

**Netaphor SiteAudit**

## **Architecture and Design**

---

July 2011

# **SiteAudit On-Site™ Architecture and High-Level Design**

## **Customer Use**

*Pioneering Printer Asset Management*

# Contents

---

<b>Product Overview</b> .....	<b>3</b>
Data collection and analysis .....	3
Components.....	3
Hardware, Windows version, and SQL Server version .....	3
Database Sizing.....	4
<b>Architectural Diagram</b> .....	<b>5</b>
<b>Network Traffic</b> .....	<b>6</b>
Network Traffic .....	6
How Discovery Works .....	6
Discovery Scans Timing .....	7
Collection by Data Type .....	8
Network Traffic Volume .....	8
<b>Security Issues</b> .....	<b>10</b>
Network discovery .....	10
Directly Connected Printer; Windows Print Server Discovery.....	10
SNMP access .....	11
Credentials .....	11
Windows Firewall .....	11
<b>Questions</b> .....	<b>12</b>
<b>Netaphor Contact Information</b> .....	<b>13</b>
General contact information .....	13
SiteAudit technical support .....	13
SiteAudit sales .....	13

## Product Overview

---

SiteAudit is an asset management tool used to measure and report printer asset utilization, service, and costs. SiteAudit does the following:

- Builds a comprehensive inventory of network and desktop printer assets
- Tracks device usage
- Detect problems with devices

By collecting, analyzing, and reporting printer data, SiteAudit enables you to assess your enterprise's printer needs. SiteAudit measures printer asset performance in terms of both invoice costs and productivity costs.

### Data collection and analysis

---

SiteAudit stores data in a Microsoft SQL Server database. Data analysis is done by a set of SQL Server stored procedures and functions.

### Components

---

SiteAudit consists of the following major components:

- **SiteAudit Viewer** – the user interface through which you see collected usage data. The SiteAudit Viewer is also used to view, edit, and customize reports that can be viewed on the Reporting Web Site.
- **SiteAudit Monitor** – the Microsoft Windows service that performs printer discovery, collects usage data, and stores the data in a database
- **SiteAudit Scheduled Reports** – a utility, that automates copier and printer meter reading, eliminating the need for on-site reads. Several other reports can be scheduled using the Windows Task Scheduler. On a configurable schedule, it emails collected meter read data for invoice processing.
- **SiteAudit Reporting Website** - SiteAudit Viewer is installed wherever the SiteAudit Reporting Web Site is installed. SiteAudit Viewer is used to configure the database used by the Reporting Web Site and to publish reports to the site.

### Hardware, Windows version, and SQL Server version

---

SiteAudit is supported on Windows XP, and Windows Server 2003, Windows Vista, Windows 7, and Windows Server 2008 with all versions of SQL 2005 & 2008 (including SQL Server Express).

Netaphor does not state minimum values for processor speed or RAM. However, when evaluating the usability of servers, speed and memory should be as close to the following recommended levels as possible. The expected number of printers to be monitored should be a basis for hardware decisions.

For a computer that runs both SiteAudit Viewer and SiteAudit Monitor in a network with more than 250 printers, Netaphor recommends the following:

Operating System	Hardware	SQL Server
Windows 2003/08 Server	<ul style="list-style-type: none"><li>• Dual Quad or better</li><li>• 4 GB available RAM</li><li>• 400 MB free hard disk space</li></ul>	SQL Server 2005/08

For a computer that runs SiteAudit Viewer and SiteAudit Monitor in a network with at most 250 printers, Netaphor recommends that following:

Operating System	Hardware	SQL Server
Windows XP with SP2/Vista/Windows 7	<ul style="list-style-type: none"><li>• Dual Quad or better</li><li>• 2 GB available RAM</li><li>• 200 MB free hard disk space</li></ul>	SQL Server Express 2005/08

Note: To host web reports must support IIS 6 or later, supported by Vista, Windows 7 and Server 2003/08 platforms

## Database Sizing

SiteAudit does not need a dedicated database server; a SQL Server installation can be shared with other applications. The hardware and database server requirements depend on the database activity, the estimated amount of data collected over the period of monitoring, and the number of databases in use. These variables can often be determined by the database administrator.

