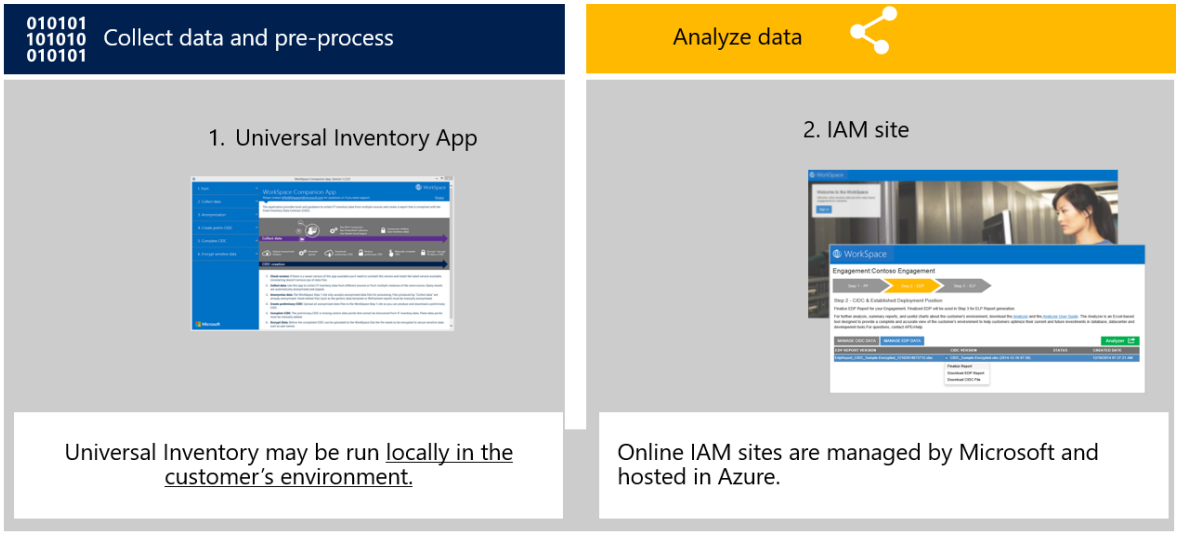
Software Asset Management (SAM) Engagement
Data Usage and Privacy Information – Intelligent Asset Manager 2018

Software Asset Management (SAM) best practices allow companies to gain a complete picture of their IT estate to enable fact-based technology decisions.

A Microsoft SAM Engagement includes four primary phases: planning, data collection, data analysis, and the presentation of the final results. This document defines the types of data collected, the inventory process, the data workflow, and security measures put in place to help protect the data and privacy of customers and their employees.

The role of Intelligent Asset Manager 2018 (IAM)

Microsoft designed IAM to provide high quality and consistent results during the data collection and analysis phases of SAM Engagements. IAM facilitates the collection and analysis of highly fragmented data through the use of two components: The Universal Inventory App and the IAM site.



The Universal Inventory App is a Windows Desktop Application installed in the customer's environment used to collect software deployment and usage data from multiple of sources to create a single, de-duplicated and normalized product inventory database. Data is stored in a local SQL express or any other SQL DB. The consolidated Microsoft usage related data goes into one Excel workbook, called the Clean Inventory Data Contract (CIDC).

The Universal Inventory App is also used to encrypt personal information prior to uploading data to the IAM site. Encryption is performed by a separately installed Universal Inventory component, the Encryption/Decryption tool.

The IAM site, managed by Microsoft and hosted on Azure, then summarizes the data in the CIDC into a report called the Established Deployment Position (EDP) for review and completion. *If required or requested by the Customer*, the IAM site may then be used to map Microsoft license entitlements to the EDP data, to generate the customer's Effective License Position (ELP) report. The CIDC, EDP, and ELP reports are all Microsoft Excel workbooks.

Microsoft

IAM rejects ALL files before being transmitted unless encrypted using the Universal Inventory App to ensure any data that could contain customer's personal information is encrypted. Except when you request ELP Services (described below), Microsoft will not have access to customer's personal information.

Data collection

A SAM Engagement requires gathering full deployment and usage data for accurate and complete results. Examples of basic product data points collected include:

- Installation Date
- Software Product Name
- Software Product Version
- Environment Type (Production, Non-production, and Training)
- Operating Division

Additionally, some data collected may contain personal information. "Personal information" means any information that identifies or can be used to identify, contact, or locate the person to whom it pertains, or from which identification or contact information of an individual person can be derived.

