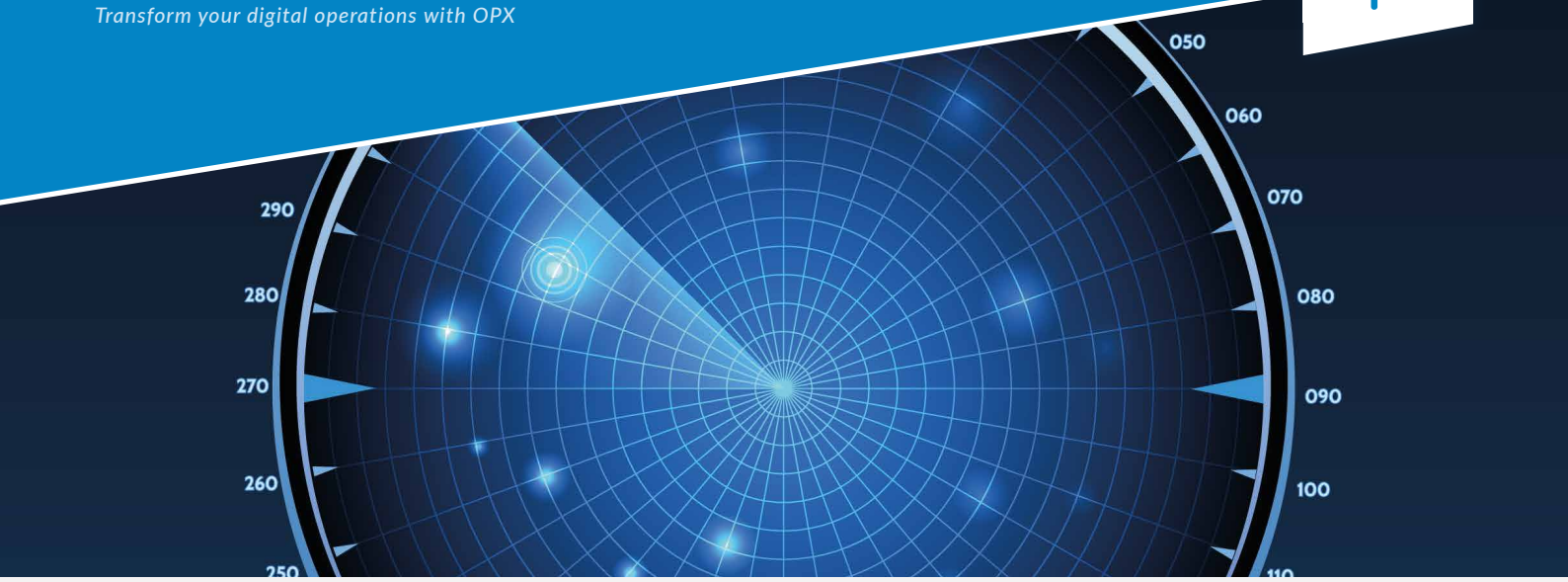
OPX Application Discovery

Transform your digital operations with OPX



Overview

OPX Application Discovery(OAD) is an OPX module that tracks a user's application use during their Windows session and reports this information back to the OPX database.

As this can sometimes be considered as sensitive operational data, this document covers the security and privacy aspects of the features to ensure that there is no room for unintended data leakage or disclosure beyond the company's defined data disclosure use.

OAD is not cloud-based and as such runs within the confines of the customer's own network. However, we have taken the view the customer may be hosting OPX in the cloud and added appropriate security measures as defined below to ensure the system is secure. These include:

- data at rest on the client is encrypted
- data in motion is encrypted using TLS
- data in Motion requires authentication
- configuration files on the client are encrypted (to avoid tampering)
- data in the OPX database on the server is only accessible via RBAC as defined by the client
- data which contains Personal Identifiable Information (PII) fields is deleted periodically with the default being 28 days

The rest of this document covers the various parts of OAD, and the measures put in place to handle the sensitive data.

OAD Client Data

The OAD client is a standalone process which runs on the PC or VDI as a Windows process. This process listens for:

- Windows events
- browser events send via browser plugin
- OPX WFU events sent from the current OPX WFU application

OAD is a single process, comprising of several library's.

OAD Server Data

Data Access

OAD server data is received over TLS and saved into the OPX database hosted by the client. The data in this database is accessed via web services provided by OPX.

- all web services are authenticated.
- all web services are over TLS 1.2 or above.
- all web services have Role-based Access Controls on the data.

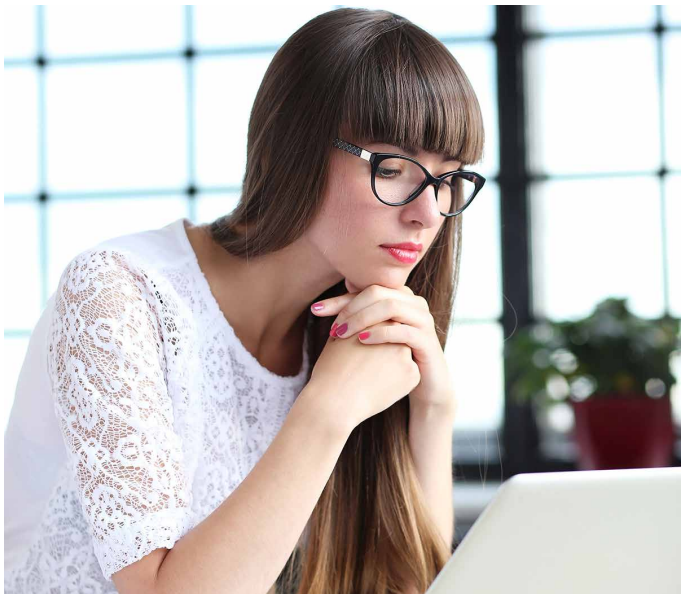
As with other operational data, it is expected that an administrator's direct manager will have access to their operational activity data, as well as designated super users within your organisation.

Data Retention

An SQL Server job executes every night and removes any data elements that refer to a user after the prescribed period (the default is 28 days). Data that could be used to possibly identify a user includes:

- user ID
- user name
- machine IP address
- machine name

For analytic purposes, the non-identifiable data may be held for a longer period and only be identifiable as a team member of a known team. In the event any data is being used for disciplinary action it can be exported beforehand to be delivered to HR.



References

The following show the standards and components being used, CMS reserves the right to change these from time to time with equally secure mechanisms to ensure continues support and onward development.

- Embedded web server TLS support
- ZeroMQ security layers using Curve25519
- Recovery logs in SQLite encryption
- MQTT security

The interfaces/ports used by the OAD process are as follows:

No	Interface	Use	Secured by
1	Windows Management Instrumentation	Gather current window and mouse or keyboard movement (not tracking)	Standard Windows OS rights, not usually exposed outside Windows instance
2	Browser domain and URL and current tab	Gather SaaS apps being used	TLS between browser plugin and embedded local browser
3	WFU event log	Gather events for Get-Next and completed states from existing OPX	Secure ZeroMQ as socket only on localhost and key-pairing for clients
4	Key request for local AES key	Get a key to encrypt local log and config file from server	Authenticated restful service returning AES 256 key
5	Event log push to server	Used to send activity logs	Encrypted using TLS
6	Configuration push	Used to enable screen shot, or desktop viewing remotely	Secure Pub/Sub mechanism using MQTT security and for screen broadcasting a one-time key required by the viewer to get access to the stream
7	Local log for recovery in the event of failure or power off or killed process	Used as temp log space	Encrypted on disk using the key