Conscia Assist

Service Description

July 2024
Version 2.1

Conscia Contact

Conscia Deutschland GmbH - Head Office Ettlingen

Otto-Hahn-Str. 18
76275 Ettlingen
Germany
Phone: +49 7243 5054-4
Fax: +49 7243 5054-899
Mail: kontakt@conscia.com

www.conscia.de

Document Control

Version	Date	Changes	Processor	Release
1.0	March 15, 2024	New Conscia Care service description	Ulrich Brüll	Ulrich Brüll Andreas Wiesert
2.0	May 25, 2024	Revision	Jörg Fritz	Ulrich Brüll Markus Zumbeel
2.1	July 15, 2024	"Advance" changed to "Enhanced"	Jörg Fritz	Ulrich Brüll Markus Zumbeel

Table of contents

1. Introduction 5
1.1. Conscia Service Overview 5
1.2. Conscia Care 6
1.3. Conscia Assist 6
1.4. Conscia Premium 6
2. Scope of services Conscia Assist Service 7
2.1. General 7
2.2. Conscia Assist service content 7
2.2.7. Incident management with remote support 8
2.2.8. Description Conscia Service Portal CNS - Best Practices Level 9
2.2.9. Regular CNS Lifecycle Meetings 10
2.2.10. Flexible service contingent 11
3. Conscia Assist Services Definition 13
3.1. Definitions of terms 13
3.2. Fault classification and prioritization 14
3.2.1. Damaging effect of a disruption 14
3.2.2. Urgency of a fault 15
3.2.3. Disruption priorities 15
3.2.4. Response times 15
3.3. Service level conditions for End-of-X 15
4. Setup and conditions for Conscia Assist Services 17
4.1. Designation of contact person 17
4.2. Setting up a customer account in the CNS portal 17
4.3. Installation CNS-Collector 17
4.4. Linking the ITSM systems 17
4.5. Use of hardware and software 17
4.6. Exceptions and delimitations 18
4.7. Contractual conditions 18
4.8. Additional information 18
5. Appendix A - Conscia Assist Service Level Agreements 19
6. Appendix B - Conscia OneNoc Description 20
7. Appendix C - CSPC collector and CNS installation 21

7.1. CSPC Server - Requirements 21
7.2. CSPC firewall - necessary releases 21
7.3. CSPC installation - Description 21
7.4. CSPC integration in CNS 21

List of Pictures

Picture 1 Conscia Service Overview 6
Picture 2 Conscia Assist - Incident Management Options 8
Picture 3 Conscia Assist - CNS Functions 10
Picture 4 CNS – Manufacturer Note 10
Picture 5 Conscia Assist - LCM options 11
Picture 6 Conscia Assist - hourly quota Changes 12

List of tables

Table 1 Conscia Assist contents 7
Table 2 Definition of terms 13
Table 3 Damage effect 14
Table 4 Urgency 15
Table 5 Fault priorities 15
Table 6 Response Times 15
Table 7 End-of-X definition 16
Table 8 SLA 19
Table 9 CNS CSPC System Requirements 21
Table 10 CNS CSPC Firewall Requirements 21
Table 11 CNS CSPC Additional Requirements 21

1. Introduction

1.1. Conscia Service Overview

This document describes the Conscia Assist Service as part of Conscia's overall service portfolio. This service description explains the available service components.

