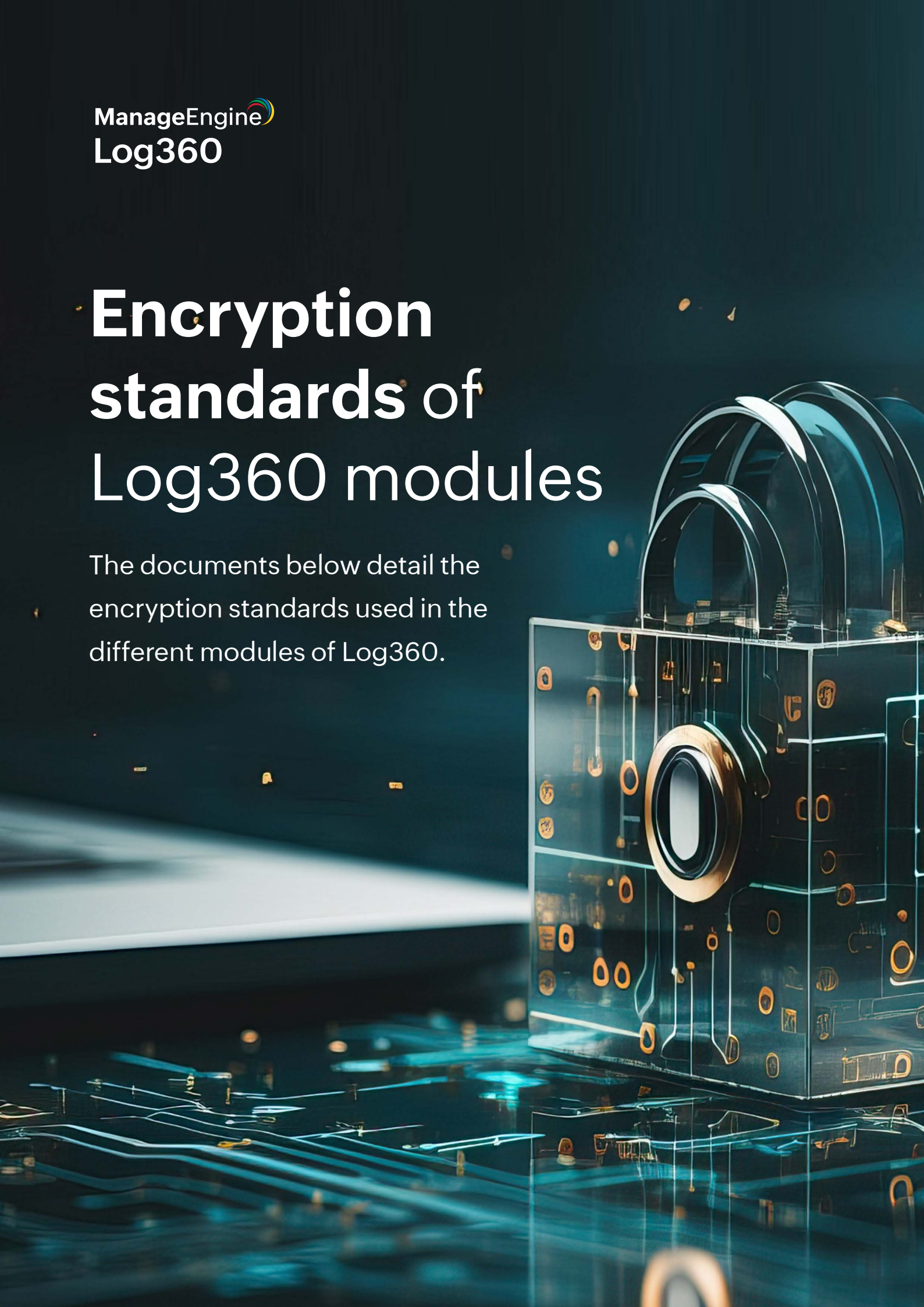
ManageEngine
Log360

Encryption standards of Log360 modules

The documents below detail the encryption standards used in the different modules of Log360.



EventLog Analyzer: Encryption and data integrity techniques

In event log management, data security and integrity are crucial for ensuring accurate and reliable analysis. EventLog Analyzer has several mechanisms to ensure that the security of log data is maintained at every stage of the log management process. This document outlines the various encryption and data integrity methods adopted by EventLog Analyzer to secure log data at different stages of data collection and processing.

Here's a list of the **common encryption modules** that are used in various data processing stages in EventLog Analyzer:

1. **WMI/DCOM:** EventLog Analyzer uses WMI, which uses authentication protocols like KerberOS or NTLM, based on the type of AD environment for secure communication, verifying data authenticity and preventing modifications during any data transfer.