This information is used in IAM to help de-duplicate inventory records, identify areas where investment optimization can occur, during the creation of an ELP, etc. As noted above, all data fields that potentially contain personal information are encrypted before being transmitted to Microsoft and remain encrypted during storage.

Examples of data collected that commonly may contain personal information:

- User Name
- Machine Name
- Domain Name
- IP Address
- Location

Only non-Microsoft data pertaining to the management and deployment of virtualized Microsoft environments is retained for final reporting. All other non-Microsoft data is purged from the IAM site during data analysis. For example, collected software deployment and usage data may contain Citrix XenApp, which may be necessary to identify what applications are being used in implementations of Terminal Services.

Data analysis

EDP Creation: The IAM site uses the encrypted and uploaded CIDC to generate a EDP report. The EDP is a detailed snapshot of the customer's Microsoft software deployments that enables the customer to validate for completeness and accuracy. While it does not include license entitlement data, it often includes information on how the software is being used and can also be used to identify opportunities for further optimization such as underutilized servers or workloads that can move to the cloud to improve efficiency within the customer environment.

ELP Creation: If requested or required, an ELP is created once an EDP is final by uploading the customer's Microsoft license entitlement information and comparing it to software deployments and usage in the EDP. This report provides the customer with their current license position.

ELP Services: This is a Microsoft led service that can create an ELP as described above. The benefits of using ELP Services are that a dedicated team is available to perform the complex work of mapping licensing to product inventory. If a customer chooses to use ELP Services, Microsoft or its subprocessor must access decrypted

personal information and will obtain the customer's written consent directly via the IAM tool prior to starting. The subprocessors may be located in the United States or in another country, and the data will be encrypted during transfer to the subprocessor. Access to personal information is limited to the duration of the ELP Services work only.

Other: In certain cases, primarily complex IAM technical support events, a SAM Partner or a customer may also desire to provide Microsoft, directly or through its partner, with the decrypted personal information to facilitate resolution. Like ELP Services, Microsoft will obtain written consent directly from the customer before any decrypted personal information is accepted.

Data workflow and privacy protection

The SAM Partner, and SAM Engagement Manager will work with the customer to ensure all Microsoft policies and procedures are met for sharing and sending personal information. All parties should be aware of the sensitive nature of the data handled in a SAM Engagement and take steps to always safeguard personal information.

Microsoft is committed to customer data protection and privacy. Although the IAM site will reject files that have not been encrypted using the Universal Inventory App, the customer and SAM Partner are responsible for the encryption of personal information data locally, before uploading to any IAM site.

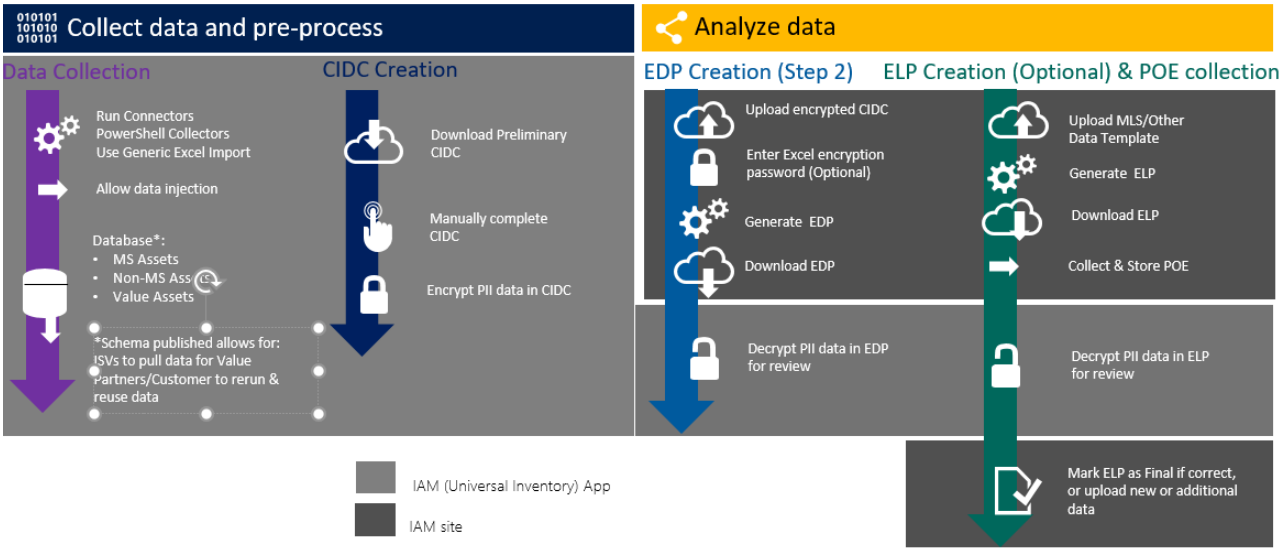
Encryption is a type of privacy protection and is defined fully below.