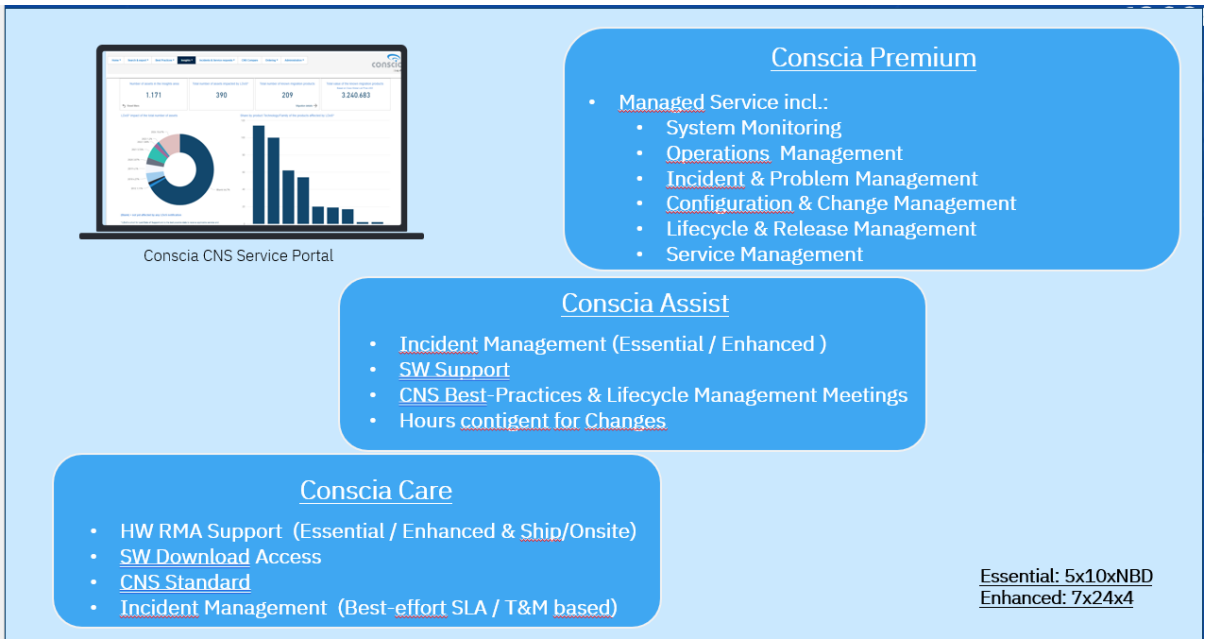
Conscia Services provide support and operation of IT infrastructures for LAN, WLAN, DataCenter Networking, Security and Hybrid Work environments and
enable you to support your infrastructures optimally and cost-efficiently, thereby minimizing downtimes and disruption times.

The Conscia Services provide various service functions in modular form from which you can choose how your infrastructures and your own support and operational organizations are optimally supported and supplemented.

Conscia services range from reactive hardware replacement services to proactive managed services with operational responsibility.

All Conscia services automatically include access to the Conscia CNS Service Portal. With the Conscia CNS Service Portal, we centralize and automate the entire asset lifecycle and provide all contractually agreed services in one portal.
The Conscia CNS Portal has direct connections to the manufacturer's systems and provides recommendations on available updates for hardware and software.
CNS allows your entire infrastructure to be documented and kept up to date through regular scans.
You also receive overviews of known potential security gaps within your infrastructure and information on how these can be closed.
For budget planning, CNS provides information that shows which investments need to be made in subsequent years in order to keep your infrastructures at a supportable and up-to-date level.
The CNS portal is also used for all ticket and RMA processing, which can also be integrated into your own ITSM fault and asset management system.

Conscia Services Overview:



Picture 1 Conscia Service Overview

1.2. Conscia Care

Conscia Care forms the basis of all Conscia services and is to be understood as a purely reactive hardware replacement service (RMA) that supports the customer in rectifying faults in the operation of hardware.
The service is always linked to a specific hardware component, hereinafter also referred to as an "asset", and is based on a partner service from the manufacturer.

In a customer infrastructure, different assets can have different SLAs from Conscia Care and the manufacturer support. When Conscia Care is commissioned for an asset, the necessary support from the manufacturer is commissioned by Conscia and
managed.

Conscia Care also includes access to the manufacturer's software download area for independent software updates and upgrades.

1.3. Conscia Assist

Conscia Assist is an extension of Conscia Care to include incident management services for fault management in the customer infrastructure, asset & lifecycle management, software support and the processing of service requests for defined service level agreements (SLA).

1.4. Conscia Premium

Conscia Premium describes a managed service for the proactive monitoring and implementation of recurring services in the customer's IT infrastructure. Conscia generally assumes overall responsibility for the operation of the agreed systems.

2. Scope of services Conscia Assist Service

2.1. General

In contrast to the Conscia Care Service, the Conscia Assist Service not only considers the individual hardware, software and service components (assets) of a manufacturer, but is a service that holistically covers the customer's infrastructure and the interoperability between individual hardware, software and service solutions. Conscia Assist is offered for the supported manufacturers in the areas of networking, security and hybrid work.

The basis for Conscia Assist is a valid Conscia Care contract for the assets in the customer infrastructure. Without Conscia Care, no hardware support can be provided for the assets.