2. **TLS:** This protocol is used to secure communication between EventLog Analyzer and various components like agents, syslog, and Elasticsearch.

3. **HTTPS:** The web interface uses HTTPS for secure communication, protecting data from unauthorized access and eavesdropping across all mediums.

4. **AES 256:** This encryption algorithm protects archived log data at rest, safeguarding its confidentiality and integrity.

5. **SHA-256:** This hashing algorithm verifies data integrity during transmission and storage, ensuring no unauthorized changes have been made.

6. **LDAP over SSL:** Fetching domain objects are done over traffic secured by protocols like SSL.

Let's look at the different stages of data transit below, along with their respective security standards.

1. Data collection medium

EventLog Analyzer collects data from multiple log sources, such as Windows systems, Unix or Linux systems, applications, databases, firewalls, routers, switches, IDSs, and IPSs. The solution supports both agent-based and agentless log collection mechanisms to cater to all devices and applications in the network. The encryption standards in use are listed below.

2. Agent communication: AES-256 and RSA

Agents will be discovered automatically by the EventLog Analyzer server once installed and will automatically collect the logs from the configured devices. This standard seamlessly pre-processes the logs and transfers data to the server in real time.

- The log data collected by these agents is encrypted using the AES-256 algorithm.
- For data in transit, the RSA algorithm is used for communication between the server and agent.
- Additionally, while transferring log zips, HTTPS can be enabled to ensure additional security. (The same ciphers as SSL communication are used.)
- Digital signatures are also used for additional assurance of the log data's authenticity and origin.

3. Agentless communication: Windows log collection

- Under agentless log collection, the Windows API is used to retrieve logs from devices using the WMI method and real-time collection. The specific logs collected are determined by the security configuration set for WMI, RPC, and DCOM in the user's environment. To understand how these configurations are set, please refer to this article.
- As for encryption, WMI uses Kerberos or NTLM authentication. The configuration of ciphers can be managed through the settings in AD. The encryption needs to be set in the user's AD environment. Please refer to this link to know more.

Syslog collection: TLS

- Since the syslog is usually forwarded from the users' end, it's advisable to communicate using the TLS protocol.

Other log sources

For other log sources, like IIS applications and vulnerability scanners, WMI is used. Secure protocols, like SMB, FTP, and SFTP, are used for importing manual logs.

4. Live logs

EventLog Analyzer stores all the live data in Elasticsearch, which is used for various querying purposes.

- The live data in Elasticsearch is stored in binary format, which is not directly readable. During a search, the data is decoded from binary format and the result is provided.
- However, the data transfer between EventLog Analyzer and Elasticsearch is secured with a search-guard plugin.
- The sensitive information, like product configuration and device details, are stored in encrypted form in DB, for which we use AES256 for postgres DB and MSSQL (Supported only above MSSQL 2000).

5. Log archival

EventLog Analyzer automatically archives all event logs and syslogs collected from Windows and UNIX devices, and other syslog devices on the EventLog Analyzer server.

- EventLog Analyzer encrypts the event log archive files with AES-128 standard to ensure the log data is secured for future forensic analysis, compliance and internal audits. This must be enabled in **Settings > Admin Settings > Manage Archives > Settings.** Refer to this document for detailed steps.
- To ensure strong password integrity, the user credentials are encrypted using the Bcrypt hashing algorithm.
- The time stamping technique ensures that the archived data files are tamper proof. If there is a modification of a file, this technique will reveal that the file has been tampered with.

6. Remote data access

EventLog Analyzer allows authorized users to access and manage the system remotely from anywhere with an internet connection.

- It's advisable to enable HTTPS to avoid any adversary-in-the-middle threat. The data in transit will be encrypted to maintain its integrity.
- Additionally, EventLog Analyzer monitors and logs all remote access sessions for auditing purposes.

7. Remote authentication for local and AD technicians

EventLog Analyzer uses different encryption standards for remote authentication based on the type of technician:
Local authentication - JAAS authentication
AD Technician - NTLM or Kerberos

- Account lockout policies are also enabled to prevent unauthorized access after multiple failed login attempts for a technician.
- EventLog Analyzer provides a built-in option to generate the audit trail of all user actions performed in the product. This ensures accountability within the solution itself.

Other security and integrity measures

- **Secure web communication:** EventLog Analyzer is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling HTTPS protocol ensures that all web communication is secure.
- **Session termination after idle time:** With EventLog Analyzer, you can set up a session expiry time after which the session will be terminated. The default setting is 30 minutes. However, users can change it if needed, with the minimum session time being 10 minutes.

