

**Microsoft**

**Asset Inventory Service (AIS)**

**Privacy Assessment Report**

**Presented by Jefferson Wells**



**May 2008**

This report is intended to be used in its full and original content. Any use of this information not in its full and original content is prohibited without the express written consent of Jefferson Wells management.

## Table of Contents

EXECUTIVE SUMMARY .....	3
OVERALL CONCLUSION .....	5
FUNCTIONAL OVERVIEW .....	6
ASSESSMENT APPROACH.....	7
SCOPE.....	9
ASSESSMENT RESULTS .....	11

## **EXECUTIVE SUMMARY**

The following report details the assessment performed on the Microsoft Asset Inventory Service product. The Asset Inventory Service (AIS) Group, in coordination with Jefferson Wells, defined the scope of the engagement and the assertions to be included in the analysis. Jefferson Wells planned and performed the documentation reviews, interviews of key personnel and testing to validate the technical design, service-specific policies and procedures, and processes related to the identified assertions.

Jefferson Wells delivers professional services in the areas of technology risk management, internal audit, tax and finance and accounting. The Jefferson Wells Technology Risk Management group specializes in Information Technology assessments, security assessments, business continuity management and privacy reviews.

The objective of the review was to determine the validity of assertions for the Asset Inventory Service. The assertions tested were identified as appropriate statements that, when tested and validated, would assess Microsoft's adherence to elements of the privacy statements related to the transmission, use and/or collection of personal information or sensitive business information.

The assessment consisted of a review of the Microsoft Asset Inventory Service Inventory Agent, Web interface, software catalog and data transformation components.

The following assertions were used by Jefferson Wells in conducting the privacy assessment:

1. End users are authenticated using Windows Live ID's, with strong passwords enforced by the Asset Inventory Service shell.
2. All communications with the Asset Inventory Service are encrypted in transit.
3. Customer data within the Asset Inventory Service may only be accessed by end-users and applications with the customer administrator's explicit consent.
4. The Asset Inventory Service is hosted in a data center with appropriate physical access controls.
5. Customer asset data is logically segregated by unique "Customer ID". Customer administrators can only access data associated with their "Customer ID".
6. The Asset Inventory Service platform is authenticated by the agent prior to customer data transmission.

7. Agent asset data uploads can only occur while a valid Asset Inventory Service subscription is active.

8. The Asset Inventory Service agent software collects and uploads only information related to system hardware and software configuration, and does not analyze or upload any information pertaining to data files or documents located on the host system.

## **OVERALL CONCLUSION**

As of **May 2008**, and based on the assertions identified and the testing performed, Jefferson Wells found that **all 8 of the assertions were valid**. Testing results are located in the “Assessment Results” section of this document.

## **FUNCTIONAL OVERVIEW**

The Microsoft Asset Inventory service as tested is comprised of the following components:

### ***Asset Inventory Service Agent***

The Agent is a downloadable client that transmits information securely to the AIS web interface on a regularly scheduled basis.

### ***Asset Inventory Service Web Interface***

The Asset Inventory Service Web Interface is an online environment that provides AIS customer administrators with hardware and software information pertaining to their environment.

### ***Asset Inventory Service Software Catalog***

The Software Catalog is a sophisticated database of applications that is based on application signatures retrieved from AIS Agent inventory upload data.

### ***Asset Inventory Service Internal Data Management and Transformation Components***

The Asset Inventory Service employs numerous internal components for the management of customer inventory data; these components include databases, data transformation agents, and database reporting services for presentation of inventory reports to customers and AIS product team members.

## **ASSESSMENT APPROACH**

Jefferson Wells Technology Risk Management consultants followed a three-phase assessment approach to determine the validity of the Asset Inventory Service assertions. The phases included: Discovery, Validation of Assertions and Testing.

### 1. Discovery

Jefferson Wells conducted interviews with key Microsoft personnel to gain an understanding of the architecture, operational scope and privacy issues related to the Asset Inventory Service. Follow up interviews and document requests were initiated from these interviews.

### 2. Validation of Assertions

Once a solid base of understanding was established, Jefferson Wells reviewed the original assertions with a focus on privacy and the published "Microsoft Asset Inventory Service Privacy Statement". Jefferson Wells provided recommendations to Microsoft to modify the language of the assertions to be focused on privacy and to limit testing to privacy related issues.

