Eracent FAQs

What is Eracent?

Eracent Enterprise Asset Management (EAM) is a tool that collects information from computer devices that can be used to support computer life cycle management and inform financial, contractual, and inventory processes to enable strategic decision making for the IT environment.

Eracent is comprised of the following modules:

- **End Point Analyzer (Eracent EPA Service):** performs a hardware and software inventory of the device. This agent collects data about what hardware and software are present. It does not collect information as to whether or not the software found is being used. It does not collect any usage-related information (i.e., monitoring of keystrokes or mouse clicks). This module also allows for the analysis of the inventoried information. Information gathered by this module is encrypted before being transferred to an on premise External Authentication Manger (EAM) server. This module is deployed on all computers imaged by UMIT.

- **Electronic Update Agent (Eracent EUA Service):** ensures the installed Eracent modules are properly maintained. The agent periodically checks with the EAM server to determine if there are any Eracent-signed updates to perform. This feature is only activated in cases where Eracent-signed packages are setup on the EAM web server and the device has been selected as a target for the update. This module does not collect any data at all from the device. This module is deployed on all computers imaged by UMIT.

- **Process Monitor (Eracent EPM Service):** collects usage information regarding the software installed on the device. This agent collects key stroke and mouse click counts on applications in order to determine level of activity in installed applications. This module is only deployed on computers at the Medical Campus, and in some student computer labs to collect information that will be used for lab virtualization.

- **System Usage Monitor (Eracent SUM Service)**: collects hardware resource usage information (including CPU, Network Interface, Memory, General IO, and Disk IO) about the device in general or about specifically tracked processes on the device. This module is not used by UMIT.

What is currently in use at the University?

Currently, the Eracent client is deployed throughout the University. The initial deployment of the Eracent client to the Medical campus included the End Point Analyzer, the Electronic Update Agent and the Process Monitor. Subsequent deployments of the Eracent client, as well as those currently being deployed, contain only the End Point Analyzer and the Electronic Update Agent. On Faculty and Staff computers, hardware and software information is being collected on the device. On approximately 50 lab machines in residence halls, the Process Monitor is installed and activated to gauge what software is actively being used. This information is being used to investigate future virtualization options in these areas.

Eracent FAQs

What is the purpose of Eracent?

The installation of the Eracent client on University-owned assets is intended to facilitate the maintenance and accurate inventory of hardware and software assets purchased with University funds.

Why is Eracent needed?

Due to the large number of assets owned and managed by the University, the installation of the Eracent client allows for the identification of aged assets in our environment, and the user to which the hardware is assigned, and reconciliation at a departmental level. This information facilitates accurate budgeting for asset replacement for each department that is eligible through the Computer Lifecycle Management Program. Furthermore, the deployment of Eracent allows us to assemble an inventory of known licensed software installed on University-owned devices. Having this information centralized and analyzed could highlight opportunities for volume purchase at a discount leading to potential fiscal savings. Without this client, such information gathering would need to be performed by manually, and would be an expensive and time consuming project.

What is the process if changes to the current Eracent client deployment are required?

In the event that an Eracent client module needs to be deployed, activated or upgraded, a change control request will be initiated through UMIT's change control board. Once approved by UMIT, ACAC will be informed of the change prior to its implementation.

Does Eracent pose a security risk?

With the installation of any software on a device comes risk. The limited risk associated with installing the Eracent client on University-owned devices far outweighs the benefits of maintaining the University's asset inventory in a secure, efficient manner, and provides opportunities to control associated software costs.

Technical Questions

Are all of the modules installed on the device even if only some are "turned on"?

Currently, only the modules in use are installed. If another module is determined to be required in the future, it would be required to be installed.

Could the Eracent information be breached if a hacker gains access to the device?

If a hacker has already compromised a machine, any information that the Eracent client has access to, the hacker also would have access to that information as well regardless of the Eracent client being installed.

Can someone get my password or read my email through the keystroke data?

No. Eracent does not know the specific keystroke, it only keeps a running count of keystrokes by application. Eracent has no mechanism to capture or store the content of the keystroke or mouse click.

Eracent FAQs

What does the keystroke and click reports look like?

A sample report is available by clicking here.

How does Eracent catalog software? Is it limited to specific commercial software (from Microsoft, Adobe, etc.), or does it catalog everything that is installed in the computer?

The End Point Analyzer takes an inventory of all software that exists on the machine, regardless of manufacturer, but does not report usage information.

The Process Monitor collects usage information on software. Default behavior upon installing the Process Monitor service on a computer is to report on all applications that are installed regardless of manufacturer. This default behavior can then be altered to limit the scope of metered applications. In the limited instances where the process monitor is installed, it is configured with the default behavior.

How often does the Eracent client installed on a computer send information back to the server (when something new is installed, every night, hourly, etc.)?

The Eracent client is in constant communication with the server for purposes of sending “keep alive” pings. However, communication of inventory information is configured to take place every seven days. Additionally, since the server is on-premise, the client needs to be on the UM network in order to communicate inventory information to the server.

Does the Eracent client scan the network that a computer is connected to and look for other devices and vulnerabilities?

No. The only part of Eracent that has the capability to perform a scan on the network is the Eracent Network Probe (ENP). The purpose of the ENP is to perform a clientless discovery, via TCP/IP, of devices that are on the University network. UMIT owns the ENP, as it is included in the Eracent suite. This module is installed on the Eracent server and not on individual computers. UMIT has used it in the past to discover devices that cannot have a client installed, such as printers, network switches and servers, in hopes of building a working inventory of those devices. It is not a tool that scans for vulnerabilities.