Seeing **beyond**

Infrastructure overview.

ZEISS Connectivity Gateway and ZEISS Health Data Platform

Purpose.

The purpose of this document is to provide information on the digital platforms of ZEISS, specifically tailored for biomedical and IT professionals. This document aims to outline the system requirements, security and compliance measures, operational support structures, and system architecture necessary for the successful deployment and operation of our digital offerings.

Contents

1.0 Introduction 4

2.0 General cybersecurity and data privacy 5

3.0 ZEISS Connectivity Gateway solution 7

3.1 Requirements 8

3.1.1 System requirements 8

3.1.2 Ports and protocols 8

3.2 Data encryption 8

3.3 Operation security 8

4.0 ZEISS Health Data Platform solution 9

4.1 Product software 10

4.2 Product support 10

4.3 Backup, restore and disaster recovery support 10

5.0 ZEISS Smart Services solution 11

5.1 Installation of ZEISS Smart Services 11

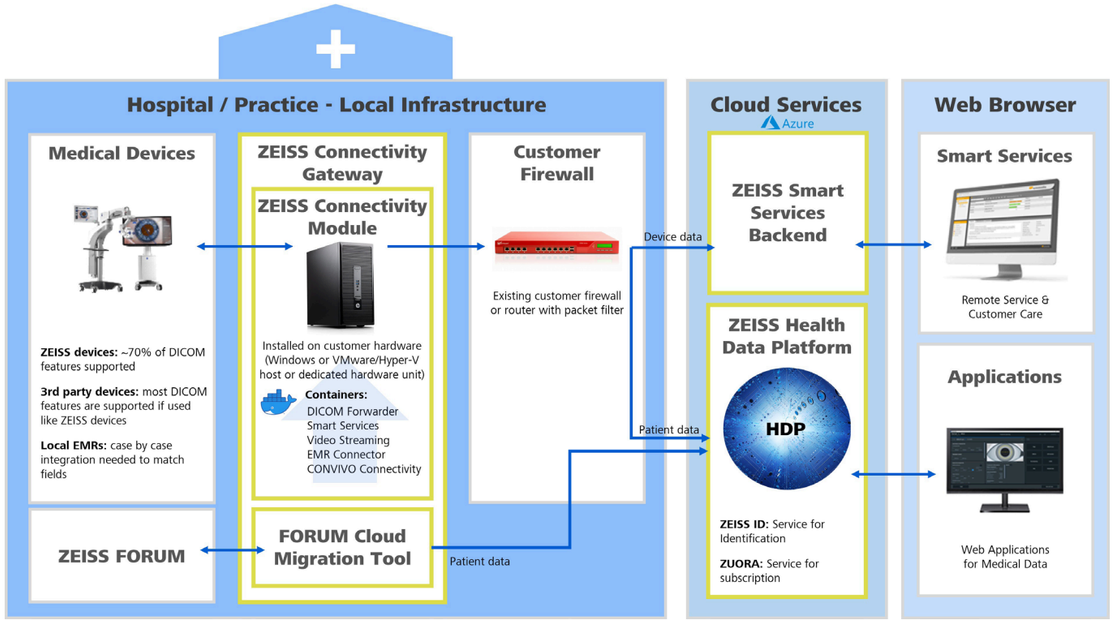
5.2 Data protection 11

5.3 Operation security 11

Appendix ZEISS Connectivity Module minimum requirements 12

1.0

Introduction



ZEISS offers several digital solutions that cater to different aspects of data management and service offerings.

Cloud-based clinical applications
This category involves applications that handle medical data, with the ZEISS Health Data Platform (ZEISS HDP) serving as the underlying platform for these applications. An example of our cloud-based clinical applications is ZEISS Collaborative Care.

Cloud-based service offerings (ZEISS Smart Services)
In this category, the primary focus is on service, maintenance, and technical device data. ZEISS Smart Services provides remote service capabilities for supported ZEISS medical devices.

For digital solutions requiring connectivity between local systems and ZEISS cloud services, the ZEISS Connectivity Module serves as the secure connectivity component within the customer network.

The diagram above shows an architectural view of the aforementioned digital platforms. The arrow direction indicates which component accesses which interfaces or services from each other.