As this document is a generic service, the functionality of the respective hardware and software is not described in detail here.

2.2. Conscia Assist service content

The following overview shows the different service levels and functions currently available in Conscia Assist:

Pos	Service	**Conscia Assist SLA**	
		Essential	**Enhanced**
2.2.1 - 2.2.6	**Conscia Care Essential** or **Conscia Care Enhanced**, (Ship or Onsite) see Conscia Care service description 2.2.1 - 2.2.6	required	
2.2.7	**Incident management** with remote support response times: P1: 1h, P2: 2h, P3: 4h, P4: NBD	10x5	24x7*
2.2.8	Access to the **Conscia Service Portal CNS - Best Practices Level** with Asset & Lifecycle Management and Insights	included	
2.2.9	Regular **lifecycle management meetings** to discuss CNS best practices, asset & lifecycle management and insights	Semi-annual	Quarterly
2.2.10	Flexible **hourly quota** for processing consulting, change and service requests	10x5xNBD	

Table 1 Conscia Assist contents

** 24/7 on-call service for priority 1 and priority 2 incidents*

2.2.7. Incident management with remote support

If the customer detects a fault in the infrastructure covered by Conscia Assist, this fault can be reported to the Conscia Service Desk via the specified reporting channels.

Incident management and fault analysis and processing are always carried out remotely. For this purpose, the customer must provide remote maintenance access for the Conscia service employees.

In the event that the Conscia Service Desk requires additional support from the manufacturer, the necessary support tickets will be opened with the manufacturer and processed by the Conscia Service Desk.

If the fault was caused by a non-functioning hardware component, replacement components are provided in accordance with the valid Conscia Care service contract. Depending on the selected service level, the hardware is sent (ship) and the customer carries out the replacement themselves or a service technician (onsite) replaces the hardware on site.

Depending on the priority of the fault in accordance with 3.2, Incident Management is started with the following response times:
Priority 1 (P1): 1h
Priority 2 (P2): 2h
Priority 3 (P3): 4h
Priority 4 (P4): Next Business Day

Conscia Assist - Incident Management Options:

- Conscia Assist Essential (10x5) includes incident management from 8:00 - 18:00 CET from Monday - Friday, excluding national holidays in Germany.
  Conscia article number: CON-ASS-ESS

- Conscia Assist Enhanced (24x7) includes incident management from 0:00 - 24:00 CET from Monday - Sunday
  Conscia article number: CON-ASS-ENH

Picture 2 Conscia Assist - Incident Management Options

Remote maintenance connection
For remote diagnostics and remote maintenance, the system installed at the customer's premises is linked to the Conscia remote management system in accordance with the Conscia OneNOC description (see appendix). The technical requirements for this must be provided by the customer.

The data connection will only be established with the customer's prior consent and in compliance with the information security measures previously agreed with the customer.

2.2.8. Description Conscia Service Portal CNS - Best Practices Level

With Conscia Assist, the following additional functions called "**Best Practices**" are made available to the customer on the CNS customer portal:

- **Insights**
  - Inventory Dashboard
    - Service level details & product age
    - Asset location with associated installation locations
  - Product Lifecycle Dashboard
  - Dashboard software version (collector required)
- **Lifecycle & Best Practices**
  - Dashboard software version (collector required)
  - Software LifeCycle Overview
  - Product lifecycle & migration recommendations
- **Security**
  - Vulnerability overview
    - Conscia recommendations for action (collector required)
  - Field Notices Overview (collector required)
    - Conscia recommendations for action

2.2.8.1. CNS Insights

The Insights module contains dashboards for inventory, product lifecycle and software versions with a corresponding export function. The inventory dashboard gives you an overview of your assets, their location and the SLA agreed for the asset. It allows you to take a closer look at the service levels, location details and the age of the product.

The Product Lifecycle Dashboard shows you when assets reach their LDoS (Last Date of Support) and provides corresponding recommendations for action. It also provides a breakdown of the affected assets by product family. The Product Lifecycle Dashboard also includes a migration overview, where you can see the optimal replacement for an affected asset and the migration product.

The Software Versions Dashboard shows which software versions are installed, including a breakdown by product family. You can compare the software versions of your assets with Conscia's recommendations to keep your software versions up to date.

