# Usage Log and Data Encryption Summary

Ext.prc.001.04 | 01.22.2024

UPM 24.x

ZINFI Confidential & Proprietary
Shared Under NDA

# Contents

# Usage Log Management

Protecting data, preserving privacy, and complying with regulations such as the General Data Protection Regulation are certainly some of the highest priorities that ZINFI provides for client business. It's critical that we audit the entirety of data processing actions taking place to be able to analyze for possible security breaches. This information from Activity Logging are maintained at the database level and are not made available at the UPM UI to be tampered and archived – for clients to audit at will, by an exclusive request to ZINFI.

This section covers how we store such audit logs of data processing activities, archive the same and how clients can access the logs to review their activity data.

## Activity Log

All administrative activities logging takes place at the backend database layer which means a single action can trigger multiple events that are logged. The following are a sample of admin events and activities which are logged:

- Group, User Management - Who was added, who was deleted, what access rights were updated.
- Configuring Modules – What Programs, Levels and Tasks got configured.
- Create, read, update, delete (CRUD) - Logging all CRUD activities.

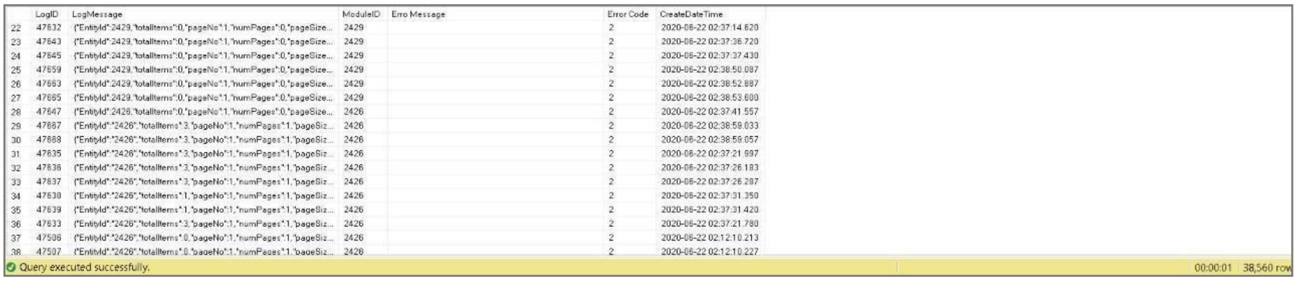
## Log storage

Logs are stored on a dedicated database at the back end and no access to the database is made public. On weekly basis the log is auto archived to a central dedicated secured database repository. All such administrator activity logs are stored securely (with no access to anyone except formally requested) at the central repository for a period; post 6 months of the expiration of the contract - except if there is a legal or business requirement which defines a specific time period.

## Log access

Logs archived cannot be accessed by any internal or external user till a formal request to access such logs is made by creating a formal ticket with ZINFI. On review and acceptance of such a formal request by the client, the admin activity log is exclusively downloaded into an encrypted format, secured with a password and shared with the client, through secure protocols.

## Example Activity Log



| | LogID | LogMessage | ModuleID | Erro Message | Error Code | CreateDateTime |
|---|---|---|---|---|---|---|
| 22 | 47632 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:37:14.620 |
| 23 | 47643 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:37:36.720 |
| 24 | 47645 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:37:37.430 |
| 25 | 47659 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:38:50.087 |
| 26 | 47663 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:38:52.887 |
| 27 | 47665 | {"EntityId":2429,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2429 | | 2 | 2020-06-22 02:38:53.600 |
| 28 | 47647 | {"EntityId":2426,"totalItems":0,"pageNo":1,"numPages":0,"pageSize... | 2426 | | 2 | 2020-06-22 02:37:41.557 |
| 29 | 47667 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:38:59.033 |
| 30 | 47668 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:38:59.057 |
| 31 | 47635 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:21.997 |
| 32 | 47636 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:26.183 |
| 33 | 47637 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:26.287 |
| 34 | 47638 | {"EntityId":"2426","totalItems":1,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:31.350 |
| 35 | 47639 | {"EntityId":"2426","totalItems":1,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:31.420 |
| 36 | 47633 | {"EntityId":"2426","totalItems":3,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:37:21.780 |
| 37 | 47506 | {"EntityId":"2426","totalItems":0,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:12:10.213 |
| 38 | 47507 | {"EntityId":"2426","totalItems":0,"pageNo":1,"numPages":1,"pageSiz... | 2426 | | 2 | 2020-06-22 02:12:10.227 |