2.0

General cybersecurity and data privacy

Through the ZEISS Cybersecurity and Data Privacy Governance Program, ZEISS manages security risks across the product lifecycle and monitors the digital landscape to protect the security of ZEISS products from emerging threats and vulnerabilities.

ZEISS products are designed and manufactured with security built in. “Secure by Design” and “Privacy by Design” principles and processes are embedded throughout the product lifecycle. ZEISS products are designed, tested and maintained based on industry standards and best practices to manage security risks across the product lifecycle. Our products are equipped with integrated security features and controls, allowing our users to securely deploy, operate, and ensure compliance with standards and regulations such as HIPAA, GDPR and ISO 27001 within their specific environments.

Within our product generation and product lifecycle processes, we address:

- Authentication and authorization
- Access controls
- Auditing and logging
- Data backup and recovery
- Data encryption (at rest and in transit)
- Malware detection/protection
- Secure configuration and hardening

With a 360° cybersecurity risk management process, ZEISS can identify, assess, mitigate and effectively manage security risks against the evolving cybersecurity threat landscape in a timely and consistent manner.

List of abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
AI	Artificial Intelligence
AU	Australia
AZ	Availability Zone
DICOM	Digital Imaging and Communications in Medicine
EMR	Electronic Medical Record
EU	European Union
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IN	India
ISO	International Organization for Standardization
IoT	Internet of Things
MAC	Media Access Control
RSA	Rivest-Shamir-Adleman
SSC	Sales and Service Center
TLS	Transport Layer Security
UK	United Kingdom
UI	User Interface
VM	Virtual Machine
ZEISS HDP	ZEISS Health Data Platform
ZEISS CMT	ZEISS FORUM Cloud Migration Tool

Secure communication with our cloud services
All communication to our cloud services and resources like ZEISS DICOMweb, ZEISS FHIR, ZEISS EMR API, ZEISS Smart Services Central, Azure IoT hub and management is TLS 1.2 or higher encrypted. All cloud services endpoints receive data sent from any containers in the ZEISS Connectivity Module and store them in the cloud services backend.

Communication with examination devices or EMR systems
The DICOM communication between diagnostic devices may be secured by TLS, dependent on the configuration. Local EMR may communicate via unencrypted HL7 and XML.

Our cloud services security certification
The operation of all cloud services, including ZEISS Smart Services is currently certified by a notified body in accordance with ISO 27001.

Regional Differentiation
Our cloud services have different data centers or endpoints located in various regions (Example of regions and locations: EU/UK in Netherlands, US/MEX in Virginia (US), IN in Pune (India) and AU in New South Wales (Australia)). Ensuring compliance with data safety requirements and regulations, therefore, restricted data can remain within the specified region without traveling outside.

Data protection
Access to an admin UI or to any data stored in the cloud services requires authentication. This ensures that only authorized users or trained ZEISS technicians have access to the relevant data, device configurations and log files. For managing infrastructure access, a role concept is in place.

Authentication
All endpoints of the cloud services, including ZEISS Smart Services require authentication. A token-based authentication is used to ensure secure communication between the ZEISS Connectivity Module and the cloud services. No information about users and credentials is shared. Each Connectivity Module has its own unique ZEISS device ID. By using the activation code within the installation process, this ZEISS Connectivity Module ID gets assigned to this installed ZEISS Connectivity Module instance. The activation code is required for the installation of the ZEISS Connectivity Module. Once installed, the ZEISS Connectivity Module requests an authentication token from the cloud services authentication service prior to sending data.

Transport Encryption
For transport encryption between the cloud services, ZEISS Connectivity Module, and ZEISS Smart Services, TLS 1.2 or higher with public key RSA 2048 bit and symmetrical AES 256-bit encryption is used. TLS certificates are managed by ZEISS.

Penetration Testing
Our cloud services, ZEISS Connectivity Module, and ZEISS Smart Services undergo regular penetration testing conducted by independent third parties to ensure the security and robustness of the system.

3.0

ZEISS Connectivity Gateway solution

The ZEISS Connectivity Gateway connects medical devices and local systems with cloud services, enabling secure and reliable data exchange.