2.2.8.2. CNS Best Practices

The Best Practices module helps you stay up to date on software versions, software lifecycle, product lifecycle, migration recommendations, security vulnerabilities and Cisco field notes.

The software life cycle shows you an overview of the software version and the associated End of Sale (EoS), End of Software Maintenance, End of Maintenance Releases, Bug fixes, and the Last Day of Support (LDoS) date.

The Product Lifecycle & Migration module provides you with an overview of End of Sale, Software Maintenance, Service Renewal, Last Day of Support, and Security Support for the devices.

The summary also shows the comparable asset for a product migration, pricing details and the service list prices for the new product.

2.2.8.3. CNS Security

The Vulnerability Module shows known vulnerabilities and potentially affected assets. The vulnerabilities are published with the associated CVE number (Common Vulnerabilities & Exposure, published by MITRE), the associated CVSS vector (Common Vulnerability Scoring System - open industry standard), the CVSS score (1-10, where 9+ is critical) and the release date.

You can log your measures and comments on security gaps directly in the system for future compliance queries and IT audits.

2.2.8.4. CNS Field Notice

The Field Notice module displays important problems that have been identified and published directly by Cisco. The problems published here usually require an upgrade, a workaround or another measure. The Field Notice usually refers to security vulnerabilities and the combination of the use of assets and software.

Conscia Assist - CNS Best Practices Functions

- CNS Insights
- CNS Lifecycle
- CNS Security
- CNS Field Notice

Picture 3 Conscia Assist - CNS Functions

Further details on CNS functionalities and the operation of the CNS dashboard can be found in the current CNS data sheet and the CNS User Guide.

Note: The individual functions and services of the CNS dashboard may vary from manufacturer to manufacturer. The available CNS functions are provided in detail for each manufacturer in advance

Picture 4 CNS – Manufacturer Note

2.2.9. Regular CNS Lifecycle Meetings

The CNS Lifecycle Meetings are an integral part of the Conscia Assist Service and are used for regular coordination between the Conscia Customer Success Manager and the customer on the content and recommendations of the various CNS functions.

During these meetings, recommendations for action and best practices are discussed, analyzed and documented with corresponding action items.
The interactive exchange enables customers to exploit the full potential of the CNS platform and manage their IT infrastructure effectively.

The CNS Lifecycle Meetings take place remotely and have an average length of one hour. The planned meeting content is provided in advance by the Conscia Customer Success Manager.

The contents of the meeting include at least the following topics:

- **Software version** - The software version dashboard shows the currently installed software and any necessary or recommended software updates.
- **Security Vulnerability** - Shows information about known security vulnerabilities, and necessary or recommended software updates to close or minimize potential security gaps.
- **RMA history** - Shows information about changes from a hardware replacement via the RMA process.
- Necessary **manual changes** - coordination of any necessary manual assignments and changes to device details.

The Lifecycle Management Meetings are included in the Conscia Assist Service according to the two commissioning options Essential or Advance with the following content:

Conscia Assist - Lifecycle Management Meeting

- Conscia Assist Essential: includes 2 lifecycle management meetings (semi-annually) within 12 months
  - Duration per meeting 1h
  - Remote implementation
- Conscia Assist Enhanced: includes 4 lifecycle management meetings (quarterly) within 12 months
  - Duration per meeting 1h
  - Remote implementation
- Optional: Onsite Lifecycle Management Meeting (billed at cost)

Picture 5 Conscia Assist - LCM options

2.2.10. Flexible service contingent

With Conscia Assist, an annual hourly quota can be ordered in order to quickly and flexibly process customer requests that go beyond the scope of services described.

This quota determines how many hours Conscia experts are available for certain types of inquiries. It enables requests to be processed efficiently and promptly.

The hourly quota can cover the following services:

- Proactive maintenance or replacement services
- Implementation of change requests
- Implementation of software updates or upgrades
- Installing security patches
- Advice on architecture issues or life cycle management
- On-site assignments (plus travel expenses)

Change management
The implementation of change requests depends on the complexity of the changes.

The Conscia change management process distinguishes between 3 types of change:

- Standard Changes
- Normal Changes
- Emergency Changes

Standard Change
A "standard change" is a minor, low-risk and predefined change to the IT infrastructure, for which the content, structure and risks as well as possible rollback plans and approvals are agreed in advance.
"Standard changes" are often carried out to make smaller, pre-documented changes to the infrastructure that have no impact on daily operations and do not require a service window.

