's network components: routing tables, access lists, firewall rules, NAT rules, VPN tunnel extensions, provider adjustments, WAN adjustments (MPLS/SD-WAN), etc.
Configuration changes on the devices to be managed (routers, switches, APs, etc.)
Updates/upgrades on the network infrastructure
Real-time monitoring of the engine located at the client (client integrates the inventory engine into the existing monitoring system)
Setting up new functionalities (features)
Preparation of special reports
Cisco devices or products that are not in the LAN, WAN, WLAN, DC area Network infrastructure from third parties (e.g. Aruba, Fortinet, Avaya, Juniper, etc.)
Reports with security-relevant information from the logs