It consists of two main components:

1. **ZEISS Connectivity Module:**
   A secure on-site gateway installed in the customer's IT environment. It connects medical devices and systems to ZEISS cloud applications and enables services such as data transfer, integration with hospital systems, and remote support.
2. **ZEISS FORUM Cloud Migration Tool:**
   A software component used in combination with ZEISS FORUM. It transfers existing data from the local FORUM system to the cloud, making it available for further use in ZEISS digital services.

   Together, these components provide a flexible and secure way to connect devices, data, and applications, helping streamline workflows and enable cloud-based services.

ZEISS Connectivity Module
By leveraging these components, the ZEISS Connectivity Gateway delivers a robust and adaptable solution for connecting medical devices and cloud-based services efficiently.

The ZEISS Connectivity Module is a secure on-premises gateway within the ZEISS Medical Ecosystem that enables data exchange between local devices, container-based connectivity functions, and our cloud services. It runs as a hardened Linux-based system with a local firewall and supports automatically deployed application containers, such as DICOM Forwarder, Smart Services, Streaming Module, and EMR Connector, depending on the subscribed use case. The ZEISS Connectivity Module provides connectivity and runtime functionality only; it does not display or process clinical data for diagnostic or treatment purposes and is not a medical device. The ZEISS Connectivity Module supports deployment in different customer infrastructure environments. Supported installation options include a dedicated Windows-based system, a dedicated virtual machine, or validated DELL hardware.

Through the EMR connector container, ZEISS Connectivity Gateway also allows the connection of our cloud services with local (on-premises) clinical management systems, planning software, and non-DICOM-compliant diagnostic devices.

ZEISS FORUM Cloud Migration Tool
The ZEISS FORUM Cloud Migration Tool (ZEISS CMT) is a software component that connects ZEISS FORUM systems with the ZEISS Health Data Platform (HDP).

Installed on a server, it enables the transfer of DICOM data and related metadata from ZEISS FORUM to HDP.

The tool supports the structured transfer of existing and newly generated data, making it available for use in cloud-based applications.

Benefits of ZEISS Connectivity Module
1. Centralized Connectivity: Enables a unified connectivity approach for communication between local systems and ZEISS Cloud Services.
2. Flexible Function Deployment: Supports different use cases through containerized modules deployed according to customer needs and subscriptions.
3. Secure Integration: Helps enable secure data exchange while avoiding direct internet exposure of connected medical devices.
4. Modular Architecture: Allows connectivity-related functionality to be added based on the required use case and system configuration
5. Simplified On-Premises Setup: Provides a single runtime environment for deployed ZEISS connectivity functions within the customer network.

The ZEISS Connectivity Module itself does not provide clinical functionality. Any clinical claims must be made only by the connected workflow solutions, applications, or medical devices.

3.1 Requirements

The main components of ZEISS Health Data Platform are delivered as cloud-based services. In deployments requiring a connectivity component, ZEISS Connectivity Module is intended to serve as the standard component within the customer's hardware or virtual environment inside the customer network.

This section describes the requirements and prerequisites for deployment of the ZEISS Connectivity Module in these scenarios, including the key technical and environmental considerations that should be addressed before installation.

3.1.1 System requirements

Your system must meet the minimum requirements listed in the Appendix for installation and operation of the ZEISS Connectivity Module.

Sufficient upload bandwidth, depending on the chosen containers, is required. The upload speed can be limited, and the limit can be adjusted after installation.

3.1.2 Ports and protocols

Depending on the containers used, different ports must be open in the local network to enable communication between the ZEISS Connectivity Module and the Medical Devices.

All connections that are required for ZEISS Connectivity Module for communication with its internet endpoints are outbound. No inbound firewall rules are necessary on the user's end.

3.2 Data encryption

Data stored locally by the ZEISS Connectivity Module as part of supported connectivity workflows is encrypted using transparent TPM-based partition encryption.

Note: TPM-based protection is enabled by default and can be deactivated on demand, depending on the deployment setup and security requirements.

Internal Data Encryption
Depending on the specific services used and the user's internal encryption measures, communication between the devices and the ZEISS Connectivity Module containers may or may not be encrypted.