Standard changes are also referred to as service requests and are predefined in the operating manual. Examples of standard changes are adjustments to properties on the LAN ports or the creation of new telephones.

Conscia fulfills standard changes as part of the Conscia Assist service contingent with an SLA of 10x5xNBD.

Normal Change
A normal change is a change to the IT infrastructure that goes through the entire change process, in which Conscia Project Management and the customer must agree on the implementation plan, the risk of implementing the change and the time of the start of the implementation as well as the planning of service windows due to possible infrastructure downtimes. A normal change can involve minor changes to the infrastructure, but also major changes with a high level of complexity.

Emergency Change
An "emergency change" is usually initiated when changes to the infrastructure need to be made as quickly as possible in order to restore stable operations or to mitigate known risks and vulnerabilities. If major incidents occur in the customer's infrastructure, emergency changes are often used to restore operations to normal.
The documentation of each implemented solution is documented in the ticket after the emergency change has been implemented and operations are back to normal.

Time frame
The quota is valid for the term of the Conscia Assist service contract from the time of commissioning and is expressed in hours.

Documentation
All customer inquiries and the hours spent on them are documented via the Conscia ticket system. The status of the hourly quota can be queried at Conscia at any time.
Unused hours expire without replacement at the end of the period.

Conscia Assist - Hourly contingent for Changes

- Hourly contingent 10x5
  - Pre-commissioned engineering hours for Changes during normal working hours 8:00 -18:00, Monday-Friday, excluding national holidays
  - SLA for standard changes: start of change implementation on the next business day (NBD)
  - Billing takes place every 15 minutes
  - Work is carried out remotely
  - Minimum contingent size: 50 hours per 12-month period
    Conscia article number: CON-ASS-DLK

Picture 6 Conscia Assist - hourly quota Changes

3. Conscia Assist Services Definition

3.1. Definitions of terms

Term	Explanation
Service level	Indication of the level of service offered by Conscia
Service time	Period in which Conscia provides the service: - 24/7: On-call service for P1 and P2 faults - 10x5: The service is provided during Conscia service hours from Monday to Friday from 08:00 - 18:00. National holidays are excluded from this
Response time	The response time is defined as the time between reporting a fault to the Conscia hotline and the callback by a qualified system engineer.
Maintenance window	Period during which the service is not available due to planned maintenance work agreed with the customer.
CNS customer portal	Web portal that provides customers with tools, dashboards, service, hardware and software-related information.
Manufacturer	Producer/supplier of the hardware or software belonging to the service
NBD	Next Business Day (NBD), 8:00-18:00, Mondays to Fridays excluding national holidays in Germany.

Table 2 Definition of terms

3.2. Fault classification and prioritization

A fault report is prioritized within a Conscia service by combining the damaging effect of a fault and the respective urgency.

As a rule, the purely technical classification of the damage effect is carried out jointly by Conscia and the customer, whereas the classification of urgency is carried out exclusively by the customer.

The fault priority is then determined from both parameters.

3.2.1. Damaging effect of a disruption

Damage effect	Explanation
Critical	• There is a defect that prevents operation, i.e. the use of the overall system is impossible or severely restricted OR • Some departments and/or locations cannot work OR • ≥ 5% of all users cannot work OR • ≥ 30% of the organization is affected by performance losses OR • The situation poses a significant financial risk or threat to life. AND • A workaround is not available
High	• There is a defect that hinders operation, i.e. the use of the system is considerably restricted OR • 2 - 5% of all users cannot work OR • 10 - 30 % of the organization is affected by performance losses AND • A workaround is not available
Medium	• The disruption has no impact on primary business applications OR • Individual, non-critical functions do not work OR • <2% of all users cannot work OR • ≤ 10 % of the organization is affected by performance losses

Table 3 Damage effect

3.2.2. Urgency of a fault

Urgency	Explanation
High	• The operation is directly at risk OR • No fallback (workaround) possible and postponement of recovery not possible OR • Immediate implementation is required
Medium	• Business operations are not impaired in the short term OR • The system is available, but with limited functions OR • A limited delay for recovery and/or workarounds is possible.
Low	• A postponement for a solution is possible OR • There is no need for immediate implementation OR • A workaround is available to temporarily resolve the issue OR • Business operations are not or will not be impaired.

