working with audits

TrakPC serves as an auditing tool for computers operating on Microsoft Windows. For background information about TrakPC and how it works, please reference the other documents related to Asset Management. This document focuses on working with the audits created by TrakPC.

glossary

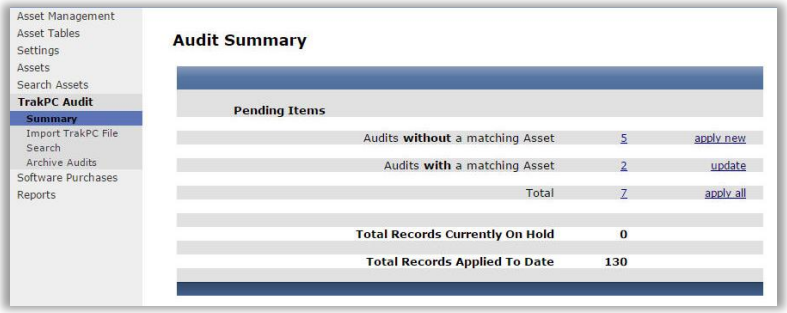
- **Audit** – Snapshot created by TrakPC detailing information about a Windows-based PC. Audits may include updates to existing assets or new machines that need to be created as assets in Issuetrak.
- **PC Asset** – A Windows-based computer record in Issuetrak. PC Assets have specific fields containing information valid to PC records only collected during a ScanPC/TrakPC audit.
- **TrakPC.exe** – Executable program launched to capture details about the target PC. It may be accessed on a local machine, a shared network drive, login script, or group policy.

audits versus assets

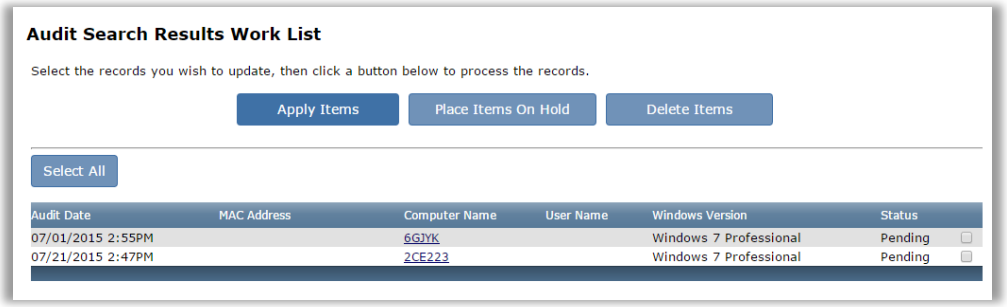
Deploying TrakPC in your environment will create an audit record of each Windows-based computer on your network each time it runs. Over time, computers will build up multiple audit records. Those records can be used to compare an asset at different times during its life cycle, which may be beneficial for troubleshooting. Audit files can be manually or automatically applied to create or update assets.

manually applying audits

Audits that haven't been applied can be viewed here: Modules > Asset Management > TrakPC Audit. There are two types of audits shown: those with a matching asset and those without.



Clicking on the number next to each type of audit will give you a work list.



Audit details are visible by clicking on the computer name. You can then apply, delete, or hold each audit by selecting the status checkbox and select the appropriate option at the top of the page.

Deleting an audit removes it from the system, which is useful if several audits were created during testing or troubleshooting. Placing an audit on hold allows you to keep it for review and apply or delete it at a later time.

When the audit is applied, existing asset records are updated with any new information contained in the audit. Audits without a matching asset record create new assets. The audits are then stored as a historical record with the asset.

automatically applying audits

If you are creating audits across a large network or if they occur frequently, you may want to set up an automated process to apply the audits through a SQL server job. Once set up, the SQL job will apply your updates and create newly discovered audit records at intervals you determine. Premise customers can configure this themselves by following the directions in Knowledge Base Article #1552 on our support site: https://support.issuetrak.com/Kb_ArticleView.asp?ArticleNbr=1552. Cloud-based customers can request automatic audit application from the Support Team at no additional charge.

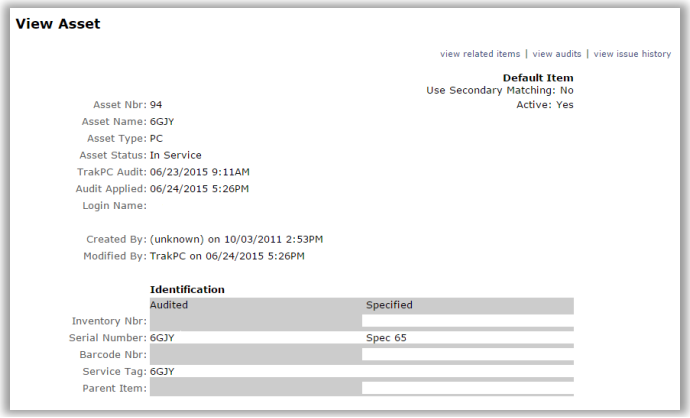
matching audits to existing assets

An audit matches an existing PC Asset if at least four primary values match. The primary values are: serial number, motherboard serial number, MAC address, computer name, bios version, and service tag. If fewer than four values match, then a new asset is created.

There is an option to allow PC Assets to use a secondary matching value of either MAC address or computer name. Secondary matching is selected on an asset by asset basis and may be useful when upgrading hardware or changing primary matching criteria on an existing machine.

after an audit is applied

Once an Audit is applied, it becomes part of the asset record. This PC Asset has multiple audits associated to it.