Query executed successfully. 00:00:01 38,560 row

The Activity Log is generally composed of the following elements:

- **LogID** – The Login ID of the admin user
- **LogMessage** – The activity summary which is logged
- **ModuleID** – The UPM Module on which the activity was performed
- **Error Message** – If operational error got logged, the error type is saved as the error message for audit purposes.
- **Error Code/Response Code** – Status Code of the operation execution, in the example Code 2 – represents execution success of the operation
- **CreateDateTime** – Logs the operation date and time of execution and log storage

# Data Encryption Techniques

256 bit AES Encryption and 2048 bit RSA NIST recommended Cryptographic Key management techniques are used to secure customer sensitive data at rest. Data encryption keys are updated on a regular basis and stored separately from the data. All customer data which is classified as nonpublic and transmitted across external and internal environments are encrypted in transit and TLS 1.2 Encryption Algorithms are used to secure data in transit. Legacy services like FTP and Telnet are not utilized by ZINFI.

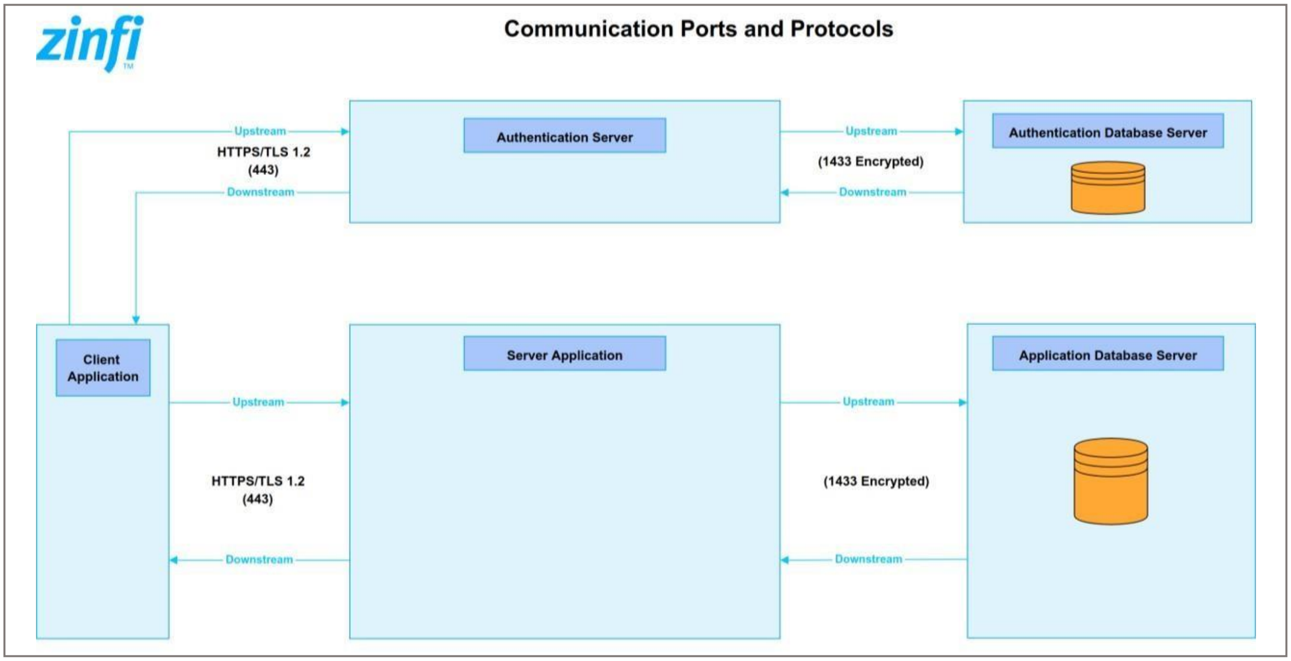
Backups, if performed are stored with the same level of protection of the data itself, viz. Data at Rest. 256 bit AES Encryption and 2048 bit RSA NIST recommended Cryptographic Key management techniques are used to secure customer sensitive data at rest. Data encryption keys are updated on a regular basis and stored separately from the data.

