Source of Truth Computer Information

FFP Software

V1.0

November 2023

Product Overview

Contents

Introduction

The Source of Truth (SoT) Computer Information System is a simple, yet powerful and importantly, agentless inventory system, designed by Systems Administrators and Engineers to provide the information about every machine in the environment that is pertinent to those that need it. It gives the ability to query the environment directly and a single, sensible way to collect and show the results.

It is because it is agentless and that it is deployed via Group Policy that SoT will record data from 100% of the online environment, where other systems that rely on an agent will not achieve that level of accuracy; agents can fail, not be installed or have missing prerequisites that will cause less than 100% coverage.

As the client script queries the machine directly, then reports that information directly to the SoT database, data is more accurate than in other systems which may use for example, installation records, or have out of date information caused by the failure of the agent. This means that the data in many other inventory and management systems can never be 100% reliable. SoT was designed to provide that certainty.

It is highly versatile and customisable, able to report on any aspect of any Microsoft Windows computer that is accessible by PowerShell. To this end, it can find and report on any element from WMI, the Windows Registry, File System or process for example. The client script can be added to, and additional columns added to the database to collect any data you may need to know about your environment. The limits of how many aspects of each from each machine is only limited by the limits of what an SQL server can hold, what one can envisage and the coding abilities of those operating it.

A client PowerShell script is deployed to the target machines via group policy, with the results sent to an SQL database. Code can very simply be added to the master script on the Sysvol share and the clients automatically update their version to the latest central script. This means that every online machine will report results to the database within one Group Policy refresh cycle.

If it is online, Source of Truth will report it with no additional client configuration, and it is because of what has been outlined above that makes Source of Truth unique on the market.

Use Cases

The Source of Truth (SoT) Computer Information System can be used to gather any information imaginable from your environment, simply and quickly.

Examples of use cases are:

1. Microsoft releases a security bulletin stating that a vulnerability has been seen in the wild that exploits code in an Edge DLL. It is *critical* to update this DLL as soon as possible, so a central WSUS or SCCM update and push is created and deployed. To ensure accurate reporting of *ALL* machines, and to identify any remaining machines, a column is added to the database called “MSKBxxxxxDLLVersion” and a simple Get-Item routine is added to the

master script to get the DLL's version. Within one GPO refresh cycle, all online machines report the version of the DLL and any gaps in the update deployment are identified and manually remediated.

