Security Overview

Kryon Process Discovery

V. 21.3

Document revision: 01-Apr-2021

Contents

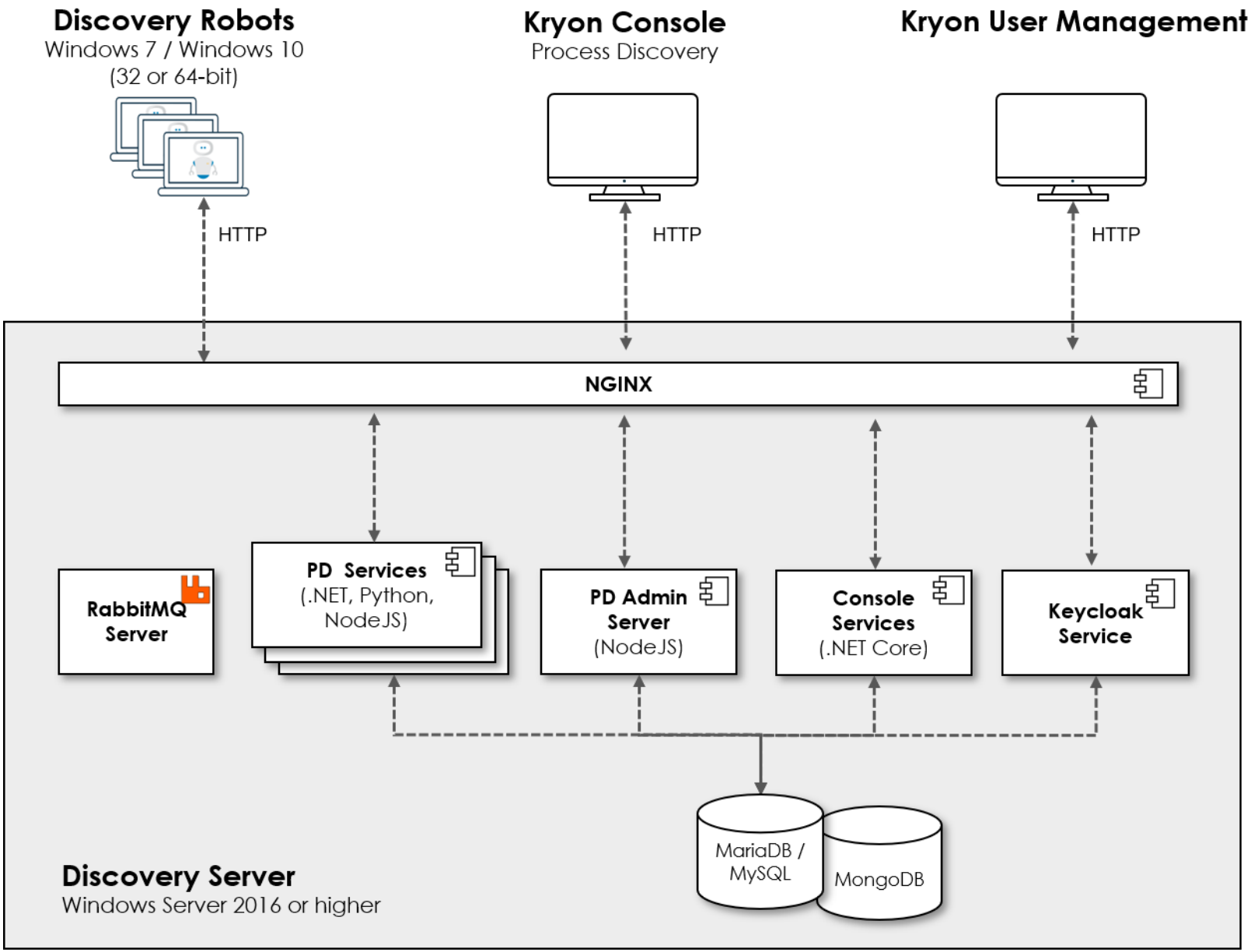
Introduction

Kryon Kryon Process Discovery is a powerful, proprietary, AI-based platform designed to identify your organization's business processes, correlate variants, and make recommendations for enhanced efficiency via automation.

The platform uses silent Discovery Robots installed on the company's computers to capture all actions that affect business outcomes. It then analyzes this data to make process improvement and automation recommendations.

The purpose of this document is to provide a high-level overview of the Kryon Kryon Process Discovery platform's security aspects . Unless stated otherwise, information in this document is relevant to common Kryon Process Discovery use cases.

System Architecture Diagram



Installed Components & Software

Discovery server

The following software is automatically installed on the **Discovery Server** by the Kryon Process Discovery server installation package, if not previously installed:

- Microsoft .NET Framework 4.7.2
- Microsoft .NET Core 2.2 – Windows Server Hosting
- Microsoft Visual C++ 2015-2019 Redistributable (x64)
- RabbitMQ Server (the queue manager for communications between the **Discovery Robots** and the **Discovery Server**)
- Erlang OTP (the programming language on which RabbitMQ is built)
- NodeJS (JavaScript runtime used by Kryon Process Discovery Admin)
- Seq (centralized logging component)

The following software can be optionally installed by the Kryon Process Discovery server installation package:

- HeidiSQL (database viewer)
- Notepad++

Discovery robot

The following software is automatically installed on the client machine during the **Discovery Robot** installation, if not previously installed:

- Microsoft .NET Framework 4.7.2
- Microsoft Visual C++ 2015-2019 Redistributable (x64/x86 as appropriate)

Third party components

Third party software provided as part of or with the Licensed Product is solely governed by its respective license terms as set forth in:

https://public.kryon.io/#PD-Versions/21.3/Documents/

Database/Servers Integration

Seq (logging server)

MariaDB/MySQL (database)

RabbitMQ (communication broker)

Network

Kryon Process Discovery is installed on-premises, without communication to servers outside the customer organization's Network, SaaS services, or any other third-party server, internal or external.

