Zuum

Service Extension Tool for Client Operations

Version Q1 2022

Publication date: 1/1/2022

Table of Contents

1 Introduction to the service

1.1 Overview

Zuum is a complimentary service extension for “Client Operations” services. The main purpose of Zuum is to provide end-user device health information directly from the devices on top of device management tools, such as Microsoft System Center Configuration Manager or Microsoft Intune. With Zuum keeping Windows, drivers and applications up to date, there will be significantly reduced attack surface that a device can be exposed to. Windows 10 updates delivered by Zuum will help with overall security while maintaining control over the process. Driver updates will reduce hardware vulnerabilities and increase stability. Application updates will decrease application exploitability. Vulnerability report will help to prioritize which applications to update first. Inventory reports will help to see the installed software, hardware details and other useful device information.

2 Gathered information

2.1 List of data points and telemetry gathered from end-user devices[1]

- Device names
- Operating System build and version
- Antimalware client version and definitions updates
- Microsoft windows, driver and software updates
- Hardware information, including attached monitors, battery health, TPM chip version
- Installed software names and versions
- SCCM Client Agent version and health status
- Error logs and reliability events
- Bitlocker status
- Free disk space
- Optional: Zuum can retrieve logged in user name from Windows 10 devices if this feature is enabled
- Optional: Zuum can retrieve network information from Windows 10 devices if this feature is enabled
- Optional: Zuum can retrieve location from Windows 10 Location Services if this feature is enabled

Operational data that is device specific is stored for 30 days. Summary reports that cannot identify a user or a specific device may be stored for 1 year or more to have historic data for comparison/trend reports. Upon customer’s request or when the contract ends, the customer tenant is deleted and all gathered inventory data is erased within 2 weeks.

Whenever new functionality is introduced in Zuum, a separate Change Request will be presented to the customer to approve it before rollout on customer devices.

[1] Sample of data gathered can be found in the Appendix at the end of this document

3 Architecture and security

3.1 Architecture details

Zuum agent installed on end-user devices is used to gather event information. The agent then connects to 3 different back-end services in Microsoft Azure Cloud – API, IoT Hub, Storage Blob.

- API – used for device registration and additional layer of communication encryption
- IoT Hub – used as a communication channel to instantly send and receive status messages
- Storage Blob – used for one-way storage of event logs, reliability events and other error messages

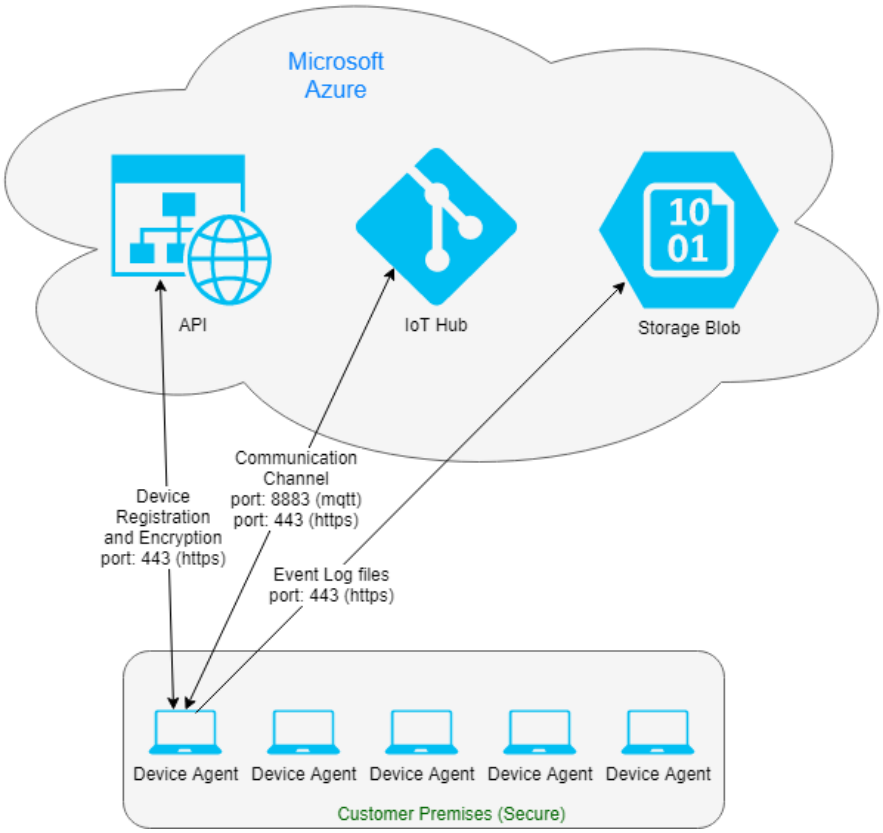


Figure 1 - Description

3.2 Security

1 Back-end isolation - all 3 back-end services are provisioned per customer and are not shared.

2 Client communication – all messages and data between end-user devices and all the back-end services are secured and encrypted HTTP over SSL encryption (https) is used for all communication. The IoT Hub can also use MQTT over TLS encryption (port: 8883).