The estimated amount of data collected depends on multiple variables, including:

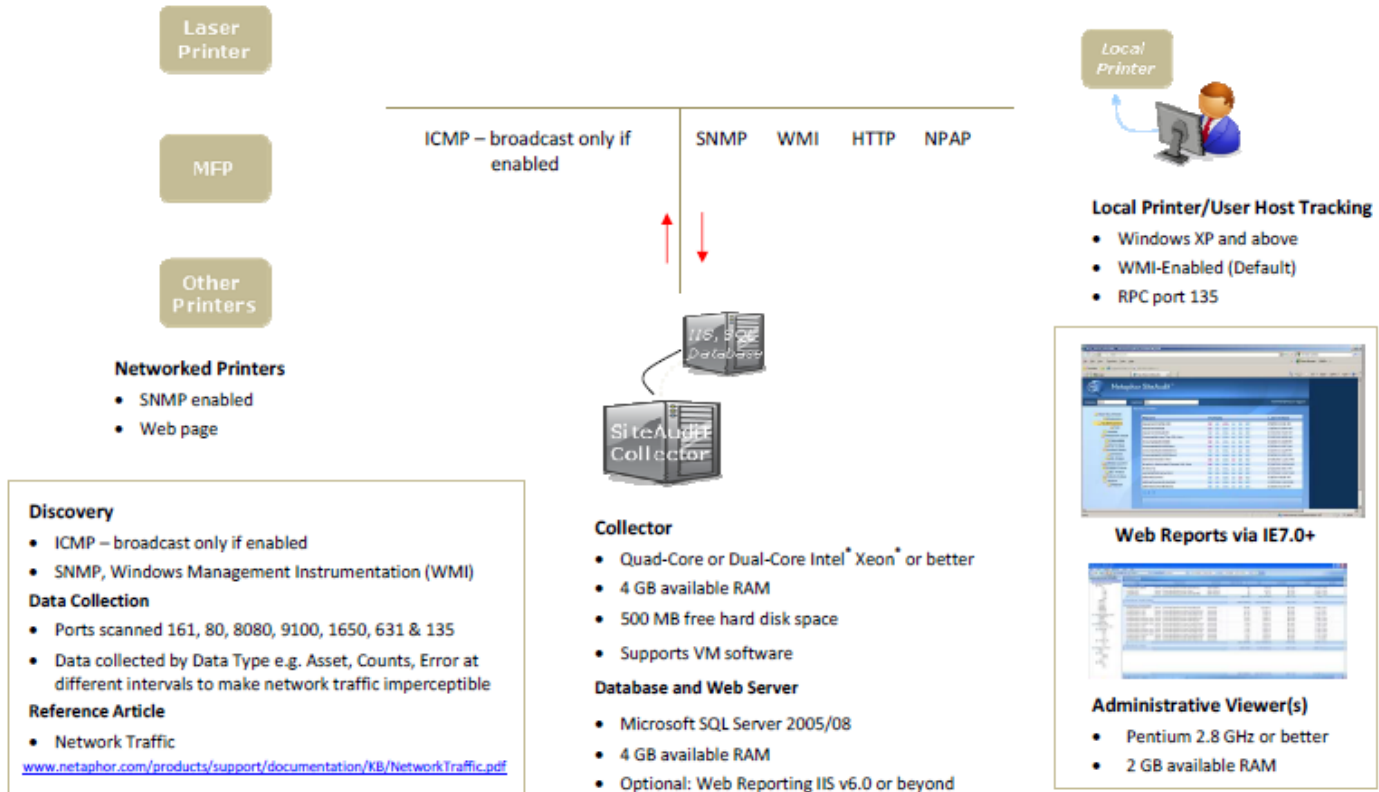
- The number of monitored printers
- The amount of printing activity
- The number of incidents and notifications

Typically the amount of database storage used varies between 500KB-1MB per printer per month.

# Architectural Diagram

The following diagram represents SiteAudit and its various components.

## SiteAudit On-Site Architecture



Netaphor Software Inc. – 2011

## Network Traffic

---

Minimal network traffic is the result of SiteAudit's design. The information below explains why network traffic is minimized.

### **Network Traffic**

Traffic can also be impacted based upon the way the network is designed and the number of networks, and its sub-netting and routing. This latter variance is of course true for any network application.

SiteAudit follows the "good citizen" principle of being unobtrusive and not adversely impacting the resources available to others in the environment.

- What is the traffic impact?

During normal operations the traffic impact cannot be measured, as it is minimal. There is no measurable impact on the network's bandwidth and quality of service. 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.

In contrast, other applications send blasts over the network. As a consequence, these types of applications require scheduling of data collection, typically during off-peak hours. *This is a product design difference* that shows up in the timing of when data is available and the amount of network traffic generated.