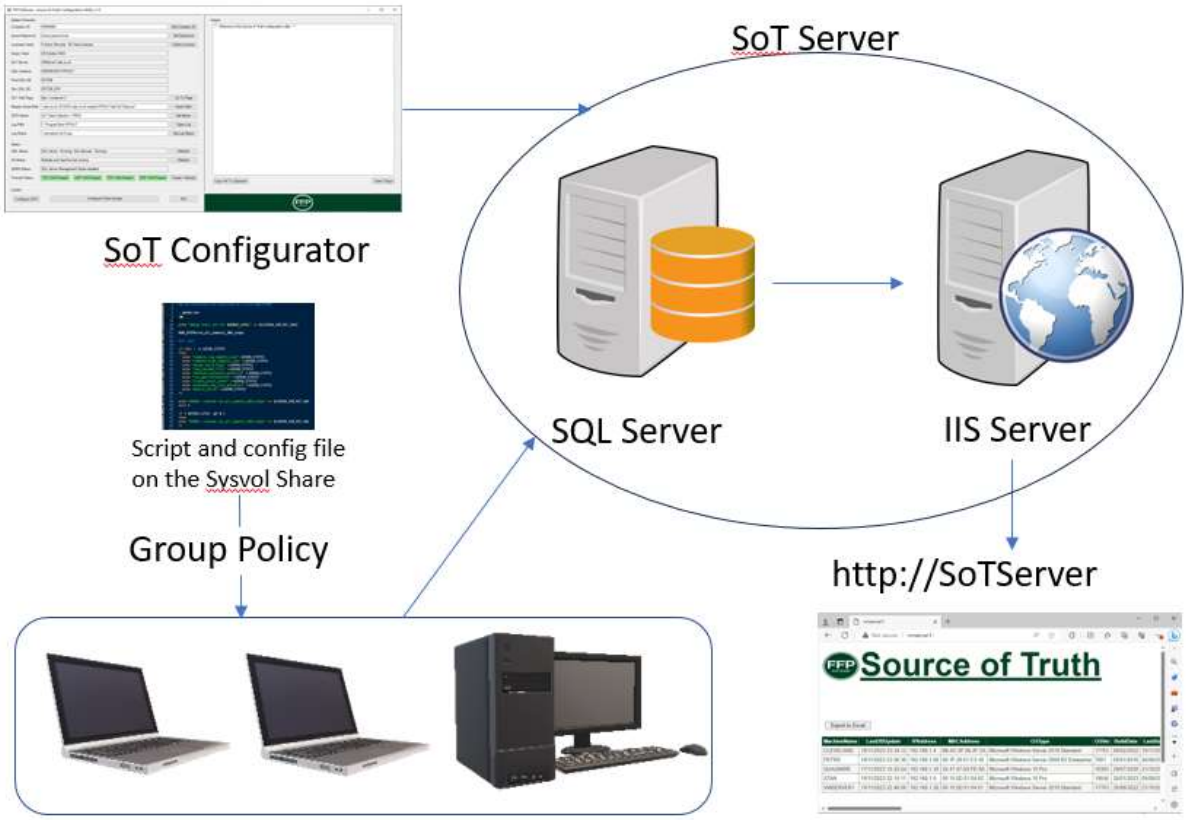
2. IT Security notice that machines are starting to be seen as offline in the online management portal of a security suite used. Source of Truth shows that these "offline" machines are still online. Manual investigation shows that for some reason, files belonging to the software are missing, and a chance finding shows that some machines do not have it installed.
    a. Code is added to SoT to get the following information:
        i. Installation status (Installed: True/False)
        ii. Version installed
        iii. Date installed
        iv. Dll file count
        v. Exe File count
        vi. Service running (Running True/False)
        vii. Logs Present (True/False)
    b. From these results, we can see which machines need to be targeted for reinstallation and which were missed from the original deployment and which can be used for root cause analysis with the vendor.
3. With a list of IP Subnets and the locations that they are in, an XML file can be created, placed along side the script in the sysvol and added to the GPO to be pushed along with the script. Taking the IP Address that the script already gets, code can be added to map the IP Address to subnet/location and from that the current location of a machine can be ascertained and reported in it's own database column.

These are just a few of the use cases for Source of Truth, but the possibilities are only limited by what the mind can imagine.

Components

The diagram below illustrates the components of The Source of Truth Computer Information System. This comprises of:

- A Configuration Utility
- A Powershell script and .config file
- A Group Policy
- An SQL Server
- An IIS Server



A Powershell script and config file is places on the Sysvol share where it is deployed by Group Policy which copies the files to a local folder on the end device. The script runs, updates the SQL server and displayed on a web page, served by the IIS server.

How it works

The Powershell script and config file is placed on the Sysvol share and deployed by GPO.

The GPO creates a folder on the end user machine in C:\Program Files, into which the script and config files are copied.

When it applies, the GPO can either create an immediate scheduled task which will run the script at every GPO update, or it can schedule it for however often is desired.

The script does have an auto-update mechanism, so if this is scheduled for every X hours/days on the client, then if there is an update to the script, the client will pick it up before executing it.