Encryption and data integrity in ADAudit Plus

ManageEngine ADAudit Plus is an auditing tool that collects raw event log data from Windows server environments and transforms it into actionable reports and alerts. ADAudit Plus employs industry-standard encryption methods to ensure the security of the data both at rest and during transit.

1. Encryption of data in transit

The data that ADAudit Plus collects can be classified into two categories:

- Event log data
- Active Directory (AD) data

For collecting event log data, ADAudit Plus lets you choose between the following event fetch modes:

- Real-time mode
- EvtQuery mode and
- WMI mode

Of the three event fetch modes, Real-time and EvtQuery modes encrypt the data transferred that is over the network by default. The WMI mode does not encrypt the data during transfer by default. However, encryption can be enabled in the WMI event fetch mode to ensure that the data is secure during transfer.

For collecting AD data, ADAudit Plus uses Active Directory Service Interfaces (ADSI) and LDAP.

Users can import third party **SSL certificates** in ADAudit Plus, to encrypt all the data that is collected and transferred over the network.

ADAudit Plus lets users:

- View the collected data in the form of reports and alerts via the **User Interface** (UI) that runs on a browser.
- Configure **alerts** to get notified of security events via email and SMS. An SMTP server configuration is used for sending emails and an SMS provider configuration is used to send SMSes.
- Forward collected data to any **SIEM** solution.

ADAudit Plus provides the option to enable **HTTPS** from within the product UI to encrypt the data accessed via the UI and the data forwarded to SIEM solutions.

ADAudit Plus allows the use of **TLS** to secure connections while configuring mail and SMS servers for receiving alert notifications. TLS versions 1, 1.1, and 1.2 are supported.

2. Encryption of data at rest

The event log data and the AD data that is collected from the configured computers, is stored in ADAudit Plus' built-in PostgreSQL database. ADAudit Plus employs the following encryption and data protection techniques to ensure that the data stored in the PostgreSQL database and the database itself are protected:

- **AES 256-bit algorithm** is used to encrypt sensitive data (such as passwords), that are stored in the PostgreSQL database.
- The database itself can be secured by a password. This password is also encrypted using AES 256-bit algorithm, additionally the key used here is instance specific.

ADAudit Plus comes with a built-in admin account with extensive privileges. However, Technician roles can be configured to limit access to the product UI and also restrict individuals from performing administrative functions such as adding or removing servers for auditing, modifying configuration settings, and more.

- Administrator and technician passwords are encrypted using **bcrypt hashing algorithm**. A salt is added to the hashing process here to mitigate password attacks further.

Other security and integrity measures

While ADAudit Plus encrypts the sensitive data both at rest as well as in transit, encryption is only a part of our security strategy. To learn more about other security aspects of ADAudit Plus, check out these resources:

- Security specifications of ADAudit Plus
- Security hardening for ADAudit Plus

ERP level-by-level encryption methods

ERP Module	Details	Stored In/ Accessed Via /Protocals	Task Group	Algorithm
Database Password	Database Password stored in database_params.conf file in encrypted form. Encrypted by the cryptag	File	Encryption	AES256
Database Connection	SSL not implemented in jdbc connection	jdbc	Encryption	SSL
Database Sensitive Column Encryption	schar columns are encrypted by the ECTag key	Database	Encryption	AES256
Database Encryption key	Database encryption key (ECTag) stored in customer-config.conf file in encrypted form. Encrypted by the cryptag	File	Encryption	AES256
InBuilt Technician Password	InBuilt technician passwords are stored in database as a hashed value	Database	Hashing	BCrypt
Export Reports with password	Exporting reports with password protected	File	Encryption	Zip File Encryption
Client Server Communication	Browser to Exchange Reporter Plus Server communication	Https	Communication	TLS 1.0, 1.1, 1.2 SSL
Server To Active Directory Communication	Exchange Reporter Plus server to Active directory communication	LDAPS	Communication	SSL
Microsoft 365 Rest API communication	Exchange Reporter Plus to Microsoft 365 communication	HTTPS	Communication	https://learn.microsoft.com/en-us/dotnet/api/system.management.automation.pscredential.-ctor?view=powershellsdk-7.0.0#system-management-automation-pscredential-ctor(system-string-system-security-securestring)