If 'Discover networks automatically' is selected, SiteAudit will use broadcasts on the local subnet (only) to find networks and devices. Broadcast can be disabled and discovery scoped to suite your environment. During the discovery cycle network traffic is measured at about 3%-to-5%. *This is the peak for SiteAudit*. SiteAudit allows IP network discovery information to be imported to facilitate quick and easy setup. (See Knowledge Base article "Importing Data").

### **How Discovery Works**

If desired, SiteAudit is designed to discover all printer assets. Broadcasts, if enabled, are sent during the discovery cycle only. Broadcast packets are of the following types:

- SNMP
- ICMP

The discovery process works as follows:

- 1) For each network on the list that is included determine the addresses in that list
- 2) Determine if any of these addresses are excluded (either via another network or via a range)

- 3) For an included address send an ICMP packet to that address
- 4) If the address responds to ICMP
- 5) Determine if it supports SNMP, use each of the specified community strings to determine which community string should be used
- 6) SiteAudit scans the following ports to find printers:
  - 161 SNMP to see if SNMP is available. SNMP is used to collect data.
  - 80 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 directly connected printers.
- 7) If it supports the Standard Printer MIB then it is a networked printer
- 8) If it supports SNMP but not the Standard Printer MIB and it supports Port 9100 (or equivalent) then it is a networked printer.
- 9) If it responds to ICMP but is not a networked printer determine if it serves Port 135.
- 10) If it supports Port 135 attempt to connect using WMI and one of the provided credentials
- 11) If the credentials worked, determine if there are any local printers or print queues on this host
- 12) The discovery process also scales to use multiple threads and connections depending on the host that it is running on and the resources

### ***Discovery Scans Timing***

The length of time that a discovery scan takes depends on a number of factors. These factors include:

- 1) The host that SiteAudit is running on and the resources available on that host (i.e. processor, memory, network bandwidth).
- 2) The number of network addresses to be scanned.
- 3) Network bandwidth including the bandwidth of all of the networks that have to be scanned
- 4) Density of the networks and ranges that are to be scanned. Sparsely populated networks will take significantly longer to scan. This is due to the fact that in sparsely populated networks a number of addresses will not respond to ICMP which in turn will require retries *after* the timeout period which causes the scan for these networks to last longer.

The default discovery scan is scheduled to run in 7 day intervals. Thus, the next scan will begin in 7 days after the end of the current scan.

### **Collection by Data Type**

SiteAudit printer data is of two types:

- Volatile Data (Data that can change frequently, default values):
  - Page Counts - collected every 3 hours
  - Print Jobs – collected every 4 hours
  - Toner Information - collected every 40 minutes
  - Alerts - checked for changes every 10 minutes
  - Thresholds – checked every 30 minutes
  - Device Status – checked every 10 minutes
  - Move Add Change – checked every 10 minutes
- Stable Data: (Data that does not change frequently)
  - Network and Identification information - Checked every 12 hours
  - Configuration Information (input/output options) - Checked every 12 hours

SiteAudit also stores data about addresses that are discovered by SiteAudit but are not printers. This data includes

- SNMP Information, Port Information
- For Windows hosts, Make/Model/Last Reboot time and Logged in User.
- For Windows hosts that are print servers and have queues located on them, SiteAudit will also collect job data (if configured to).

### **Network Traffic Volume**

Network traffic is dependent on the number of devices that SiteAudit is monitoring. The following factors go into calculating the number of packets:

- **Discovery Traffic:**
  - ICMP: An ICMP packet is sent to each IP address for each network on the list for discovery. If the broadcast address for a network is included then an ICMP broadcast is sent to that network. The packet is retried 3 times for devices that do not respond.
  - SNMP: An SNMP packet is sent to each IP address for each network on the list for discovery. If the broadcast address for a network is included then an ICMP broadcast is sent to that network. The packet is retried 3 times for devices that do not respond. The packet is retried for each community string in the list of community strings that are provided. This particular packet type can be reduced by

removing community strings that are not required from the list of pre-seeded community strings that have been provided.