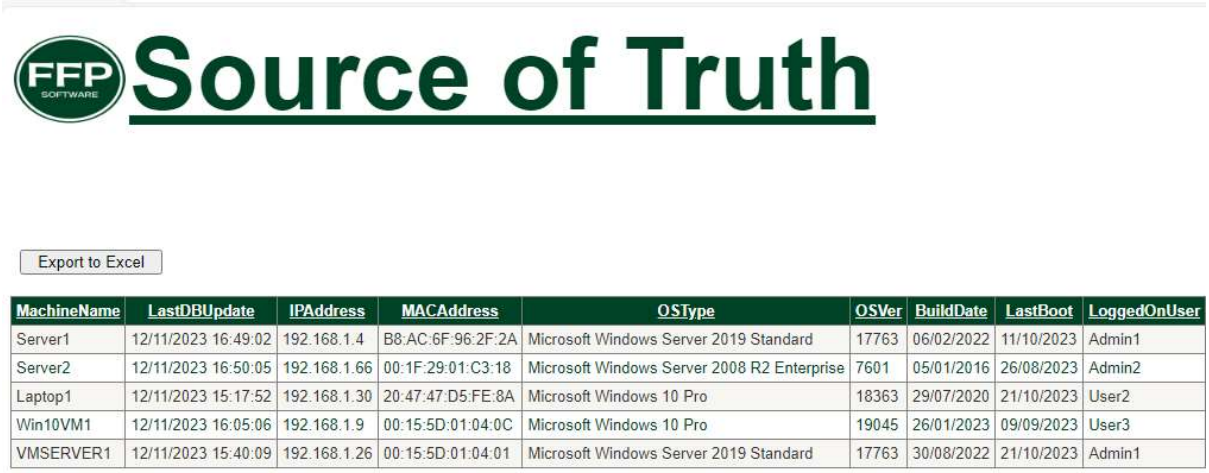
The client script writes logs to a folder in C:\ProgramData for troubleshooting any code that has been added and is not working as expected. Only up to 11 logs of around 8kb are kept.

The next action is to check if there is an updated config file or script on the Sysvol share. If there is, it will replace the existing file(s) and re-execute, meaning that both the script and config files are self-updating.

When the script has run and collected all the data, it will connect to the SQL server and either create a new record if one does not exist, or update the existing record with new data.

The IIS server hosts a simple .aspx page that displays the MainDetails table (where all the data is stored) as a web page in table format. This can be exported to Excel (.xlsx format) with one button on the web page.

An example of what the output looks like on the web page can be seen below: (additional columns cropped from the screenshot)



MachineName	LastDBUpdate	IPAddress	MACAddress	OSType	OSVer	BuildDate	LastBoot	LoggedOnUser
Server1	12/11/2023 16:49:02	192.168.1.4	B8:AC:6F:96:2F:2A	Microsoft Windows Server 2019 Standard	17763	06/02/2022	11/10/2023	Admin1
Server2	12/11/2023 16:50:05	192.168.1.66	00:1F:29:01:C3:18	Microsoft Windows Server 2008 R2 Enterprise	7601	05/01/2016	26/08/2023	Admin2
Laptop1	12/11/2023 15:17:52	192.168.1.30	20:47:47:D5:FE:8A	Microsoft Windows 10 Pro	18363	29/07/2020	21/10/2023	User2
Win10VM1	12/11/2023 16:05:06	192.168.1.9	00:15:5D:01:04:0C	Microsoft Windows 10 Pro	19045	26/01/2023	09/09/2023	User3
VMSERVER1	12/11/2023 15:40:09	192.168.1.26	00:15:5D:01:04:01	Microsoft Windows Server 2019 Standard	17763	30/08/2022	21/10/2023	Admin1

You can see that this is listed by machine name and shows some basic, default details that would be pertinent to most engineers, administrators and support personnel, with the LastDBUpdate column being the last time the machine checked in, hence the last time seen on the domain.

Minimum Requirements and Prerequisites

Source of Truth requires the following requirements and prerequisites to be met for installation and operation:

Server:

- Windows Server 2016 or later (physical or virtual)
- 16GB RAM (64GB or greater recommended)
- 10GB free disk space at a minimum. This requirement will grow with large client bases.
- Dual core processor (4 cores or greater recommended)
- Powershell enabled in Full Language mode.
- Windows Firewall ports TCP/UDP 1433,1434 opened (for SQL Database)
- HTTP Port 80 for the IIS web page
    - If this is set by GPO at an organisational level, these will need to be excluded from the SoT server.
    - The SoT Configurator will open the SQL ports and the IIS installation opens the HTTP port.
- If Applocker is enabled, then scripts from C:\Program Files\FFPSoT allowed.