3 When device connects to IoT hub with its unique DeviceID, it stays permanently connected and can either send or receive messages from IoT hub and read or update its own information. One device cannot read or update information about another device. If a device re-registers with the same DeviceID then for security purposes previous information about the device in IoT Hub is archived and deleted.

4 Zuum agents on devices may need to upload a log file to Storage Blob for troubleshooting purposes. This data is sent and stored on the Azure Storage Blob. The communication and access mechanism is “upload only”. Therefore, a device agent can upload but cannot read information from Storage Blob (including the information it has uploaded before).
5 Zuum data is encrypted in transit and at rest.

3.3 Zuum Agent functionality

Commands received from IoT hub can be used to initiate only predefined actions on the device. The current release of Zuum agent can perform the following defined actions:

3.3.1 Zuum agent:

- Uninstall Client – This action will uninstall Zuum from the device
- Update Client Policy – This action will update Zuum applied settings and refresh device inventory data
- Device:
  - Force Reboot – This action will reboot the device immediately (can be used for unattended devices)
  - Send Message – This action will send a custom message to the currently logged in user
  - Running Processes – This action will list all running processes on the device
  - Running Services – This action will list all services on the device

3.3.2 SCCM:

- Trigger SCCM schedule – This will trigger a pre-defined manual SCCM Client Agent action
- Repair SCCM Client – This action will trigger a manual SCCM Client Agent re-installation
- Request Reboot – This action will prompt the currently logged in user for a device reboot with an option to postone it
- Repair WMI – This action will trigger Windows Management Instrumentation repair
- Repair WUA – This action will trigger Windows Update Agent repair

Zuum agent will keep itself up-to-date for bugfixes and stability purposes.

3.4 Zuum Agent bandwidth and resource consumption

3.4.1 Estimated bandwidth metrics:

The agent is always running as long as device is connected to the Internet.

- 24 KB per agent policy sync (1 per hour per device)
- 100 KB estimated per log file upload (per request, used rarely)
- 40 MB for agent update (1 per device every 2 weeks)

The total estimated daily network bandwidth consumption is 1 MB per device.

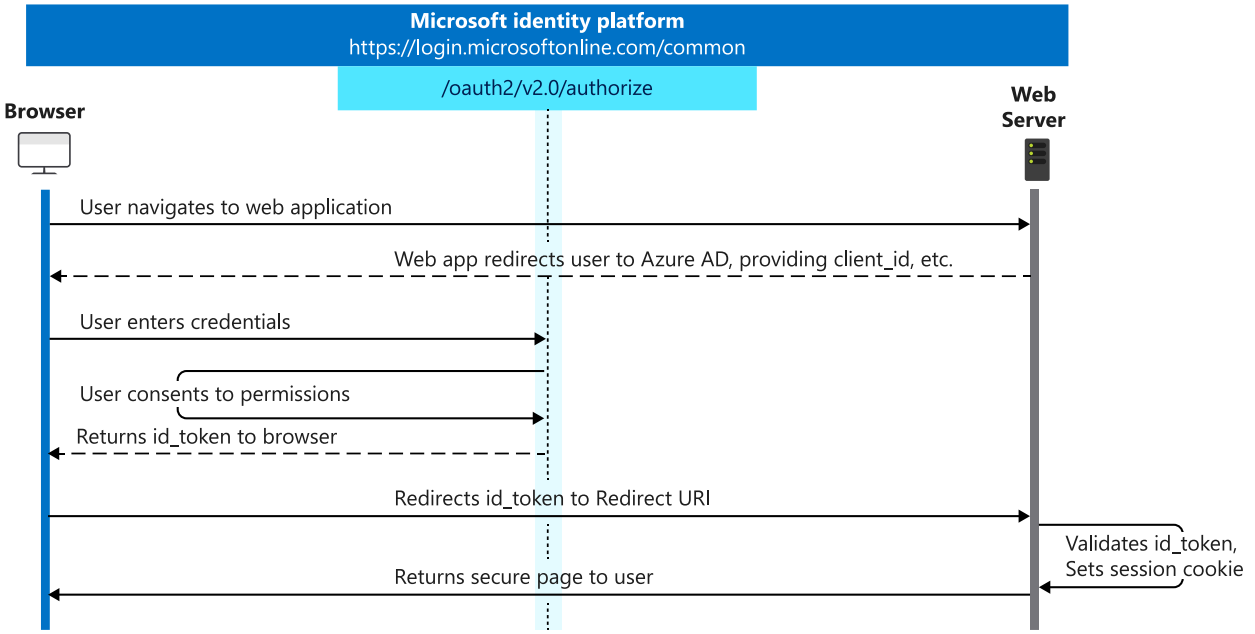
For 1000 devices it would be 1 GB/daily. The number can be further reduced by polling data less frequently.