Local TLS certificate-based encryption (optional)
For local DICOM communication between the examination devices and ZEISS Connectivity Module containers, users may use their own TLS certificates where supported.

3.3 Operation security

After installation and initial configuration, ZEISS Connectivity Module and its deployed containers are designed to operate with minimal ongoing user interaction, apart from configuration, monitoring, or service activities where applicable. Patches, feature- and security updates for ZEISS Connectivity Module and all containers are managed by ZEISS by an automatic provisioning and deployment process. Summaries of these changes may be provided to the customer via email upon request. The ZEISS Connectivity Module is designed to isolate its data from unauthorized access by other processes on the same hardware.

If storage from a ZEISS Connectivity Module virtual machine is copied to another system, the data remains protected by encryption.

4.0

ZEISS Health Data Platform solution

The ZEISS Health Data Platform (HDP) serves as the central cloud-based backbone for data management within the ZEISS Medical Ecosystem. It provides a secure and compliant infrastructure for the collection, management, and display of medical and non-medical data. ZEISS Connectivity Gateway (see section 2.0) is always required as the basis for ZEISS HDP, enabling the data flow from medical devices and health record systems into a cloud-based solution.

Benefits of ZEISS HDP

1. **Seamless Integration:** ZEISS HDP offers a cloud-based data management solution that integrates and manages large amounts of data from ZEISS and third-party medical devices and EMR systems using interoperability standards like DICOM and FHIR.
2. **Secure and Compliant Infrastructure:** Built on ISO 27001 certified Azure Cloud, ZEISS HDP ensures data integrity, confidentiality, and compliance with industry standards, safeguarding sensitive health information. It provides a secure data storage, complying to General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).
3. **Remote Access:** ZEISS HDP is designed to help health care professionals to access and review their patient data from anywhere, supporting them in extending patient care beyond their practice.
4. **Single Platform for data management:** As a single platform to store, access, view and manage patient data and by providing data via standardized APIs, ZEISS HDP enables data integration and digital application across multiple clinical workflows.
5. **Robust Support and Maintenance:** Comprehensive service and support structures are in place, ensuring timely updates, troubleshooting, and user training.

4.1 Product software

ZEISS HDP is a software-only product and includes the following security-related features and aspects:

Multi-Tenancy
ZEISS HDP ensures data compartmentalization through multi-tenancy. Data will be isolated within tenants, and it will not be possible to access data associated with another tenant. The authentication mechanism will restrict the authenticated principle to a tenant, and all data access will take the current principle's tenant into consideration.

Access Control and Permissions
Access to resources and operations via APIs is restricted according to a role-based security model. Users are assigned to one or more roles which determine the resources that can be accessed.

Auditing and Logging
Logging and monitoring ensure that problems can be identified and analyzed after the fact and appropriate action taken. Logging guidelines ensure that no sensitive or personally identifiable information is logged, to ensure logs do not themselves create a security violation.

Interoperability
ZEISS HDP can work with all devices and software products that support the DICOM standard and are compatible with HDP in accordance with the applicable DICOM Conformance Statement of ZEISS HDP platform.

4.2 Product support

The continued operability of the Cloud Infrastructure is maintained by ZEISS MED Operations. Product Support is assured by the existing Support Structure. For new installations, the latest software version is always installed. Existing installations are either updated remotely by ZEISS MED Operations or maintained by ZEISS local Sales and Service Centers (SSCs).

4.3 Backup, restore and disaster recovery support

Availability of ZEISS HDP is supported by hosting components in multiple availability zones (AZs) within the region. Failure of a single AZ will not result in a loss of availability. Loss of an Azure region, however, is not currently mitigated against and would result in a downtime and manual recovery. More information about Azure region recovery can be found under What are Azure regions? | Microsoft Learn.

Notwithstanding these measures, the platform is not designed to serve as a long-term data archive or primary backup system. Customers are responsible for maintaining authoritative copies of all relevant data on premises to comply with local regulatory requirements regarding data archiving, retention, and availability. The platform's disaster recovery capabilities are intended to support operational continuity of the cloud services and do not replace the obligation to maintain compliant on-premises data archives.