View Asset

view related items | view audits | view issue history

Default Item
Use Secondary Matching: No
Active: Yes

Asset Nbr: 94
Asset Name: 6GJY
Asset Type: PC
Asset Status: In Service
TrakPC Audit: 06/23/2015 9:11AM
Audit Applied: 06/24/2015 5:26PM
Login Name:

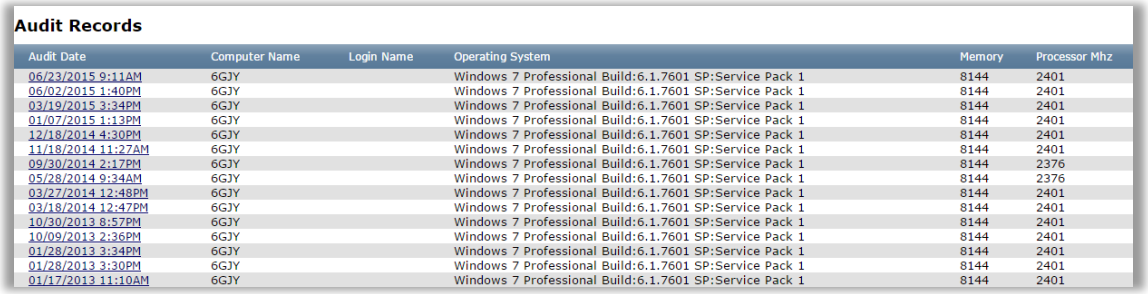
Created By: (unknown) on 10/03/2011 2:53PM
Modified By: TrakPC on 06/24/2015 5:26PM

Identification

	Audited	Specified
Inventory Nbr:		
Serial Number:	6GJY	Spec 65
Barcode Nbr:		
Service Tag:	6GJY	
Parent Item:		

The “Audit Applied” date says when the last audit was applied, and the “TrakPC Audit” date says when that audit was created. To view multiple audits that have been applied, click the “View Audits” hyperlink.

This asset has audits going back to 2013.



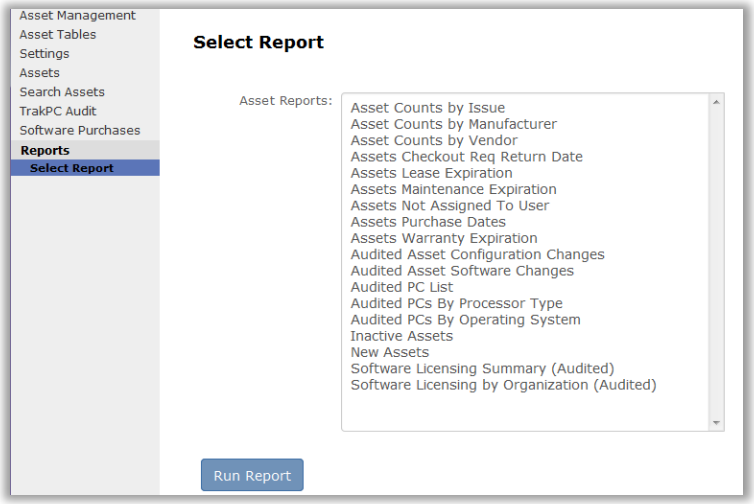
Audit Records

Audit Date	Computer Name	Login Name	Operating System	Memory	Processor Mhz
06/23/2015 9:11AM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
06/02/2015 1:40PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
03/19/2015 3:34PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
01/07/2015 1:13PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
12/18/2014 4:30PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
11/18/2014 11:27AM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
09/30/2014 2:17PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2376
05/28/2014 9:34AM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2376
03/27/2014 12:48PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
03/18/2014 12:47PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
10/30/2013 8:57PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
10/09/2013 2:36PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
01/28/2013 3:34PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
01/28/2013 3:30PM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401
01/17/2013 11:10AM	6GJY		Windows 7 Professional Build:6.1.7601 SP:Service Pack 1	8144	2401

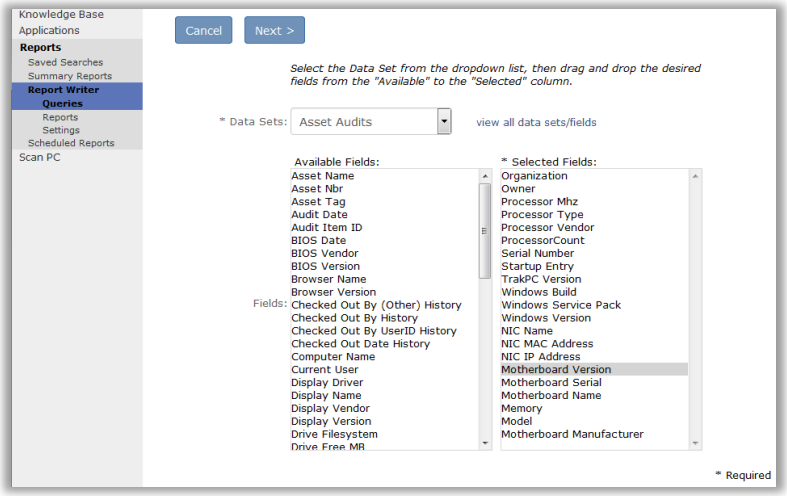
Viewing or reporting on these audits lets you see the hardware and software changes that have been made to this asset over time.

reporting on audits

There are several ways to report on Audits. The Asset Management Module comes with built in reports that show audited information such as “Audited Configuration Changes” and “Audited PC List.”



You can also use the “Asset Audits” dataset in the Report Writer to create queries and reports specific to audits.



next steps

Audit history takes up valuable storage space, so do archive audits that are no longer useful. Archiving an audit removes it from the system, freeing up space and allowing audit-based reports to run faster.

Many features of the Asset Management module such as Software Purchases, working with Audits and the TrakPC/ScanPC application have additional documentation available. Check them out or contact us at proservices@issuetrak.com with any questions.