Clients:

- Windows 7 or later with Powershell 3.0 or higher
    - Whilst the client script *MAY* work on Windows XP or Vista, these operating systems *MUST* have at least Powershell 3.0 installed, but even then, this has not been tested and is not warranted.
- No particular RAM, CPU or Disk requirements.
- Line-of-Sight to the Domain Controllers and SoT DB Server.

Customisations

This is where the extensible nature of this system really comes into its own; the ability to add Powershell code to the script to produce additional data to report.

As this is added to the master script on the Sysvol share, due to the self-updating nature of the files and how it is deployed via GPO, at its fastest, it can have every machine in the environment update its records within the hour, depending on GPO frequency.

To add customisations to the system, there are several steps necessary.

For this example, reporting on a software version is used; Microsoft Silverlight (in case a vulnerability has been found in a certain version of a software product and that version needs to be reported quickly)

1. Add code to the script. The key part is to ensure that the result is stored in a variable. This variable will be used in the SQL Insert/Update statement to push into the database.

```
$SilverLightValue = Get-ItemProperty -Path HKLM:SOFTWARE\Microsoft\Silverlight -Name Version

if ($SilverLightValue -ne $Null)
    {
        $SilverLightVersion = $($SilverlightValue.Version)
        Write-Log -Message "SilverLight Version: $SilverLightVersion"
    }
Else{
        $SilverLightVersion = "Not Installed"
        Write-Log -Message "SilverLight Version: $SilverLightVersion"
    }
```

2. Add the $SilverlightVersion variable to the SQL Insert command. This just needs to be placed at the end of the string command.
   Note: It is advisable to leave the Get-SoTData script version as the last column. This can be very helpful for seeing which machines have updated since the last change was made.

3. Add the column SilverLightVersion to the end of the SQL dbo.MainDetails table, before the VERSION column.

4. Repeat this process for each new item of data that needs to be collected.

Operation and Usage

Once Source of Truth has been installed, configured and the Group Policies deployed, it will, to a large extent run itself and work quietly in the background, collecting the data from your environment.

Extracting Data:

In order to view the data held by Source of Truth, you will need to open a browser from within your environment and enter HTTP://%SoTServerName% (Where %SoTServerName% is the name of the server where SoT is installed). This will bring you to the Source Of Truth web page for your environment.

Export to Excel

MachineName	LastDBUpdate	IPAddress	MACAddress	OSType	OSVer	BuildDate	LastBoot	LoggedOnUser
Server1	12/11/2023 16:49:02	192.168.1.4	B8:AC:6F:96:2F:2A	Microsoft Windows Server 2019 Standard	17763	06/02/2022	11/10/2023	Admin1
Server2	12/11/2023 16:50:05	192.168.1.66	00:1F:29:01:C3:18	Microsoft Windows Server 2008 R2 Enterprise	7601	05/01/2016	26/08/2023	Admin2
Laptop1	12/11/2023 15:17:52	192.168.1.30	20:47:47:D5:FE:8A	Microsoft Windows 10 Pro	18363	29/07/2020	21/10/2023	User2
Win10VM1	12/11/2023 16:05:06	192.168.1.9	00:15:5D:01:04:0C	Microsoft Windows 10 Pro	19045	26/01/2023	09/09/2023	User3
VMSERVER1	12/11/2023 15:40:09	192.168.1.26	00:15:5D:01:04:01	Microsoft Windows Server 2019 Standard	17763	30/08/2022	21/10/2023	Admin1

Click the Export to Excel button and this exports the grid on the web page to an xlsx file for use in Excel.

