SiteAudit Technical Article

SiteAudit OnSite v7 Security

In This Article:

June 2020

SiteAudit Overview

SiteAudit OnSite is an MPS application for collecting local and networked printer data. It employs a data collection agent and a viewer(s) that runs at the customer site. Data is collected at the customer site and sent to a Microsoft SQL database. It provides a secure and easy way for MPS providers to collect and manage counts, supplies, errors and printer information.

The following diagram represents SiteAudit OnSite and its various components

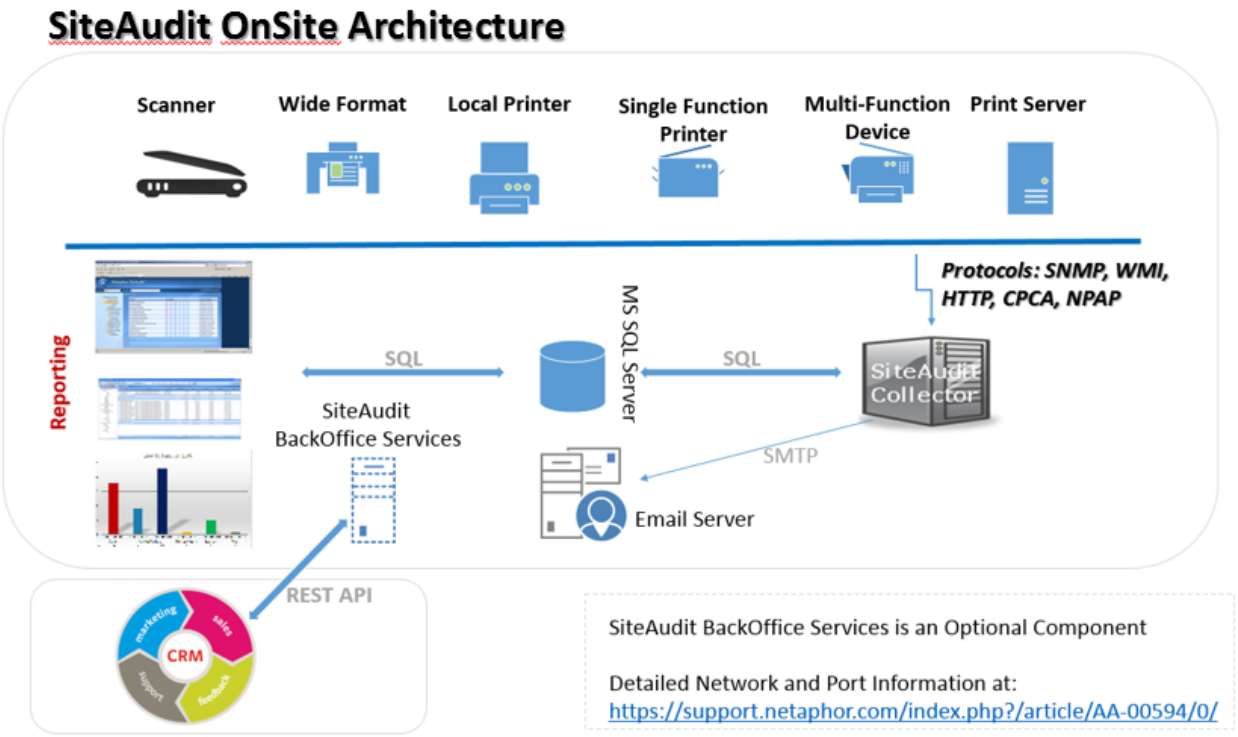
Components

SiteAudit consists of the following major components:

SiteAudit Viewer –The SiteAudit Viewer is used to view, edit, and customize reports

SiteAudit Monitor – The Microsoft Windows service that performs printer discovery, collects usage data, and stores the data in a database

SiteAudit Reporting Website – Installed web site provides access to reports



Discovery and Data Collection

SiteAudit performs a discovery using SNMP. The discovery allows both inclusion and exclusion of IP addresses. Discovery over SNMP v1/v2c and SNMPv3 with SA V6.4 or later

- each included network, range, static IP on the list determines the addresses in that list
- each excluded network, range, static IP determine if any of these addresses are excluded

The discovery process works as follows:

1. SiteAudit performs broadcasts to find devices and routers if a broadcast address is explicitly included as one of the discovery addresses.