Encryption
Advanced Encryption Standard - 256 bit (AES-256) is used to replace personal information within the CIDC with generic values during Data Analysis before it can be uploaded to the IAM site. AES is a specification for the encryption of electronic data, established by the National Institute of Standards and Technology (NIST). This method uses a cryptographic key (password) to both encrypt and decrypt the data. Since the CIDC feeds into the EDP and ELP reports, any personal information stays encrypted as long as it is in the IAM site. Once downloaded, the customer can decrypt the reports using the same password and the Universal Inventory App. **If a CIDC is not encrypted by the Universal Inventory App, it will be rejected by the IAM site.**

Microsoft has implemented multiple measures to support the security of customer data and to prevent access from outside of the IAM site. For example, to determine if files are approved for upload, the Universal Inventory App places a value based key (referred to as an Encoding Token) within the files when they are encrypted. Upon upload, the IAM calculates the value on the uploaded file and compares it to the value written to the Encoding Token by the Universal Inventory App. If the files have not been encrypted using the Universal Inventory App, then these values (Encoding Token) will not match the file and, by design, the files will be rejected by the IAM.

Additionally, Role Based Security is implemented throughout the process, an audit trail is maintained and monthly security reviews are conducted. The only administrators for the application system are the Microsoft IAM Team.

This flowchart shows the IAM engagement steps, including where encryption takes place:



Data storage and sharing

A SAM Engagement does require the transfer of encrypted personal information. This information is transferred to the United States for processing by Microsoft. When you or a SAM Partner asks Microsoft to provide ELP Services, Microsoft and its subprocessors will access unencrypted personal information. The subprocessors may be located in the United States or in another country, and the data will be encrypted during transfer to the subprocessor. Microsoft only collects data which is necessary for the legitimate interests of the customer, the partner, and Microsoft. Before loading any data into the Universal Inventory App it is the responsibility of the customer and partner to determine if the engagement and data can be managed in a way that complies with local laws, including determining whether customer and partner need to enter into a data processing agreement with one another. Microsoft abides by current European data transfer requirements regarding the collection, use, and retention of data from the European Economic Area and Switzerland.

When the engagement is complete, product use summary data is transferred from IAM to a Microsoft data storage infrastructure and is retained indefinitely for internal purposes including but not limited to analysis, training and product planning. However, data points which may contain personal data are deleted and are not transferred. SAM Engagement data is purged from the IAM site 90 days after the close of the engagement. Customers receive the final CIDC, EDP, and ELP reports for their future use, and all reports can be decrypted by the customer or SAM Partner. Further, the customer retains their UI database containing the centralized, de-duplicated full scope of their IT estate.

As always, Microsoft strongly recommends that customers and partners password protect or encrypt all Microsoft Excel files prior to transmitting via email or other means (e.g. FTP). Passwords should be provided through separate communications and never sent with the protected report.

Resources

Microsoft, its affiliates, subprocessors, or agents will use your data in accordance with this Software Asset Management Engagement Data Usage and Privacy Information document and the below Microsoft Privacy Policy and commitments under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

Microsoft's Privacy Policy: https://privacy.microsoft.com/en-US/privacystatement

For additional information on Microsoft Corporate Citizenship and Law Enforcement requests, visit: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

For additional information on Microsoft Principles, Policies and Practices, visit: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/

Microsoft participates in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks https://privacy.microsoft.com/en-us/microsoft-eu-us-privacy-shield

Managing and protecting information https://www.microsoft.com/en-us/legal/compliance/buscond/managinginfo.aspx