To access the Dev data, enter HTTP://%SoTServerName%/Default-Dev.aspx . This will bring back the data from the Dev database:

Export to Excel

MachineName	LastDBUpdate	IPAddress	MACAddress	OSVer	BuildDate	LastBoot	LoggedOnUser	LastLoggedOnUser	LastLoggedOnDate
Laptop1	22/10/2023 13:15:52	192.168.1.30	20:47:47:D5:FE:8A	18363	29/07/2020	21/10/2023	User1	User1	21/10/2023
Win10VM1	22/10/2023 13:15:07	192.168.1.9	00:15:5D:01:04:0C	19045	26/01/2023	09/09/2023	User2	Admin1	20/10/2023
VMSERVER1	22/10/2023 13:25:18	192.168.1.26	00:15:5D:01:04:01	17763	30/08/2022	21/10/2023	Admin1	.NET v4.5	21/10/2023

The data is exported to Excel in the same manner.

Explanation of the columns:

Source of Truth comes with a number of default columns as listed below with a brief description of each.

- MachineName: The computername of the machine to which the record pertains.
- LastDBUpdate: The last time the machine updated the database, ergo the last time the machine was online.
- IPAddress: The current IP address of the machine.
- MACAddress The MAC address of the connected network adapter.
- OSType: The type of operating system, i.e Windows 10, Windows 11, etc.
- OSVer: The build version of the operating system.
- BuildDate: The date the operating system was installed.
- LastBoot: The last time and date the computer was booted.
- LoggedOnUser The currently logged on user.
- LastLoggedOnUser The user who logged on previously to the currently logged on user.
- LastLoggedOnDate The date the currently logged on user logged on.
- Manufacturer The manufacturer of the machine.
- Model The model of the machine.
- SerialNumber The serial number of the machine.
- ProcessorModel The processor type.
- ProcessorCores The number of cores in the processor.
- ProcessorCurrentSpeed The current speed (in MHz) of this processor.
- ProcessorMaxSpeed The maximum speed (in MHz) of this processor.
- BIOSVersion The current BIOS version.
- FirmwareVersion The SMBIOS Version.
- TotalMemory Total RAM installed (In GB).
- FreePhysicalMemory Free physical memory (in MB).
- HDDSize HDD total size (in GB).
- HDDFreeSpace HDD free space (in GB).
- BitlockerProtectionStatus Whether Bitlocker protection is On or Off.
- BitlockerVolumeStatus What the current status of encryption is on the protected drive.
- BitlockerPercentEncrypted What the percentage of the drive is currently encrypted.
- Version The latest version of the SoT Client script that has been run. Used when validating which machines have run the latest version after an update. Recommended to leave this column on the far right hand side.

Licensing

Source of Truth is licensed on a per-machine basis. When an expression of interest is received by FFP Software, an account is created in the FFP tenant in Azure and a unique account number is issued. This account number is used by the SoT update mechanism on the local SoT server to contact the FFP licensing system and retrieve the customer licensing record.

The number of records in the local SoT database is compared to the number of licenses purchased. If the local database has more records than the number of licenses purchased, then the database will stop accepting connections and data updates from the endpoint machines. The SoT web page on the SoT server will also change to red and have (UNLICENSED) after the title. Likewise, if the subscription date lapses, the same occurs.

In the event of license numbers being exceeded or the subscription lapsing, contact FFP Software to purchase more licenses or extend the subscription.

The licensing mechanism on the local SoT server reaches out to the FFP licensing system multiple times per day (the data involved is only several KB) to ensure license compliance. This is logged to a folder in C:\ProgramData and a maximum of 100 logs are kept.

Updates

Updates to the SoT files are automatically and seamlessly pushed from the FFP tenant in the cloud. This is run once per day and a log file is written (maximum of 10 logs are kept). Nothing in these updates will affect anything that has been configured or set by the customer. This is logged to C:\ProgramData\FFPSoT and a maximum of 100 logs are kept

Contacts

General Information:	Info@ffpsoftware.com
Sales:	sales@ffpsoftware.com
Support:	support@ffpsoftware.com