5.0

ZEISS Smart Services solution

ZEISS Smart Services (ZSS) is a remote service solution based on the ZEISS Connectivity Module. It connects ZEISS medical devices through a gateway container on the ZEISS Connectivity Module to a remote service application used by ZEISS technicians. For this purpose, a ZSS Agent is integrated into device software, which is suspended, if device is in medical use. The Agent is active in two scenarios: Once per day, if the device is connected, to collect a diagnostic package (logfiles), or whenever the user proactively triggers a connection, e.g. by raising a service request or approving a remote session request.

ZEISS Smart Services is not a medical product.

Benefits of ZEISS Smart Services*

1. **Instant service requests:** Enables the user of ZEISS medical devices to send service requests or problem reports directly on the device and receive assistance swiftly.
2. **Remote service by ZEISS:** Allows ZEISS technicians to analyze the device remotely, diagnose problems, and suggest solutions without having to physically access the device. Remote desktop connections enable hands-on support by ZEISS technicians.
3. **Remote software deployment:** Allows software update packages to be sent to the device remotely, enabling a quicker update process.
4. **Enablement of proactive services:** Allows collection of logfiles from the medical device on a regular basis to enable proactive service and maintenance.

5.1 Installation of ZEISS Smart Services

The ZEISS Connectivity Module must be installed and used on clients' hardware or virtualization environment within the clients' network. The ZEISS Smart Services Gateway container must be installed and run on this ZEISS Connectivity Module instance.

The same system requirements (section 3.1.1) and ports and protocols (section 3.1.2) guidelines apply as for the ZEISS Connectivity Module.

5.2 Data protection

Access to the Admin UI or any data stored in the ZEISS Smart Services dashboards require authentication from our employees. This ensures that only authorized users and trained ZEISS technicians have access to the relevant data, device configurations, and log files. Access to the platform is based on a strict roles and permissions concept (Least Privilege Principle).

5.3 Operation security

The features of ZSS are only available to users who have authenticated themselves on the medical device. From there, users can send service requests, with the attached diagnostic package containing exclusively technical data (logfiles).

Remote access to the device must be requested by an authenticated ZEISS technician and confirmed by an authenticated user on the device. Unconfirmed remote access requests are automatically denied.

Software update roll-outs can only be authenticated by ZEISS technicians. Installation on the device can only be initiated by authenticated ZEISS technicians with specific permissions or Biomed/IT admins of the customer.

*Depending on enabled functionality on device

Appendix

ZEISS Connectivity Module minimum requirements

User rights	Rights to start a command prompt as an administrator
CPU Architecture	x86_64 device with 4 virtual cores INFO: All cores must be provided by a single CPU socket
Installed RAM	8 GB
Free RAM	4 GB
Free hard disk space	75 – 250 GB
Hypervisor	Microsoft Hyper-V / VMware
Prerequisites for Microsoft Hyper-V	CPU support for VM Monitor Mode Extension (VT-x for Intel CPUs) and Second-Level Address Translation (SLAT)
Operating System	Windows 10 Pro and Enterprise edition, build 19042 and higher Windows 11 Pro and Enterprise edition, build 22000 and higher Windows Server 2022, build 20348 and higher Windows Server 2019, build 17763 and higher Windows Server 2016, build 14393 and higher

Information

- A stable internet connection is required, and a wired network connection is recommended.
- Installation on a system dedicated to ZEISS Connectivity Module without running productive processes is recommended.
- Installation on a domain controller is not supported.
- If you are using “BeyondTrust Privilege Management” software on the system on which you are installing ZEISS Connectivity Module, we recommend version 5.7.328.0 or later for this purpose. Earlier versions may cause increased CPU load.
- The system on which ZEISS Connectivity Module is installed must be connected to the user’s network and the Internet.

Carl Zeiss Meditec
5300 Central Parkway
Dublin, CA 94568
USA

EC REP **Carl Zeiss Meditec AG**
Goeschwitzer Strasse 52
07745 Jena
Germany

en-INT_38_025_0149II CZ-VII/2026 International edition: Only for sale in selected countries.
The contents of the brochure may differ from the current status of approval of the product or service offering in your country. Please contact our regional representatives for more information. Subject to changes in design and scope of delivery and due to ongoing technical development.
© Carl Zeiss Meditec, Inc., 2026. ALL rights reserved.