SiteAudit scans the following ports to find printers:

- 161 SNMP to see if SNMP is enabled.
- SNMP is used to collect data
- 80 & 8080 HTTP to see if there is an embedded web server. HTTP is used to collect data
- 9100 Print protocol for printers, used to collect data
- 1650 Same as 9100
- 631 IPP print protocol, used to collect data.
- 135 RPC, used to detect a Windows host for local printers
- 47545 (CPCA) and 9300 (NPAP) may also be used if the printer supports those protocols
- Ports 21 (FTP) and 23 (Telnet) to identify potential security vulnerability

To minimize network traffic, data is collected by type and in configurable intervals. Read more about discovery and data collection at https://support.netaphor.com/index.php?/article/AA-00594
Read about DNS discovery https://support.netaphor.com/index.php?/article/AA-00391/0/

Encryption and Authentication Compliance

SiteAudit implementation of SNMP v3 is compliant with the following:

- SHA-1 and SHA-256, SHA-384, SHA-512
- MD5
- DES
- AES-128

Compliance with:

- FIPS 140-2
- TLSv1.2

Direct Connect (Local) Printer & Windows Firewall

SiteAudit finds printers directly connected (via USB or parallel connections) to Windows hosts. SiteAudit requires the credentials of a user who is an administrator on the host machine. To make sure that discovery succeeds:

Provide a credential that works on all Windows host machines

Ensure that these credentials do NOT get locked out after several failed attempts

Direct Connect (Local) Printer & Windows Firewall - continued

Run the Diagnostics > Unauthenticated Hosts report to identify Windows hosts that did not allow access and add the credentials for that host.

If Windows Firewall is enabled, it must be configured to allow SiteAudit access to the remote Windows hosts for locally connected printers. The Windows Firewall on Host machines must allow corresponding packets in and responses out. Enabling “Remote Monitoring” enables all the firewall accesses that SiteAudit needs on a remote host.

Credentials

SiteAudit requires credentials in the following instances:

- Installation of SiteAudit on a server or workstation requires a local account running as a service
- Installation of the SQL Server or SQL Server Express database requires a system administrator (sa) password or, if integrated security is used, login credentials of an individual who has administrator-level access to the database
- For directly connected printer discovery, Windows administrator credentials for the hosts with attached printers.
- Direct printer discovery using WMI requires an account that has full permissions for the ROOT WMI namespace.
- For SNMPv3 discovery

Note: SiteAudit stores all passwords in Windows Protected Storage and can only be decrypted on the machine where they were entered. If the DCA is moved to a new machine, these passwords must be reentered on this machine.

Access Security

- Users are granted access to SiteAudit data stored in a MS SQL Server DB using their Windows accounts or via a MS SQL Server account.
- Netaphor SiteAudit SiteAudit functional security is optional and is designed to control access to various SiteAudit functions. Control is maintained by assigning users to roles much like a Windows administrator assigns users to roles to permit or deny capabilities on a Windows machine. SiteAudit roles are defined and are defined and maintained within the SQL Server database used by SiteAudit.
- Users are authenticated using the mechanism used to login. Active Directory Account is used with Integrated security and a username/password is used with a SQL account
- No separate access control is maintained by the application. Access is either via Active Directory or SQL Server Accounts.
- User identifications are not used outside the customer network.

Network Traffic

SiteAudit data collection can be characterized as a *slow, steady receipt of packets*. This results in a smaller percent of the network bandwidth being used. Network traffic is dependent on the number of devices that SiteAudit is monitoring. Below are examples of network traffic utilization for three different fleet sizes: 250, 1,000 and 10,000 printers.