## Encryption of Data in Transit

ZINFI offers TLS/SSL encryption for keeping data private as it moves from one location to another. We utilize the Transport Layer Security (TLS 1.2) protocol to protect data when it’s traveling between the cloud services and customers. Our datacenters at Azure, negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

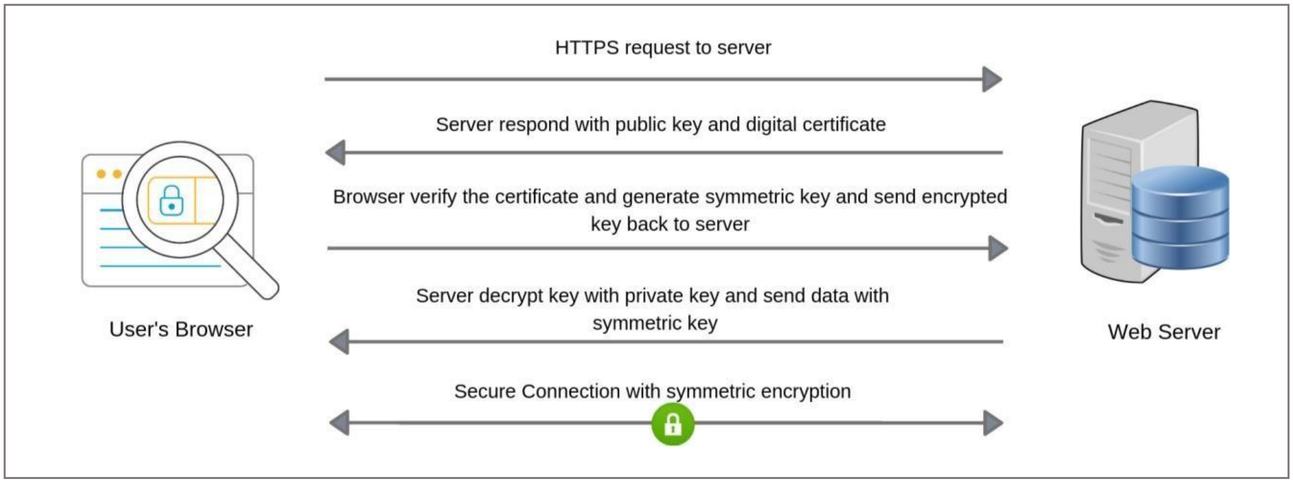
## Data encryption across Internal Environment

Encryption techniques are utilized by the server application or calling application. When leveraging this encryption model, usage of standard encrypted protocols for data transmission across the Server Application and the Database Server are ensured. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use. For data moving between on-premises infrastructure we consider appropriate safeguards such as HTTPS, and all transactions occur via HTTPS.



## Data Encryption across External Environment

When data traverses to external environments, all transactions take place over HTTPS. We enforce the use of HTTPS when REST APIs are called to access UPM objects. We provide client-side SSL certificate to the external system for server-side validation through encryption handshake, resulting to dynamic encryption during data transmission. The primary reason for using Secure Sockets Layer (SSL) certificates is to keep sensitive information sent across the internet encrypted so that only the intended recipient can understand it.


HTTPS request to server
Server respond with public key and digital certificate
Browser verify the certificate and generate symmetric key and send encrypted key back to server
Server decrypt key with private key and send data with symmetric key
Secure Connection with symmetric encryption
User's Browser
Web Server