

## **ZEISS Predictive Service**

Technology information for our Remote Service Program

# ZEISS Predictive Service

## Technology information for our Remote Service Program

Author: Dr. Christian Schwindling, Marcus Jacob  
Carl Zeiss Microscopy GmbH, Germany

Date: January 2022

**This document describes the architecture and security features of ZEISS Predictive Service.**

**It is intended to help IT decision-makers understand how ZEISS Predictive Service operates within your environment and how it meets your technical security requirements. It is also intended to address questions about key issues such as communication through firewalls and network security.**

### Connectivity

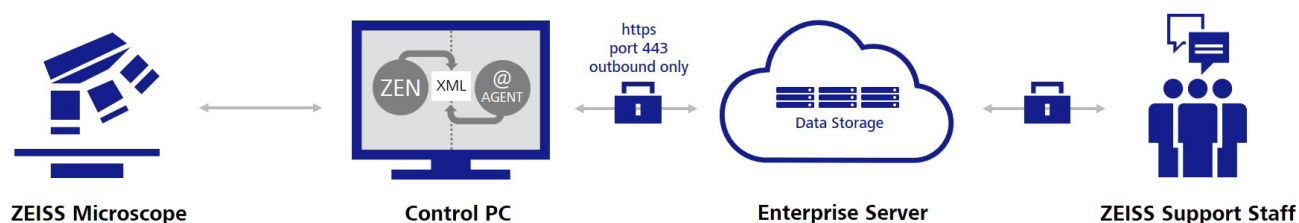


Figure 1 Connectivity

The central part of the network connectivity is the so-called Agent, a small software package installed on the microscope’s control PC. It is configured to run as a Windows service with local system privileges as “ZEISS Predictive Service Agent”.

When running, the ZEISS Predictive Service Agent will try to establish a connection to the ZEISS enterprise server at predictive-service.zeiss.com using the https protocol with TCP port 443 and 256-bit TLS (transport layer security) end-to-end encryption. This connection is always outbound only.

This means the communication channel is always initiated by the agent so that the agent can only receive messages over an established connection. It is important to know that at no time the ZEISS Predictive Service agent will act as a server and open ports for inbound connection, effectively avoiding a typical attack vector. If the local network requires a proxy server, the server address can be configured. If a user name and password is required, the password will be

stored using strong AES 256-bit encryption in the installation directory of ZEISS Predictive Service agent.

Typically there is no need to modify firewall settings, if outbound HTTPS connections towards predictive-service.zeiss.com are already permitted.

The enterprise server predictive-service.zeiss.com is hosted using Microsoft Azure Cloud infrastructure, certified and audited according to international standards (e.g. ISO 27001, HIPAA, FedRAMP, SOC1, and SOC2).

The application running on enterprise server is based on PTC ThingWorx, which includes industry-standard security features like HTTP authentication and authorization, security logging sub-systems, encrypted storage of all sensitive data (login data), support for transport layer security to ensure that all data transmitted over the wire is encrypted (TLS 1.2 with Advanced Encryption Standard (AES) 256 bit).

The communication between ZEISS enterprise server and the agent follows the secure WebSocket Standard.

There will be an initializing phase where the agent establishes a secure connection to the enterprise server over the HTTPS. Over that connection, a WebSocket upgrade is done to allow bidirectional communication between agents and ZEISS enterprise server. After the initializing phase, the agent pushes the specified data values that are important to monitor the instrument health data or to generate customer reports. Data values could be for example operating hours, component level voltages, or connection status. Also, the log files will be transferred over the same established connection. Every data transfer requires an established communication channel, which is always initiated by the agent. Consequently, the enterprise server can only request data over an established secure connection. Once the connection has been established it will be maintained until a connection loss requires establishing a new connection.