Traffic estimates are based on a typical environment, but results may vary depending on mix of local and networked printers, number of counters, address spacing, number of IP addresses and other factors.

Number of Printers	% Usage in 100 MB Network	% Usage in GB Network
250	0.003	0.000293
1000	0.001	0.000977
10000	0.103	0.010058594

Read more about network traffic at https://support.netaphor.com/index.php?/article/AA-00594

SNMP Access

The SNMP protocol includes a provision for access control using “community” strings. A community string is required to access a device. SiteAudit maintains a list of community strings used to communicate with devices.

This “community” list is ordered, and SiteAudit tries each string in turn until one succeeds or there are no more strings to try. The list is pre-seeded with the default “public” community string and a user can edit this list and change the order in which community strings are tried.

Some SNMP agents within a device may be configured to generate “authentication failure” traps when a community string is used that is not valid for that device. To avoid getting these authentication failure traps:

- Ensure that the list of community strings contains only those that are needed
- Ignore the authentication failure traps if they indicate that the source of the request (the application sending the message with the invalid community string) is SiteAudit
- Disable the authentication failure traps on the device

Data Collected

Data collected consists of printer asset information, counters, supplies and error information. A sample of the collected data is listed below.

Asset Information	**Supplies**	**Counters**
Manufacturer	Supplies Remaining Level %	Total Pages
Model	Original Supply Level	B/W All
IP Address	Percentage of Supplies Used	B/W Print
Printer Name	Date Toner Detected	B/W Copy
Product Number	Replaced On Date	B/W Large
Serial Number	Supplies Description	Color All
Asset Tag	Supplies Type	Color Print
Location	Supplies Part Number	Color Copy
Printer MAC Address	Supplies Serial Number	Color Large
Host MAC Address	Supplies Installation Date	Large
		Small
Errors	**Errors (continued)**	Copied
Alert Code	Service Level Agreement Name	Print
Severity Level	Contact	Fax
Training Level	Total Errors	Scanned
State	Uptime %	
Resolution Status	Last Successful Communication	
Incident Description	Last Notified	
Incident Duration	Device Status (Ready/Error/Warning)	
Incident Start & End	Response Time	

There is no credit card or personal data stored. Job data may be collected if SiteAudit is configured to collect this information. By default, this feature is disabled. Local administrator credentials with access to the target workstations is required to configure this feature. For a complete list of data see https://support.netaphor.com/index.php?/article/AA-00779/104/

Common Questions about Data Collection

- Device Data Collection: Only device data is collected. Information, such as user accounts on the device for Follow Me Printing or secure print or the list of jobs on devices, is not collected
- No Personally Identifiable Information (PII) such as user passwords, credit card information, SSN etc. are collected or stored by SiteAudit
- Job Data collection is optional. This data is collected from the Windows Spooler but must be enabled by the user to allow this
- Data is stored in a SQL Server: The customer controls the SQL server in a SiteAudit OnSite environment and can optionally decide that the data on the server be encrypted
- External Communication – outside the firewall: This is under control of the customer. The only external communication is via notification email or scheduled reports. The customer can control which notifications are sent and to whom. The same is true for scheduled reports

Netaphor Software Inc.

SiteAudit OnSite was launched in October 2006 and is sold to customers in over 50 countries.

Founded in 1997 and headquartered in Irvine, Calif., Netaphor Software, Inc. (www.netaphor.com) develops and sells asset management tools that help companies control printer costs and improve service. The company's flagship product, SiteAudit, is the leading software solution in the Mid-Market & Enterprise spaces to identify and manage costs and service saving organizations up to 30 percent during the printer asset lifecycle. Netaphor SiteAudit 5.0, 6.0 and 7.0 are the winners of the Buyers Lab (BLI) "Pick" award as Outstanding Fleet Management Solution by the editors at BLI analysts.