### 3. Testing

Jefferson Wells developed formal test plans in order to create a repeatable process to execute the testing. The formal test plans should also provide individuals not directly involved in the testing with an understanding of the methodology used to validate the assertions and recreate the results, assuming there have been no changes to the product since Jefferson Wells testing was completed. Jefferson Wells testing methods included:

1. Observing the behavior of the product under specified conditions
2. Collecting screen shots of evidentiary data
3. Capturing and analyzing packets with a network "sniffer" while navigating to specified test URLs in a simulated end-user environment
4. Creating and utilizing test accounts within AIS to validate the assertions,
5. Collecting security and privacy related information from operations personnel and AIS product team members.
6. Collecting and reviewing AIS data management documentation, policies and procedures

Testing by use of capturing and analyzing packets was executed on non-Microsoft owned equipment and networks. The testing was designed to closely mirror a typical end-user's broadband environment. Test computers were deleted and clean installs of Microsoft Windows XP Professional and Windows VISTA Business with all service

packs were completed prior to testing and when switching between Internet Explorer 6 and Internet Explorer 7.

During the execution of the test plans, Jefferson Wells collected and cross referenced the appropriate evidence to the assertion test objectives in order to determine their validity.

## **SCOPE**

Jefferson Wells' scope was to attempt to validate the following management assertions as determined by the Microsoft Asset Inventory Service Group:

1. End users are authenticated using Windows Live ID's, with strong passwords enforced by the Asset Inventory Service shell.
2. All communications with the Asset Inventory Service are encrypted in transit.
3. Customer data within the Asset Inventory Service may only be accessed by end-users and applications with the customer administrator's explicit consent.
4. The Asset Inventory Service is hosted in a data center with appropriate physical access controls.
5. Customer asset data is logically segregated by unique "Customer ID". Customer administrators can only access data associated with their "Customer ID".
6. The Asset Inventory Service platform is authenticated by the agent prior to customer data transmission.
7. Agent asset data uploads can only occur while a valid Asset Inventory Service subscription is active.
8. The Asset Inventory Service agent software collects and uploads only information related to system hardware and software configuration, and does not analyze or upload any information pertaining to data files or documents located on the host system.

In order to complete the assessment, Jefferson Wells performed an evaluation of the Asset Inventory Service and the supporting environment, both development and production. The development area was reviewed for use of production customer information, and to ensure documented change management procedures are followed with respect to the privacy impact of proposed service changes. The following areas were evaluated to support the assertions:

1. The authentication process between the service, inventory upload agents, and customer administrator web interface in the production environment
2. Encryption of data transmissions between the service, inventory agents and customer administration web interface
3. Access to data in the development and production environments by system support personnel and the AIS product team
4. The development environment was reviewed for the use of customer.

## **ASSESSMENT RESULTS**

The assessment results were subject to testing of the following Microsoft Asset Inventory Service features for the related assertions noted below. The testing components included:

1. Asset Inventory web and client applications tested with Windows XP and Internet Explorer 6 and Internet Explorer 7 web browsers as of April 2008
2. Asset Inventory web and client applications tested with Windows Vista Business and Internet Explorer 7 as of April 2008.

	<b>Assertion</b>	<b>Valid</b>	<b>Not valid</b>
1	End users are authenticated using Windows Live ID's, with strong passwords enforced by the Asset Inventory Service shell.	X	
2	All communications with the Asset Inventory Service are encrypted in transit.	X	
3	Customer data within Asset Inventory Service may only be accessed by end-users and applications with the customer administrator's explicit consent	X	
4	The Microsoft Asset Inventory Service is hosted in a data center with appropriate physical access controls	X	
5	Customer asset data is logically segregated by unique "Customer ID". Customer administrators can only access data associated with their "Customer ID"	X	
6	The Asset Inventory Service platform is authenticated by the agent prior to customer data transmission	X	
7	Agent asset data uploads can only occur while a valid Asset Inventory Service subscription is active	X	
8	The Asset Inventory Service agent software collects and uploads only information related to system hardware and software configuration, and does not analyze or upload any information pertaining to data files or documents located on the host system	X	