### Condition Monitoring

This section describes the use case Condition Monitoring, which is based on the connectivity model described above. Condition Monitoring is the systematic retrieval of relevant instrument health information and its server-based processing. The goal is to detect deviations in the instrument performance before they impair the user's result or even result in unplanned downtime. A typical example is the preventive replacement of a mechanical component which has reached its maximum movement cycles. Instrument health data can be, for example, operating hours, movement cycles of motorized components, component level voltages, firmware versions, and error messages. The exact scope is device-specific. All relevant data is collected by the system operating software of the ZEISS microscope and saved to separate log files (see table 1). These files can be opened with a text viewer. The log files are continuously monitored by the agent software. As new data is stored, the agent parses the log file and transmits the data items to the enterprise server over the established connection. Information about operating system and system operation software (e.g. ZEN, SmartSEM) are retrieved through the registry and Windows Management Instrumentation (WMI). This data can contain an operating system version, PC serial number, and hard drive utilization. Besides the parsing, complete log files will also be transferred to the server to help ZEISS support personnel to identify

### Connectivity Summary

- Windows service ZeissPredictiveServiceAgent.exe
- Only outbound HTTPS, 256-bit TLS/SSL secured connection on port 443
- No open ports for inbound connections
- Proxy server support
- Typically no changes to firewall settings
- Microsoft Azure cloud infrastructure certified and audited according to international standards (ISO 27001, HIPAA, FedRAMP, SOC1 and SOC2)

system failures quickly without the need of collecting the respective log files manually. Before data upload, all potentially sensitive personal data will get anonymized. Based on our testing, we expect average network traffic to be less than 2 MB per day. Log files are typically uploaded once per day. These estimates are highly dependent on system usage. When the agent is first installed, higher than normal network traffic is expected while historical data is uploaded. Below you will find a list of the log files with corresponding storage locations on the customer's system control PC. On the server, data is stored with a timestamp and checked against predefined rules. Actions, such as the notification of a ZEISS service engineer can be triggered. Trained and authorized ZEISS staff can log on to the enterprise server and review the full data set and its history for diagnostic purposes. At no time, results from the microscope user for some processed images are transmitted in this data stream.

### Condition Monitoring Summary

- Only log file data from specific log file storage locations are transmitted (see table 1).  
These files are fully transparent and plain-text readable
- No user-specific information or files are included in continuous monitoring

Device type	Log file name	Description	Path
Electron microscopes	EM Server.log	Information about EM Server	C:\ProgramData\Carl Zeiss\SmartSEM\Log\EM Server.log
Electron microscopes	Log Folder	Includes SmartSEM Logs (GIS, FIB,...)	C:\ProgramData\Carl Zeiss\SmartSEM\Log
Electron microscopes	Snapshot Folder	Includes Capella System Snapshots	C:\ProgramData\Carl Zeiss\Capella\SystemBackups
Electron microscope	Log Folder	Data monitoring of EM Service Center Software	C:\ProgramData\Carl Zeiss Microscopy GmbH\EmServiceCenter\DataMonitoring\External  D:\EmServiceCenter\DataMonitoring\External
Light microscopes	remote service.log.xml	Already parsed information from ZEN.log.xml and ZENCore.log.xml	C:\ProgramData\Carl Zeiss\Remote Service\remote service.log.xml
Light microscopes	ZEN.log.xml	Information about ZEN software	C:\ProgramData\Carl Zeiss\Logging
Light microscopes	ZENCore.log.xml	Information about ZEN core software	C:\ProgramData\Carl Zeiss\Logging
X-ray microscopes	XradiaAppn.log where n=1,2,...N used in system software v11.1  XradiaApp_n.log where n=1,2,...N used in system software v12	Information about Versa system parameters	C:\Program Files\Carl Zeiss X-ray Microscopy\Xradia Versa\XX.X.XXXX.XXXXX\Log Files
X-ray microscopes	Centre.log Comms.log FilStore.log Getter.log Healthcheck.log Serial.log TCC.log Tube.log Vac.log Warm.log	X-ray source logs	C:\Program Files\Carl Zeiss X-ray Microscopy\Xradia Versa\XX.X.XXXX.XXXXX\logs

**Table 1:** Overview of log files

### Optional image upload

You have the possibility to select the optional Image Upload function regarding automated Sample Finder. This option can be selected or unselected during the activation process or afterwards within the Predictive Service settings menu on your system. At these points the referring General Conditions of this feature can be viewed at any given time.

This automated Sample Finder Image Upload mainly helps ZEISS to improve Machine Learning models to further enhance Sample Finder functionalities and efficiency.

### Installation

After approval of Predictive Service by you and your IT department, there are two options to get your ZEISS microscope connected. The precondition for both options is that your system is connected to the internet with all necessary security measures (e.g. antivirus software). Please see also our recommendations for data security.

#### 1. Preinstallation in factory

For selected system types (LSM, Axioscan, etc) the Predictive Service agent software is already preinstalled in our factory.