Table 4 Urgency

3.2.3. Disruption priorities

Fault priorities		Damage effect		
		Critical	High	Medium
Urgency	High	P1	P2	P3
	Medium	P2	P2	P3
	Low	P3	P3	P4

Table 5 Fault priorities

3.2.4. Response times

Ticket processing in the Service Center is based on the following response times:

	Priority			
	P1	P2	P3	P4
Response time (h)	1	2	4	NBD

Table 6 Response Times

3.3. Service level conditions for End-of-X

The Conscia services depend directly on the respective support level of the manufacturer, and are therefore only available in the way they are supported by the manufacturer.

Depending on the life cycle status of the hardware and software, the availability of the Conscia services can be adjusted according to the table below.

Phase Life-Cycle	Manufacturer support	Conscia Support
No EoX notification	No restrictions (support according to SLA)	No restrictions (support according to SLA)
End of Sale (EoS)	No restrictions (support according to SLA)	No restrictions (support according to SLA)
End of SW support	Restriction of support - software bugs are no longer rectified.	Restriction in support/SLA - software errors can no longer be rectified. Workarounds may be possible.
End of Security Support	Additional restrictions on support - Security vulnerabilities or security deficiencies are no longer corrected in the software.	Further limitations in support/SLA according to the limitation of support by the provider. No SLA or guarantee from Conscia for the elimination or mitigation of security risks or security incidents.
End of New Support Contract	No takeover of existing service contracts or conclusion of new service contracts possible	Support is limited to the replacement of defective Hardware, if available and on a best-effort basis without reinsurance from the manufacturer on a best-effort basis
End of Support	No further support (hardware or software) possible from the provider.	Support is limited to the replacement of defective Hardware, if available and on a best-effort basis Basis.

Table 7 End-of-X definition

Note: The exact end-of-X definitions may vary depending on the manufacturer, but will be made transparent to the customer before the contract is concluded.

4. Setup and conditions for Conscia Assist Services

The following aspects must be taken into account when setting up Conscia Assist:

4.1. Designation of contact person

The customer names the technically responsible contact persons. All potential users of the Conscia Assist Service must be named in advance with their name, telephone number, e-mail address and function.

4.2. Setting up a customer account in the CNS portal

Creation of a customer account in the CNS customer portal for the customer's named contact persons. The account is set up by Conscia.

4.3. Installation CNS-Collector

The Cisco Common Service Platform Collector (CSPC) is an SNMP-based tool that detects and collects information about the Cisco devices installed in your network. The CSPC software provides a comprehensive collection mechanism to capture various aspects of device data.
The data is used to create inventory reports, product alerts, configuration best practices, technical services, lifecycle information and many other detailed reports and analyses for both hardware and operating system software.
It is necessary to configure SNMP on all devices so that the data can be recorded automatically.
The information collected is automatically and clearly displayed in our service and lifecycle management platform CNS.

The CNS collector is installed by the customer on systems provided by the customer.
The necessary system requirements and firewall approvals are provided by Conscia (see Appendix C)

If the installation is to be carried out by Conscia, the costs will be invoiced every 15 minutes.

4.4. Linking the ITSM systems

In principle, it is possible to link the Conscia CNS Service Portal with the customer's ITSM ticket system via a REST API interface in order to achieve effective integration into the customer's service processes.

Before linking the systems, a technical feasibility check and a consideration of the effort and associated costs must always be carried out.

4.5. Use of hardware and software

The customer must ensure that the hardware and software are used in accordance with the manufacturer's specifications, including environmental conditions, the use of own or third-party software and

Configuration files.

If this is deviated from, Conscia will not be able to fulfill its contractual obligations. Support will then be provided to the best of Conscia's ability and any resulting additional costs to rectify the fault will be charged to the customer

If Conscia determines that such deviations have been found, Conscia will
report this and give the customer the opportunity to correct it. If the correction is not made, Conscia reserves the right to discontinue the services.