Security

We recommend using secure network protocols among all system components. The Kryon platform is regularly updated with the latest security fixes to ensure data safety and that privacy is not compromised.

The transport protocol uses Certificates encryption. The supported network protocols include HTTPS & TLS1.2. the PD Console application currently does not support HTTPS.

- The certificate must be provided by customer
- Unsecured network protocols are also supported (HTTP/AMQP/MySQL protocol)

> **NOTE**
>
> User action images are **encrypted** in-transit and in-rest, regardless of the network protocol used.

Firewall & port configuration

Kryon port configuration and network protocols can be configured to support all common firewall requirements.

Kryon's default port configuration is as follows (all can be customized in accordance with the organization's security requirements):

- Between the **Discovery Robots** and the **Discovery Server**:
  - Unsecured communication: 5672
  - Secured communication: 5671
- Between the **Process Library** and the **Discovery Server**:
  - Unsecured communication: 80
  - Secured communication: 443
- [Optional] Between the **Discovery Server** & **Process Library** to a **Remote DB**: 3306

External ports are opened automatically in the Windows Firewall during the Discovery Server installation.

Data Privacy & Segregation

Administrators can manage roles and permissions for organizational security. Kryon's multi-Team architecture allows administrators to configure separate working environments for different business units for separating business domains and for scaling.

Multi-tenancy

Enterprises can create fully separated and secure environments. Resources including Discovery Robots, database storage, Kryon Process Discovery analysis and more can be allocated to each team.

Administrators can provision multiple companies within an organization, and for each provisioned company, separate the data and Kryon Process Discovery results.

HIPAA and GDPR Compliance

In addition to the encryption & authorization mechanisms mentioned above,

username in all data recorded/transmitted by the **Discovery Robots** can be hashed. The customer can enable/disable this option on a per-robot basis according to its needs.

Furthermore, raw data is not saved over time, and no sensitive information is persisted over time.

Encryption

Encryption is enforced by default for all sensitive data both in-transit and in-rest.

All data stored on the server side is encrypted using the Advanced Encryption Standard (AES) 256-bit key and kept in the Kryon database. Encryption is done on the client side only, so data is transmitted encrypted.

No data is stored on the client side: once a Discovery Robot is finished recording and the session ends, all sensitive data is cleared (unless "Standalone mode" is enabled)

- The encryption mechanism and key length for all encryption processes used within this product, including data in transit, data at rest (stored within the application), and any special storage (such as passwords), are as follows:
  - AES-256
  - SHA-256
- When the product communicates with itself, a client system, or another third-party system, the encryption options available to facilitate the communication in a secure manner are as follows:
  - HTTPS
  - TLS1.2
- Passwords are stored in a non-reversible format, SHA-256 or better
- RSA is used to encrypt/decrypt messages over the network using asymmetric keys.
- See Credentials Vault for details regarding the encryption methodology used by the Kryon Credentials Vault.

FIPS compliance

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB140-2), is a U.S. government computer security standard used to approve cryptographic modules.

All encryption methods used by Kryon, both client and server-side, are FIPS compliant.

Auditing & Logs

Kryon audits all mission-critical events and changes with complete traceability into robot and/or server history and activities. These logs can be a useful resource for troubleshooting.

Discovery Robots logs events to the local hard driver using files.

Log file access is restricted by Windows file system permissions according to organization policy, to restrict unauthorized modification, access to, or deletion of the log file.

To locate the logs

The **Discovery Server** & **Process Library** send log messages to Seq – a centralized logging server. Seq is a third-party component installed a part of the Kryon Process Discovery server installation.

- Browse `%LocalAppData%/Kryon/ActionsRecorder/logs` folder

To access the logs

If you wish to access Seq from a remote machine, please make sure port 5341 is open.

Event types which are logged include: connection establishment/failures, data processing invocation, processing result track and more.

Log messages do not contain any sensitive data.

- Open your browser and navigate to `http://%YourServerFQDN%/seq`

Data Retention

Kryon Kryon Process Discovery is a client/server solution.

Server Data

All data is saved in the **Discovery Server**'s internal repository and is not transmitted or exported outside the server, automatically or manually.

Raw data is not saved over time, and no sensitive information is persisted over time.

Client Data

Data recorded by the **Discovery Robot** is stored in a local cache (SQLite) which empties when a connection with the server is established.

On standalone mode, the **Discovery Robot** stores raw data to SQLite local file. An administrator should collect this file at the end of the recording and delete it from the user's machine.

Credentials Vault

The Credentials Vault is a module within the Kryon Process Discovery platform used to manage login credentials for systems that Kryon Process Discovery's components needs to access. Passwords are stored securely using data encryption.

The Credentials Vault enables administrators to utilize the required credentials for any operation without hard coding specific passwords into configuration files and without exposing credentials to unauthorized parties.

Architecture

Credentials Vault data is saved in an encrypted format to a local file:

- **server.keys** – stores usernames and encrypted passwords for all relevant components (e.g. database credentials, message broker credentials and more)
- **pddr.keys** - stores username and its encrypted password to use for the server connection