# **What is the Alchemy Gold Discovery Application?**

Alchemy Gold’s Discovery Application gathers data about your environment to assist you in uncovering risk, opportunities to optimize, and chances to reduce unnecessary expenditures.

# **The Data we Gather**

|  |  |
| --- | --- |
| **Network**By scanning your internal subnets, we can detect all devices on the network and store their IP addresses. ­ | **Hardware**Manufacturer and model information is recorded, as well as hardware specific details like CPU and RAM. |
| **Software**From general installed software records to database instances, we collect as much as we can without accessing personal data. | **Active Directory**By pulling user and device data from Active Directory, we can gain useful analytical insights as well as have a reference for discovery progress. |
| **Virtual Infrastructure**Collecting virtual management, host, and guest relationships is relevant in cloud readiness and server optimization activities. | **Usage and Performance**Activity metering and resource utilization are valuable in assessing your cloud readiness and uncovering optimization opportunities. |

Our application is designed to be a simple and quick method of gathering discovery data, in scenarios where a simple snapshot is required or virtual architecture is not available to deploy our flagship virtual appliance.

## **Who will have access to my data?**

During the course of this engagement, and in order to prepare your deliverable(s), our analysis and support team at Alchemy will have the ability to view the data that has been gathered, which will be destroyed after 90 days.

## **How much of my time will this take?**

## The setup of the application takes 10 minutes or less. Once the proper network scope and service accounts are input, the rest is handled by the tool – just leave it running, and let it do its thing. If you need a hand, just contact us. We’ve worked hard to make this easy!

## **Operating System and Hardware Requirements:**

* **Recommended:** Windows 10 (or Windows Server 2016), 8GB of RAM, CPU w/ 4 cores
* **Minimum:** Windows 7 (or Windows Server 2008R2), 4GB of RAM, CPU w/ 2 cores

*If possible, we recommend installing Alchemy Gold Discovery Application on a non-mission critical endpoint to avoid an unlikely scenario of interruptions or slower server response times due to increased workload.*

## **You’ll want to have on hand:**

* **Network:**All internal networks in scope; CIDR notation or single IP addresses are accepted
* **Active Directory:**A domain controller per domain in scope; IP address or FQDN formats are accepted
* **Windows Inventory:**A service account that has any two of the following 3 levels of access will accomplish inventory:
	+ Access to C$
	+ The ability to run NET RPC / Remote Registry
	+ Remote (read-only) WMI
* **Virtual Infrastructure:** Read-only administrator credentials for each vCenter Server in scope.
* **Linux Inventory:** A local or domain credential with access to files in /proc/. Superuser rights preferred for accurate data collection, but not required.
* **Office 365:** Your global administrator account, for authentication of our application to gather read-only Office 365 data such as your Secure Score, Usage and Activation data

**The Ports We Leverage**

A question we often get leading up to deployment or during troubleshooting is: *what ports will your inventory and other processes be leveraging on my network?* We have a complete list below – but some good news is that these ports are very rarely – if ever – blocked. Here is the complete list of ports we presently leverage for inventory purposes:

|  |  |
| --- | --- |
| * TCP 135, 1025-5000 and 49152-65535 (wmi)
* TCP 445 (smb v2 / v3 – remote procedure calls)
* TCP 139 & 1025 (netbios and alternate netbios)
* UDP 137 (netbios)
* TCP 389 (ldap)
* HTTP/SSL 443 (outbound data access)
* TCP 22 (SSH - Linux Inventory)
 |  |

## **Our Architecture**

Our application interacts with the on-premise and cloud assets to compile a portrait of the environment. Reporting and deliverables are prepared in Alchemy Gold’s Azure Analytics Tenant, and presented together with your assessment or solutions partner.



|  |  |  |  |
| --- | --- | --- | --- |
| **Your On-Prem & Cloud Environment(s)** |  | **Alchemy Gold’s Azure Analytics Portal** | **Reports & Deliverables via your Assessment Partner** |

**Appendix: FAQ: Regarding Access Levels & Network Impact**

**Local Administrator privileges**

* *Why do we need this?*
	+ Our inventory work leverages three Windows services: SMB, WMI and RPC.  The most time-effective way to ensure we can communicate using those services is to use a service account with local administrator privileges. If this is a concern, we can also instruct you in enabling access to these services for a specific service account.

**Domain Administrator privileges**

* *Why do we need this?*
	+ Many servers do not have local administrator accounts – for example, PDC and BDC servers. In those cases, we leverage this privilege level to conduct any inventory activities that would otherwise have leverage local admin privileges / the administrative share. However, as above, an account with Remote Registry and read-only remote WMI can successfully complete an inventory. Domain Administrative privileges are a nice to have but not a must have.

**VMware Access**

* *What access do we need?*
	+ We need an account on your vCenter server that has read-only access to the complete vSphere environment, including license manager.
	+ This account is typically an account created in a vSphere SSO domain – this can be an SSO domain administrator or a new service account created for the purpose of inventory.
* *Why do you need this data?*
	+ Microsoft and Oracle products, in particular, base their licensing in many cases on the architecture of the host upon which a guest VM is running. To properly offer licensing advice and ensure a customer is not exposed to compliance risk or overpaying for this software, we must understand the details of the guest/host relationship and the hardware specifications of the host servers.
* *Do you need root access to our ESXi hosts?*
	+ Absolutely not. The vCenter SSO account should provide sufficient data regarding your virtual environment.

**Linux Access**

* *What access do we need?*
	+ In order to inventory Linux machines, we need a local/domain user with rights to access files in the /proc/ directory. Access to dmidecode and sneep (if installed) would be ideal, but not necessary to have. While an account with superuser rights is nice to have, it is certainly not required.

**General**

* *How much of my time will this take?*
	+ Truly, very little. The setup of the application takes 10 minutes or less. Once the proper network scope and service accounts are input, the rest is handled by the tool - just leave it running, and let it do its thing. If you need a hand, just contact us at support@block64.com. We've worked hard to make this easy!
* *Who will have access to my data?*
	+ During the course of this engagement, and in order to prepare your deliverable(s), our analysis and support team at Alchemy Gold and/or at the partner you are collaborating with will have the ability to view the data that has been gathered, which will be destroyed after 90 days.

**Network Impact**

* *What will the impact to my network be?*
	+ We leverage standard protocols (NetRPC, SMBv2 & v3, etc) that should not cause any alert conditions in a standard environment
	+ The amount of bandwidth our solution consumes is configurable at the appliance level, or even via your virtualization technology itself.
	+ In its default settings, our appliance will typically run at 150 - 250KBp/s, comparable in bandwidth to streaming a standard definition video on YouTube.
	+ In its maximum settings, our appliance will typically run at up to 1000 KBp/s, comparable in bandwidth to streaming a high definition video on YouTube.
* *Do I need to take any special care with my endpoint protection, antivirus or intrusion detection systems?*
	+ As an agentless solution, it is possible, though exceedingly unlikely, that our inventory activities will be detected by IPS or IDS solutions. In these cases, most security solutions offer the ability to allow a solution such as ours to be whitelisted and traverse your network without raising any unnecessary red flags. That said, our traffic largely goes unnoticed by most systems of this type.