Xtract Universal.iQ. Data Security, Privacy, and Compliance Overview

About this Document

This document provides a high-level overview of the data processing, information security, and privacy-related aspects of Xtract Universal.iQ. It is intended to support customer security, compliance, and data protection assessments but does not replace product-specific configuration guidance or the customer's assessment of its own deployment. Theobald Software maintains an Information Security Management System (ISMS) and protects information assets through appropriate organizational and technical measures. Additional information is available in our Information Security Policy.

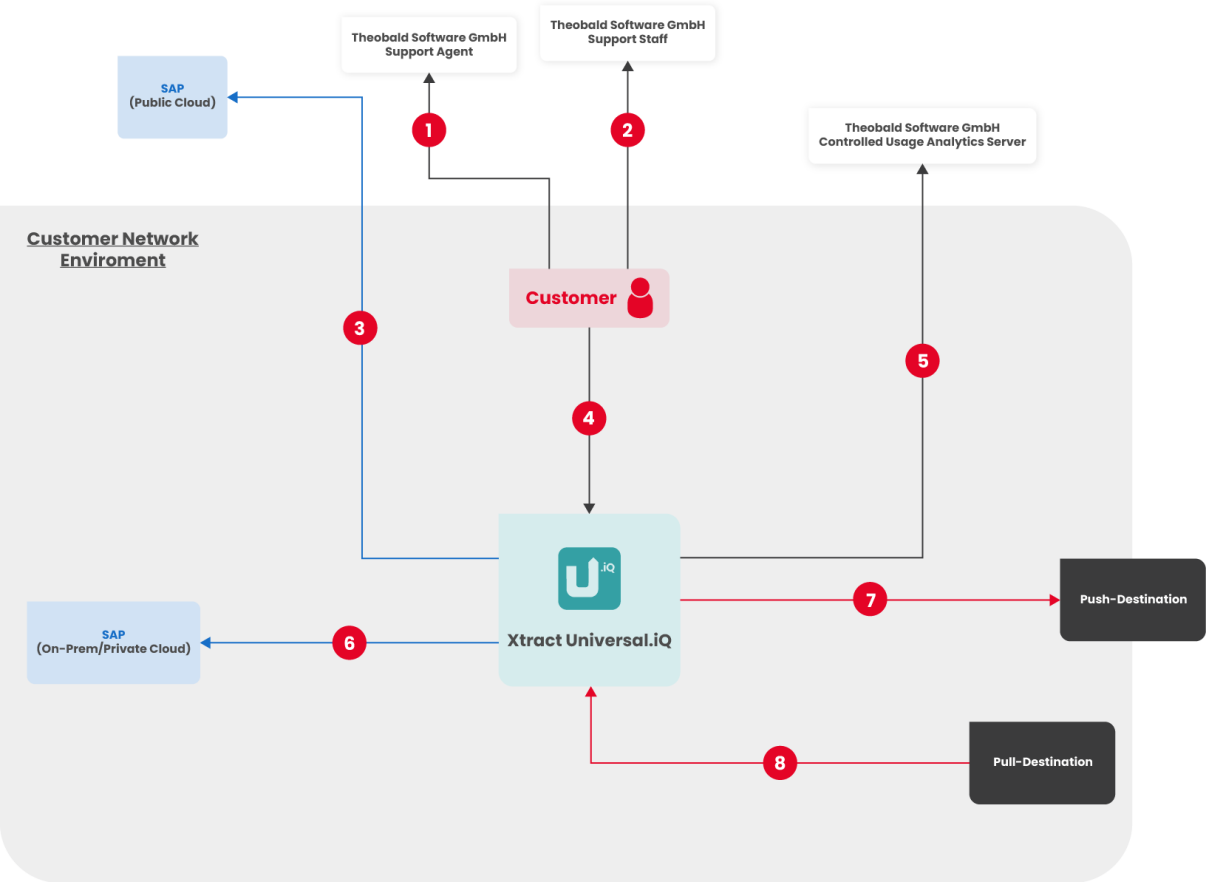
Theobald Software processes personal data in accordance with applicable GDPR requirements and retains it only for the relevant processing purpose or statutory retention period. Data that is no longer required is securely erased under the applicable deletion concept unless a legal obligation prevents deletion. Further information about data subject rights is available in our Privacy Policy.

Product Overview

Xtract Universal.iQ is a software product developed by Theobald Software for extracting and transferring data from SAP systems to third-party systems or back to the SAP source system. The product is installed and operated within the customer environment.