3.4.2 Estimated resource consumption:

- The agent itself does not do any CPU-intensive tasks. Periodically it may initiate Windows Update scan against Microsoft Update service to detect missing security updates.
- The agent could consume periodically 60 MB of RAM or less.
- The agent does not have hard drive intensive activities, such as file searches or file processing that could lead to noticeable disk usage.

3.5 Zuum Portal Authentication & Authorization

Zuum Portal utilizes Microsoft OpenID Connect over OAuth 2.0 authentication protocol. Therefore users authenticate in their own Azure AD, respecting defined two factor authentication and other security policies. Authenticated users are then assigned roles and permissions within the Zuum portal itself.



Therefore there are multiple layers of security. First layer is the customer's Azure AD authentication. Second layer is Zuum role assignment. If a user has no role assigned within the Zuum User Management page, access is denied. If a user is removed from either customer Azure AD or Zuum User Management page, access is denied.

4 Delivery of the service

4.1 Tools used for the service delivery

Tool/Solution/ System	Explanation	Vendor	Processed PD types*	Processing methods*	Storage
Azure IoT Hub	Used for communication with the devices	Microsoft	1,2,3,4, 5**	1,2,3,4,9	Netherlands
Azure Function App (API)	Used for Enrollment to IoT Hub and other Zuum functions	Microsoft	1,2,3,4, 5**	1,2,3,4,9	Netherlands
Azure Storage Blob	Stores information gathered from the devices	Microsoft	1,2,3,4, 5**	1,2,3,4,9	Netherlands

Tool/Solution/ System	Explanation	Vendor	Processed PD types*	Processing methods*	Storage
Azure Storage Tables	Stores information gathered from the devices	Microsoft	1,2,3,4, 5**	1,2,3,4,9	Netherlands
Azure DataFactory	Used to merge and convert different device data types for reports	Microsoft	1,2,3,4, 5**	1,2,3,4,9	Netherlands

*Personal Data types and methods is defined in table below:

4.1.1 Data processing type and method clarification

	List of Personal Data types
1	Name Surname
2	Business contact information (email)
3	Employment details (employer)
4	IP address
5	Location **(Location data of Customer's assets is collected only if agreed with Customer in the Agreement)

	List of processing methods		
6	View	**4**	Store
7	Collect	**9**	Erase
3	Record		

**The last known device location can use Windows 10 Location Services to determine its location. To enable this feature, it must be ensured the Data Processing Agreement between Atea and Customer covers this type of data.

4.2 Risk in the service delivery

Atea has identified the following risks regarding the service delivery at hand and Atea cannot be held liable for those. The general risks of service delivery are described in Service Delivery Management process description.

- Failure is due to Force Majeure
- Failure is due to lack of access for Atea to the systems/solutions to deliver the service at hand
- Failure is due to systems or infrastructure not under Atea responsibility and control (such as but not limited to failures or errors in the network or customer firewall settings)
- Failure is due to information security related actions conducted to avoid greater damages and which are not due to Atea previous negligence

- Failure is due to an error or defect in operation systems or applications provided by a third party, which Atea is not able to fix by itself with reasonable costs or where there is no fix available
- Failure is due to the customer missing a maintenance or support service agreement for fixing the hardware or application problem before the failure takes place
- Failure is due to the customer preventing Atea to perform fixes or to apply fixes to applications or is not performing the fix

5 Prerequisites

5.1 Technical pre-requisites

Customer's firewall must allow Zuum Agent communication to these core Azure endpoints:

- [customer_prefix].azure-devices.net (HTTPS port 443 and optional MQTT protocol, port 8883)
- [customer_prefix].blob.core.windows.net (HTTPS port 443)
- [customer_prefix].azurewebsites.net (HTTPS port 443)
- All three endpoints have unique prefixes per customer, therefore precise endpoint FQDNs will be provided during implementation.

Windows 10 or Windows 11.

Access to Microsoft Update URLs:

http://windowsupdate.microsoft.com

http://*.windowsupdate.microsoft.com

https://*.windowsupdate.microsoft.com

http://*.update.microsoft.com

https://*.update.microsoft.com

http://*.windowsupdate.com

http://download.windowsupdate.com

https://download.microsoft.com

http://*.download.windowsupdate.com

http://wustat.windows.com

http://ntservicepack.microsoft.com

http://go.microsoft.com

http://dl.delivery.mp.microsoft.com

https://dl.delivery.mp.microsoft.com

6 Rollout procedure

Zuum Agent first is set to safe “Read-only” mode. It can gather and report relevant information but does no interaction or changes to the end-user’s devices.