SSL certificate management	SSL Certificate Tool in Exchange Reporter plus	Self-signed cert signature algorithm: SHA256WithRSA Key algorithm: RSA	Encryption	
Email Server Communication	Javamail used for email communications	JavaMail	Encryption	TLS 1.0, 1.1, 1.2 SSL
SMS Server Communication	org.smslib used for sms communication			
Microsoft 365 MSOnline Module (Powershell)	ADmanager Plus to M365 communication via powershell	Powershell (https)	Communication	
Other ME Product Integrations	Integrations with other ME products like AD360, SDP, ADMP etc.. using auth token and tight integrations	HTTPS	Communication	
Exchange Communication	On Prem Echange communication using powershell	Powershell (https)	Communication	
Active Directory Authentication	AD login	Kerberos/NTLM	Communication	TLS 1.0, 1.1, 1.2 SSL
Database Backup zip	7zip is used and zip is password protected	Files	Encryption	
Log Collection - Files	Collecting event data from Exchange Traffic/ IIS Logs	Files - SMB (Windows File Share)	Communication	
Elastic Search Communication	ERP stores/retrieve event data from/to Elastic Search	HTTPS(Search guard)	Communication	

Encryption standards and data integrity measures implemented in M365 Manager Plus

ManageEngine M365 Manager Plus is a comprehensive solution that can generate reports as well as manage, audit, and monitor the objects and data within your Microsoft 365 environment. Several measures have been taken to ensure that the data processed in the product is handled securely and that its integrity is not tampered with. This document outlines the various encryption and data integrity methods implemented to ensure the safety of all the data gathered and handled by M365 Manager Plus.

The data processed in the different modules of M365 Manager Plus is secured using a range of encryption algorithms. These include:

- **AES-256:** This robust, efficient algorithm is used to encrypt the passwords of the product database and audit logs from Microsoft 365.
- **SSL:** This cryptographic protocol is used to ensure the integrity and security of the emails, notifications, and log traffic in the product.
- **Bcrypt:** This password hash function is used to securely store the passwords of the built-in technician accounts.
- **TLS:** This protocol secures the data of the audit, alert, and monitoring modules and ensures the integrity of the emails and notifications from the product.
- **HTTPS:** This is used by the web browser (client) to secure the communications that are sent out to the M365 Manager Plus server and Microsoft 365 servers.

Here is how the data in each module of M365 Manager Plus is processed and secured:

1. Data collection

a. M365 Manager Plus uses PowerShell, the Microsoft Graph API, and REST APIs to collect data from Microsoft 365 and execute any actions in your Microsoft 365 environment. This is secured using HTTPS. This ensures that none of the data transferred between the client and the M365 Manager Plus server is tampered with. The collected information is stored in configured databases and can be accessed as reports. Sensitive data is not stored in the scripts or API calls, and only the necessary information is used in the calls for interacting with Microsoft 365 servers.

b. All the actions carried out by users in M365 Manager Plus are recorded in an audit report and stored in the product database. This makes it convenient to track unplanned operations, privilege abuse, and untimely logins.

c. You can archive audit log data beyond the standard 180-day limit of Microsoft 365. This archive can be stored on the same server or on a remote server by using a log forwarder. The security of the archived data is ensured by setting up a password of your choice and encrypting it using the AES-256 protocol.

2. Secure communications

a. The browser client can be accessed by entering the IP address or host name and the port number of the M365 Manager Plus server as the URL. Communications between the client and the server can be secured by enabling HTTPS after applying an SSL certificate.

b. All communications and API calls from M365 Manager Plus to Microsoft 365 servers are secured using HTTPS.

c. The reliable delivery of log messages is ensured with TCP.

d. A mail server can be configured to send product notifications, alerts, and emails to technicians in M365 Manager Plus. If you use SMTP to authenticate the mail servers, you can choose to use OAuth to secure your authentication better. You can also set up Microsoft or Google mailboxes to act as servers using their respective API authentication.

e. The JavaMail API used for emails and notifications is encrypted using SSL and TLS algorithms.

f. Integrations with other ManageEngine products, like AD360, are secured using authentication tokens. Communications between these products are conducted through HTTPS.

3. Microsoft 365 and PII data security

a. Data backed up using the Exchange Online Backup add-on can be encrypted with a password of your choice using the AES-256 encryption standard.

b. Reports generated with M365 Manager Plus can be exported and stored locally on the server or emailed. They can be exported as a password-protected ZIP file. You can create a password of your choice, and it will be encrypted using AES-256 and stored in the product database.

4. Database security

a. M365 Manager Plus has a built-in PostgreSQL database. You can also configure an external Microsoft SQL Server or PostgreSQL database for product data. This database stores all the product settings, including audit, monitoring, and report profiles, as well as technician information. To protect sensitive data, the database is password-protected and encrypted with CrypTag using AES-256. The encryption key is also encrypted using CrypTag with AES-256.

b. In addition to the database, M365 Manager Plus also leverages Elasticsearch for faster performance. All audit, alert, and monitoring data, along with data backed-up using the Exchange Online Backup add-on, is stored here. Access to this data is restricted to the Elasticsearch API and the product's certificate. The Search Guard plug-in for Elasticsearch guarantees the secure transfer of Elasticsearch data when TLS is employed.