Xtract Universal.iQ runs within the customer network and connects to configured SAP systems using the applicable SAP user context. The figure summarizes the main data flows and indicates where encrypted communication is used or can be configured.

Xtract Universal.iQ: Data Flows and Connections



Position number	Description
1	Customer–support agent chat: encrypted connection. Entered data is not public and is processed within Theobald Software's enterprise environment. Avoid entering sensitive information unless necessary.
2	Diagnostic information and support ticket data, such as logs, traces etc. provided by the customer to Theobald Software. ⚠ Trace exports contain unencrypted SAP data.
3	Public Cloud connection: WebSocket or OData encrypted with TLS
4	Customer–instance access: Configuration, diagnostics (logs, traces), or usage analytics data.
5	Usage analytics: anonymized technical data – sap object names, extraction names, run information, connection names, feature usage; no user information, no sensitive data
6	On-Prem/Private Cloud connection: • WebSocket, OData encrypted with TLS or • RFC encrypted with SNC, if configured
7	Outgoing target-system (destination) connection: Encryption depends on target configuration; typically TLS.
8	Incoming consumer-system (destination) connection: TLS-encrypted, if configured.

Data leaves the customer environment only through defined communication paths. This includes diagnostic information that customers explicitly provide to Theobald Software for support purposes. The types of diagnostic data, their transmission, and their protection are described under Support and Troubleshooting Data.

Xtract Universal.iQ may also transmit limited product usage data to an analytics server controlled by Theobald Software. The scope, purpose, and activation of this feature are described under Usage Analytics.

Data Handling and Access

Xtract Universal.iQ processes data within the customer-controlled environment. During data processing, data is read from the SAP source system, transformed into the configured output format, and transferred to the designated target system. Xtract Universal.iQ does not operate a vendor-managed cloud service for customer business data. Storage locations and retention settings depend on the customer's deployment and configuration.

Data Processing and Protection

Business data is generally processed according to the configured scenario. Storage locations, retention periods, backup strategies and infrastructure components remain under customer control. Xtract Universal.iQ offers the configuration of state of the art encryption and security mechanisms (TLS / SNC) for all incoming and outgoing communication.

Customers are responsible for backing up their data and protecting it against unauthorized access.

Identity and Access Management

Xtract Universal.iQ offers direct integration in Microsoft Entra ID environments by using its respective authentication and authorization concepts. Alternatively, the construction of a custom Xtract Universal.iQ-specific user and group-based access management environment is supported.

Authentication and authorization against source and target systems use each system’s own access control mechanisms and a user context defined by the Xtract Universal.iQ user.

Audit Logging and Traceability

Xtract Universal.iQ logs selected user activities together with the associated user context. When authentication is enabled, these records can help customers reconstruct activities such as the execution or deletion of a service for internal reviews, security investigations, or audits. The availability and attribution of logged activities depend on the configured authentication and logging settings.

Data Shared with Theobald Software

Support and Troubleshooting Data

Theobald Software Support does not have direct access to customer systems. For troubleshooting purposes, customers may provide relevant technical information to Theobald Software.

When troubleshooting a support case, customers may be asked to provide log files, configuration data, trace data and, in rare cases, memory dumps. Neither logs nor configuration data contain sensitive data, and the connections to the support portal are encrypted.

Trace files and memory dumps may contain business data and SAP secrets and are therefore handled with particular care in accordance with applicable legal requirements.

Customer information received for support or troubleshooting purposes is protected in accordance with applicable data protection and information security requirements and securely erased under the applicable deletion concept when it is no longer required and no legal obligation prevents its deletion.

Usage Analytics

Xtract Universal.iQ includes a default Usage Analytics feature. The transmitted data consists of anonymized statistics about extraction activity and product usage, including the number of extractions, extracted row volumes, success and error rates, throughput, extraction duration, and the distribution of extractions across SAP source systems and configured target systems. SAP business data and user activities are never transferred.

Theobald Software uses this data solely to analyze product usage patterns, improve product performance, and support product development.

Organizational Security (ISO 27001 / ISMS)

Theobald Software maintains an Information Security Management System certified according to ISO/IEC 27001. The ISMS provides the organizational framework for managing information security risks and maintaining applicable security measures. Secure software development activities include code reviews, vulnerability management, and security testing.

Contact

For information security questions, contact security@theobald-software.com. For privacy and data protection questions, contact data.protection@theobald-software.com.