4.6. Exceptions and delimitations

The following services are not part of the Conscia Assist Service, unless they are available via the flexible service contingent:

a) Proactive maintenance or replacement services
b) Implementation of change requests (change requests or service requests)
c) Implementation of software updates or upgrades
d) Provision and installation of any necessary system hardware (CPU, memory, virtual environment) to carry out software updates or software upgrades
e) Necessary maintenance and operating services for virtual environments that are not covered by Conscia
f) Installing security patches and/or signature updates
g) Monitoring the hardware and software performance of systems
h) Advice on architecture issues or life cycle management
i) Implementation of system backups and provision and operation of backup environments
j) Connection of Conscia CNS to a customer ITSM system via a REST API interface
k) Carrying out a root cause analysis (RCA) after incident processing

4.7. Contractual conditions

All terms and conditions that apply to Conscia Assist are described in this document. The terms and conditions of Conscia Care also apply to Conscia Assist where applicable.

As Conscia is continuously developing its services, this document will be updated regularly. The latest version is available on the Conscia customer portal and is deemed to be the valid version. If changes to the service affect existing agreements, the customer will be informed in advance.
With the purchase of a Conscia Assist service, this service description applies.

4.8. Additional information

For more information on our services, such as white papers, use cases and references, please visit www.conscia.de or contact your Conscia Customer Success Manager.

5. Appendix A - Conscia Assist Service Level Agreements

Conscia services	Conscia Assist Service Level		Remark
	Essential	Enhanced	
Service Desk			
Service Desk Availability by telephone	10x5	24x7*	*On-call service for P1 and P2 faults
Service Desk Accessibility by e-mail or Conscia customer portal CNS	10x5	10x5	
Incident Support			
Delivery of replacement hardware		4	Delivery of replacement hardware within 4 hours of confirmed hardware fault detection
	NBD		Delivery of replacement hardware on the Next Business Day (NBD), after confirmed hardware fault detection by no later than 14:00 on the same working day. Availability for replacement hardware is subject to stock at the manufacturer.
On-site installation of replacement hardware	O	O	For manufacturers who offer on-site services, in accordance with the manufacturer's SLA
Manufacturer support (incident management)	x	x	Response time P1: 1h, P2: 2h, P3: 4h, P4: NBD
Access to manufacturer software updates	x	x	Download on the respective manufacturer download portal
Access to the Conscia customer portal CNS-Best-Practices	x	x	
x = Included; o = Optional			

Table 8 SLA

6. Appendix B - Conscia OneNoc Description

The current OneNoc description is provided by the Conscia Customer Success Manager and presented to the customer in detail.

7. Appendix C - CSPC collector and CNS installation

7.1. CSPC Server - Requirements

The following system requirements apply for the installation of the Cisco Common Service Platform Collector (CSPC), depending on the size of the network to be covered:

	Ultra Small (up to 5,000 devices)	Small (up to 10,000 devices)	Medium (10,000 to 20,000 devices)	Large (20,000 to 40,000 devices)
vCore count	2	4	8	12
RAM	2 GB	4 GB	8 GB	16 GB
HDD (GB)	40	250	500	1000

Table 9 CNS CSPC System Requirements

7.2. CSPC firewall - necessary releases

The following firewall releases must be prepared:

Quell IP	Quellport	Ziel IP	Zielport	Protokoll
CSPC Server IP	any	72.163.7.125	443	TCP
^	any	72.163.7.113	443	TCP
^	any	72.163.7.60	80 + 443	TCP
^	any	72.163.7.60	80 + 443	TCP
^	any	173.37.146.12	80 + 443	TCP
^	any	173.37.144.208	443	TCP
173.37.144.208	any	CSPC Server IP	443	TCP

Table 10 CNS CSPC Firewall Requirements

7.3. CSPC installation - Description

The software installation and configuration manual for the CSPC collector is available on the Cisco homepage:
Software installation and configuration manual for the CSPC acquisition platform - Cisco

7.4. CSPC integration in CNS

The following information must be kept ready or prepared for the integration of the CSPC collector into the Conscia CNS platform:

zu scannende IP Range	
SNMP Community: Credential Name Read Passwort	
gewünschte IP für Collector	
DNS Server	
NTP Server	
Proxy vorhanden? (j/n) *falls ja:* *IP* *Port* *Login*	
Externe Remotezugang auf VM Umgebung vorhanden? (j/n) *falls nein: gemeinsamer Zugriff über WebEx oder TeamViewer?*	

Table 11 CNS CSPC Additional Requirements