When you will start your system operation PC for the first time, a pop-up screen of Predictive Service software will appear and will guide you through the activation process (e.g. terms and conditions acceptance, internet settings).

#### 2. Installation via TeamViewer remote desktop sharing

- All necessary information and documents are sent to ZEISS and a remote installation session is scheduled. Please clarify also if there are specific proxy settings needed and if so, please have these settings available for installation
- You will receive an e-mail from ZEISS service with a link to download the TeamViewer Quick Support software. Please note that this software will not be installed permanently on your PC
- Start the TeamViewer Quick Support software and accept the TeamViewer session request and remote control request
- ZEISS tech support will install ZEISS Predictive Service Agent
- Test, if the connection between the Agent software and the Enterprise server is established

For more security details please check on TeamViewer: <https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf>

#### 3. Installation by field service engineer

- All necessary information and documents are sent to ZEISS and an on-site visit is scheduled. Please clarify also if there are specific proxy settings needed and if so, please have these settings available for installation
- ZEISS field service engineer will install ZEISS Predictive Service Agent
- Test if the connection between the Agent software and the Enterprise server is established

### Security relevant Updates

ZEISS may update the Predictive Service Software from time to time to provide the latest functionality and security updates. These updates will be installed automatically unless you explicitly reject the consence of the General Conditions of Predictive Service.

If the consent is rejected Predictive Service will be deactivated at all.

**Technical facts**

Ports	443
Protocols	HTTPS, Secure Websocket
URL of ZEISS server	predictive-service.zeiss.com www.predictive-service.zeiss.com
IP addresses	52.174.243.245
Certification of Microsoft Azure cloud infrastructure	ISO 27001, HIPAA, FedRAMP, SOC1 and SOC2
Connection security	TLS 1.2 with AES 256bit
Supported proxy settings for installation	- No authentication - Basic authentication - Digest authentication - NTLM authentication
Available and patched local area network connected to ZEISS system PC	RJ 45 connector for LAN
Security patched and measures according to your local IT security standards	e.g. installing antivirus software; please see recommendations for data security policy on ZEISS Microscopy Systems (see references)
Established and working outbound internet connection	

**Overview of Data Security**

This section will give you an overview of data security standards and measures in the context of ZEISS Predictive Service IoT product.

**PTC ThingWorx IoT platform**

- Server security (due to IT security reasons, individual measures will not be listed here)
- Secure design principles
- Authentication and authorization
- Matrix multi-tenancy
- Security logging sub-system
- Encrypted storage of all sensitive data
- Recommended and supported backup strategy
- Protection against common vulnerabilities
- Support for transport layer security
- Additional security features
- File transfer and application tunneling with ThingWorx EMS
- Secure and scalable on-demand centers
- Connectivity security
- Manufacturer’s requirements for connected product security
- End-customer requirements for connected products

**Testing and validation of data security measures**

- Continuous (daily) testing due to automated tests of custom implemented features
- Evaluation of permissions to access different backend services of custom implemented features
- Penetration Tests (“Pen Tests”) are executed once every year by trusted and verified external partners. Any findings will be fixed.
- Continuous updates on Internet-facing systems and core dependencies
- Secure development environment
  - Access to the office
  - Access to the systems
  - Separation of productive- and test-platform
  - Backup
- Version control
- Change control
- Acceptance test
- Secure programming techniques

### Microsoft Azure cloud storage

- Access and permission management
  - Security groups
  - Permission levels
  - Permission states
- DDoS protection
- Secure by design
- Credential security
- Live site response
- Service security
- General Data Protection Regulation (GDPR)
- Data residency and sovereignty

### Testing and validation of data security measures

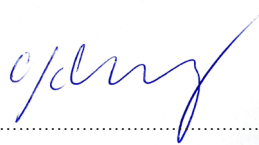
- Different kinds of testing
- No changes of third-party software (Exception: security holes)
- Training measures of employees
- Control of outsourced development

### References

Recommendations for data security policy on ZEISS Microscopy Systems  
AGBs General terms and conditions Predictive Service



.....  
**Martin Fischer**  
Head of Global Service & Customer Care  
ZEISS Research Microscopy Solutions



.....  
**Dr. Christian Schwindling**  
Head of Remote Service & IT Support  
ZEISS Research Microscopy Solutions