Create GPO or deploy agent via SCCM or Intune.

Monitor installation progress and verify that all devices have Zuum Agent installed.

Once everything is configured and ready, Atea creates Change Request to set Zuum Agent in “Interactive” mode that allows it to fix detected anomalies (for example: install missing software updates that are required and have been approved).

New functionality or new configuration is applied via Change Requests that are reviewed and approved by the customer.

7 Terms and abbreviations

Abbr.	Term	Explanation
AMS Riga	Atea Managed Services Riga	IT infrastructure company delivers world class services and software products.
BD	Business Day	Service delivery is provided on business days from Monday to Friday (including), excluding public holidays in Latvia.
BH	Business hours	From 08:00 – 17:00 Central European Time (CET) from Monday to Friday of a Business day.
	Change	The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items
CAB	Change advisory board	A group of people that support the assessment, prioritization, authorization and scheduling of changes. A change advisory board is usually made up of representatives from: all areas within the IT service provider; the business; and third parties such as suppliers.
	Customer	The Customer of an IT service provider is the person or group who defines and agrees the service level targets.
DPO	Data Protection Officer	Person responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements
GDPR	General Data Protection Regula	Regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas
	Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service.

Abbr.	Term	Explanation
ISM	Information security management	The process responsible for ensuring that the confidentiality, integrity and availability of an organization's assets, information, data and IT services match the agreed needs of the business.
IT	Information technology	The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software.
ITIL	The Information Technology Infrastructure Library	A set of best-practice publications for IT service management.
ISO	International Organization for Standardization	World's largest developer of standards. ISO is a non-governmental organization that is a network of the national standards institutes of 156 countries.
	IT Operations	Information technology operations, or IT operations, are the superset of all processes and services that are both provisioned by an IT staff to their internal or external clients and used by themselves, to run themselves as a business.
ITSM	IT Service Management system/solution	The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.
	Major Incident	The highest category of impact for an incident. A major incident results in significant disruption to the business.
PD	Personal Data	Any information relating to an identified or identifiable individual
	Problem	A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.
RFC	Request for change	A formal proposal for a change to be made. It includes details of the proposed change and may be recorded on paper or electronically. The term is often misused to mean a change record, or the change itself.
RACI	Responsibility assignment matrix	A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted and informed.
	Service	A means of delivering value to Customers by facilitating outcomes Customers want to achieve without the ownership of specific costs and risks.
SDM	Service Delivery Manager	A service delivery manager identifies a client's needs and oversees the delivery of the services within the context of the business. The foundation of this position is establishing processes to provide consistently high levels of Customer service in a cost-effective manner.

Abbr.	Term	Explanation
SLA	Service Level Agreement	An agreement between an IT service provider and a Customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the Customer.
SOP	Standard operating procedure	Documentation containing instructions detailing all relevant steps and activities for a procedure
SSR	Standard Service Request	Pre-defined Standard Request
	Transition	A change in state, corresponding to a movement of an IT service or other configuration item from one lifecycle status to the next.
	Vendor	Party responsible for Service Delivery tool development and compliance with GDPR and security requirements

Appendix 1 – Log files

Log files list accessible by Zuum Agent:

- C:\Windows\CCM\Logs*
- C:\Windows\WindowsUpdate.log
- C:\Windows\Temp\WMIRepair.log
- C:\Windows\Temp*Install.log
- C:\Windows\Logs\Software

Appendix 2 – Sample of information

SAMPLE OF INFORMATION GATHERED FROM THE DEVICES (AS IS)

{
"deviceId": "PCAGSLV00956.ONE.LOCAL",
"connectionState": "Connected",
"lastActivityTime": "2019-09-13T05:57:09.6157142",
"reported": {
"AgentVersion": "1.31.0.0",
"OSComputerName": "PCAGSLV00956",
"OSCaption": "Microsoft Windows 10 Enterprise",
"OSArchitecture": "64-bit",
"OSInstallDate": "2019-06-19T11:20:03Z",
"OSRebootDate": "2019-09-12T07:39:55.5Z",

"OSPendingReboot": false,
"OSReleaseID": "1903",
"OSUBR": "295",
"OSReliabilityIndex": 6.442,
"OSRebootCount": 8,
"AntivirusName": "McAfee Endpoint Security",
"AntivirusProtection": "On",
"AntivirusDefinitions": "Updated",
"HWManufacturer": "LENOVO",
"HWModel": "20LS0016MH",
"HWFamily": "ThinkPad L480",
"HWSerialNumber": "PF16BK01",
"Notifications": "Enabled",
"OSUpgradePending": false,
"WULastScan": "2019-09-12T09:48:24Z",
"WULastInstall": "2019-09-12T07:50:34Z",
"SCCMVersion": "5.00.8740.1042",
"SCCMService": "Running",
}
}