5. Authentication for Microsoft 365 and Active Directory technicians

a. M365 Manager Plus supports adding users from Microsoft 365 and Active Directory as help desk technicians.

b. Microsoft 365 users will be redirected to Microsoft 365's login page, where the authentication will take place. Once they log in to Microsoft 365, they will be redirected to M365 Manager Plus.

c. Active Directory users will be authenticated in M365 Manager Plus with Kerberos and NTLM authentication.

d. The passwords of the default technicians are hashed and stored in the configured database using bcrypt encryption.

Encryption in the ADManager Plus database

ADManager Plus' database uses the following encryption methods to store sensitive data:

Database	Encryption method
PostgreSQL	AES-256-CBC
Microsoft SQL	AES-256-CBC

The following sensitive information is encrypted and stored in the database:

Functionality	Encryption standard used for storage	DataType
ADManager Plus Technician credentials	Hashed password BCRYPT Algorithm with SALT	CHAR
AD Domain Setting credentials	AES-256 Encryption	SCHAR
Mail Server and SMS Gateway Credentials	AES-256 Encryption	SCHAR
Technician's Auth Tokens	AES-256 Encryption	SCHAR
DB Password	AES-256 Encryption	Encrypted text
Proxy Settings	AES-256 Encryption	SCHAR
Export result and DB backup - Password	AES-256 Encryption	SCHAR
Encrypt Key store Password - SSL	AES-256 Encryption	SCHAR
Microsoft 365 Account credentials	AES-256 Encryption	SCHAR
End Users Password - Audit data	AES-256 Encryption	SCHAR
External Integration - Account details	AES-256 Encryption	SCHAR
Username and password of high	AES-256 Encryption	SCHAR
availability settings	AES-256 Encryption	SCHAR

User and Entity Behavior Analytics (UEBA) - Encryption and data integrity techniques

UEBA is a module within Log360 dedicated to detecting abnormal patterns in user and entity activities. Through behavior analysis, UEBA aids in identifying potential threats and bolstering overall security in the network.

This document provides an overview of the diverse encryption techniques and integrity checks deployed at each stage of data processing in UEBA, ensuring the security and reliability of log data.

1. Data collection

Data within UEBA is sourced from EventLog Analyzer via API calls. As a standard precautionary measure against MITM attacks, it's imperative to enable HTTPS, thereby ensuring robust data encryption during transit.

2. Real-time log collection via ActiveMQ

Data retrieval in UEBA occurs in real-time from EventLog Analyzer through an ActiveMQ messaging queue. This system utilizes the open wire binary protocol to facilitate high-performance messaging.

3. Data storage and archive

UEBA utilizes Elasticsearch as its primary data storage solution. Anomalous data within Elasticsearch is stored in binary format, which is inherently unreadable. When conducting a search, this binary data is deciphered to provide the desired results. However, to ensure secure data transfer, the following techniques are employed:

- Sensitive information such as product configuration and device details is stored in encrypted form within the database.
- For PostgreSQL databases, AES256 encryption is utilized.
- For MS SQL databases, encryption is supported for versions above MS SQL Server 2000. Further details can be found here.
- Model files are stored using the Java Serialization method.

4. Password integrity

To ensure strong password integrity, the user credentials are encrypted using Bcrypt hashing algorithm.

5. Remote authentication for local and AD technicians

UEBA uses different encryption standards for remote authentication based on the type of technician:

- Local authentication - JAAS authentication
- AD Technician - NTLM / Kerberos

Account lockout policies are also enabled to prevent unauthorized access after multiple failed login attempts for a technician. In addition, UEBA also generates an audit trail of all user actions performed within the product. This functionality ensures accountability within the solution itself.

6. The list of ciphers supported in UEBA are given below:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

7. How is the product installation directory secured?

The product installation directory is secured to guarantee file security and integrity. Access to the installation directory is granted only to the following types of user accounts:

- Local system account
- User account utilized during product installation
- Administrators group

This is applicable for installations of build 4050 and above.

Other security and integrity measures

- **Secure web communication:** UEBA is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling the HTTPS protocol ensures that all web communication is secure.

- **Session termination after idle time:** With UEBA, you can set up a session expiry time after which the session will be terminated. The default setting is 30 minutes. However, users can change it if needed, with the minimum session time being 10 minutes.

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

About ManageEngine Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download