

trakPC/scanPC

TrakPC and ScanPC are executable files that audit Windows-based PCs and return the discovered data to Issuetrak as an XML file to be processed into a new or updated asset.

glossary

- **Audit** – Snapshot created by TrakPC detailing information about a Windows-based PC. Audits may include updates to existing assets or new machines that need to be created as assets in Issuetrak.
- **Login Script** – A script file containing a series of instructions that a computer follows when a user logs on. Login scripts can be administered locally through Active Directory or a Group Policy.
- **PC Asset** – The record of a Windows-based PC in Issuetrak's Asset Management module. PC Assets can be associated to a specific user within your Issuetrak system; can contain purchase or lease information; can be linked to other assets in a parent/child relationship; and show hardware and software information captured during an audit.
- **ScanPC** – Allows on demand audits of a target computer within Issuetrak from the Home menu. Captures the same details as the TrakPC.exe program.
- **TrakPC.exe** – Executable program launched to capture details about the target PC. It may be executed on a local machine, a shared network drive, or via a login script.

gathering information with trakPC

The TrakPC.exe executable scans a PC and creates an XML file to send the information back to Issuetrak. There are several options for deploying TrakPC.exe. The three most common options are:

- **Active Directory Login Script** – This method sets the login script as a domain default in Active Directory. It executes the script parameters for TrakPC.exe from a network share and completes the audit. In this case the script can be centrally managed and enforced across a domain through Active Directory.
- **Local Batch File or Login Script** – TrakPC.exe can also be deployed either through a login script or a batch file executed locally by a Windows Scheduled Task. This usually calls TrakPC.exe from a network share to execute the audit. This option allows you to execute the login script on an individual schedule.
- **ScanPC** – An on-demand deployment designed to run on the local machine when a user selects the ScanPC menu option within Issuetrak. This could be used when a machine is first



set up on the network or when a tech needs current information on the machine. ScanPC downloads a local copy of the TrakPC.exe file and executes the audit.

creating a login script

When you need to create a login script to execute TrakPC.exe, it must contain parameters that tell TrakPC.exe where to send the audits it creates. The example script uses the "/u" parameter to tell TrakPC.exe to send the file to the website "<http://hdtraining.issuetrak.com>" and process to the web page "Inv_TrakPC_URLSubmit.asp," which then turns the audit file into a record within the Asset Management module.

```

logon script.bat - Notepad
File Edit Format View Help
echo off
net use M: \\file14\PUBLIC\ProServices\Documents
\\file1\trakpc\Trakpc.exe /u"http://hdtraining.issuetrak.com/Inv_TrakPC_URLSubmit.asp"
    
```

KB article 69 within the Issuetrak Support site includes more information about parameters, proper syntax, and assistance with creating login scripts:

https://support.issuetrak.com/Kb_ArticleView.asp?ArticleNbr=69.

Once a login script is created, it can either be copied to the machines that you want audited, or use Active Directory to set up the login script as a domain default. For the domain default option, the login file will need to be saved to a shared location and provide the .bat name for Active Directory to pull it from NetLogon. NetLogon is a common location all users can reach, and most logon scripts end up here. If you use a network share, ensure all users have rights to access that location.



In this example, the login script is accessed from a shared location named "File14\public." Each time the user logs into a computer on the domain, the login script will call TrakPC.exe from the network share.

creating audits

When TrakPC.exe is executed, it scans the hardware and software on a computer and saves that scanned information as an XML file in the current user's temp folder (App Data\Local\Temp) or another location you specify. This XML file can automatically be sent back to Issuetrak, or it can be retrieved and manually uploaded later.

Once Issuetrak receives the XML file, it creates an audit record that contains the scanned information about the PC. The Audit contains hardware details like the number of drives, IP and MAC addresses, and software information such as currently running processes and installed software titles.

next steps

An example audit appears on the next page. Audits are not associated with a PC Asset until after they have been applied within Issuetrak. Many features of the Asset Management module have additional documentation available. Check them out or contact us at proservices@issuetrak.com with any questions.



Audit Item #: 196
 Audit Date: 06/08/2015 10:42AM
 Login Name:
 Audit Applied:

System Information

Manufacturer: Dell Inc.
 Model: Latitude E6400
 Service Tag: 6GJ
 Serial Nbr: 6GJY
 Computer Name: 6GJY
 Computer Desc.:
 Registered Owner: admin
 Registered Org:

OS: Windows 7 Professional Build:6.1.7601 SP:Service Pack 1
 Browser: Google Chrome Vers:
 Mail Client: Microsoft Outlook Vers:12.0.6691.5000
 Mail Path: C:\PROGRA~2\MICROS~1\Office12\OUTLOOK.EXE

Hardware Information

Memory: 8144
 Nbr of Processors: 1
 Processor Vendor: GenuineIntel
 Processor Type: Intel(R) Core(TM)2 Duo CPU P8600 @ 2.40GHz ()
 Processor Mhz: 2376
 Processor Max Mhz: 2401
 Bios Vendor: Dell Inc.
 Bios Version: A14
 Bios Date: 05/11/2009

Motherbrd Manuf: Dell Inc.
 Motherbrd Name: OW620R
 Motherbrd Version:
 Motherbrd Serial: .6GJY .CN129619

Enclosure Vendor: Dell Inc.
 Enclosure Serial: 6GJY
 Enclosure Tag: System Enclosure 0
 Enclosure Type: Laptop

Display Name: @oem6.inf,%icntg0%;Mobile Intel(R) 4 Series Express
 Display Vendor: @oem6.inf,%intel%;Intel Corporation
 Display Driver: Intel Corporation
 Display Version: 8.15.10.2302

Nbr of NICs: 2
 Match MAC Addr:
 IP Address (1):
 MAC Address (1):
 Description (1): VirtualBox Host-Only Ethernet Adapter
 NIC Name (1): {1811CBEO-930B-43E5-9BAF-221D2
 IP Address (2):
 MAC Address (2):
 Description (2): Intel(R) 82567LM Gigabit Network Connection
 NIC Name (2): {53D61BBF-8D2A-4905-828D-5A0FE27

Letter	Type	Size MB	FreeMB
C	Fixed	152525.0	64361.0
D	CD-ROM/DVD-ROM		
E	CD-ROM/DVD-ROM		
S	Remote		
U	Remote		

Name
7-Zip 9.20 (x64 edition)
Size: Installed Date: 01/22/2013
Adobe AIR
Size: Adobe Flash Player 17 ActiveX
Size: Adobe Reader XI (11.0.11)
Size: Installed Date: 05/13/2015
Adobe Shockwave Player 12.1
Size: AutoHotkey 1.0.48.05
Size: AutoHotkey 1.1.09.02

Exe	Priority
[System Process]	0
AESTSr64.exe	0
ALMon.exe	32
ALsvc.exe	0
AutoHotkey.exe	32