- Port Scan: Each device that responds to an ICMP packet will also receive port scan packets. The port numbers that are scanned for each device are 161, 80, 8080, 9100, 1650, 631 and 135. All these are TCP ports with the exception of port 161 which is a UDP port. Each scan is retried 3 times.
- **Monitoring Traffic:**
  - Volatile data: This depends on the type of the device and the number of counters and consumable information available for each device. Advanced devices support about 20 counts. Each count requires one packet. Typical devices support 3-4 counts. Each packet is 512 bytes. There are no retries. Consumable data is similar to count data. Advanced devices support 3-4 types of consumables and each consumable has 6 pieces of information required for it. Thus, 18-24 packets for advanced devices may be required. Alerts are polled by examining the alert table. If there are no changes in the alert table then it is not retrieved. The alert table has 7 individual pieces of data for it that is retrieved.
  - Stable data: Typically about 100 packets of data per device are retrieved per day.
- **Local Printers and Queue Data:**
  - All of this data is retrieved using WMI. WMI uses RPC and windows authentication. 5 separate queries per host that is to be polled are issued. The packets are TCP and the size and number of the packets depends on the network packet size, the type of authentication present and the query being issued.
- **SQL Traffic:** SQL traffic is used to update the DB when data changes. This is TCP traffic to the server. SQL traffic also exists for queries between SiteAudit viewer applications and the database. The amount of traffic depends on the number of devices present, the maximum size of the network packet and the type of authentication used. The traffic is only between the hosts running SiteAudit and the SQL server.
- **Other Traffic:** Other traffic may exist if email notifications need to be generated. Additionally, if scheduled reports are used then these reports will be emailed to the destinations. Email traffic is to the SMTP server.

# Security Issues

---

## Network discovery

---

As part of the discovery process, SiteAudit first attempts to find a device and then tests to see if that device is a printer. Security software in the network may register these actions as suspicious.

To avoid these false positives, the **security software should be configured to ignore requests issued from the IP address where the SiteAudit monitoring software runs.**

Details of SiteAudit's network discovery activities:

1. SiteAudit performs broadcasts to find devices and routers.
2. SiteAudit performs ping sweep to find network devices.
3. SiteAudit scans the following ports to find printers:
  - 161 SNMP to see if SNMP is available. SNMP is used to collect data.
  - 80 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.
  - 135 RPC, used to detect a Windows host for directly connected printers.

## Directly Connected Printer; Windows Print Server Discovery

---

SiteAudit finds printers directly connected (via USB or parallel connections) to a Windows host. To access the host, SiteAudit requires the credentials of a user who is an administrator on that host.

To make sure that discovery succeeds, you should:

- Provide a credential that will work on all hosts
- Ensure that these credentials do NOT get locked out after a number of failed attempts
- Run the "Unauthenticated Hosts" reports to see which hosts did not allow access, and add the credentials for that host

## 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 that it uses to attempt to access SNMP data from a device.

This 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 a set of commonly used community strings) but a user can remove or add strings and can change the order in which 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, you should:

- 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

## Credentials

---

SiteAudit requires credentials in four 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 an 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.

## Windows Firewall

---

If Windows Firewall is enabled on Microsoft Windows XP, it must be configured to allow SiteAudit access to RIP, ICMP, SNMP, SQL Server, and the remote hosts for directly connected printers. On remote hosts that SiteAudit accesses, Windows Firewall must allow the corresponding packets in and the responses out. Enabling “Remote Monitoring” enables all of the firewall accesses that SiteAudit needs on a remote host.

On Windows XP Professional, ensure that remote logons are not ‘forced’ to the GUEST account — the default setting for computers not attached to a domain. For Security Policy, Network Access: Sharing and security model for local accounts, make sure this is set to ‘classic’.

On Windows XP SP2, Professional and Home editions ensure that remote administration is allowed. Access to TCP port 135 must be enabled on the SiteAudit Monitor host and all Windows target computers.

# Questions

---

## **Issue: How is Discovery Information provided to SiteAudit?**

Discovery information can either be entered manually via the SiteAudit user interface or via an import file. Information on importing this data is available at <http://netaphor.com/products/support/documentation/kb/DataImport.pdf>

## **Issue: Can virtualization be used for SiteAudit deployment?**

Yes, there are no known issues concerning virtualization (VMware etc.)

## **Issue: How are notifications generated in SiteAudit?**

Notifications are generated using email. The email is formatted as an XML and a XSL stylesheet may be used to customize this email to turn it into an alternate format. Information on this is available at <http://netaphor.com/products/support/documentation/kb/Notifications.pdf>

## **Issue: Where are reports that are automatically generated by SiteAudit stored?**

Automatically generated reports are delivered either via email, as an attachment or to a location specified by the user. Details on this are at <http://netaphor.com/products/support/documentation/kb/SchedulingReports.pdf>. Manually generated reports (via the SiteAudit Viewer or SiteAudit Reporting website) can be exported to any user specified location.

## **Issue: What is the software update process?**

There are no automatic updates in SiteAudit. Notifications of new releases are sent to registered users who must download the software and manually run the updates.

# Netaphor Contact Information

---

## General contact information

---

15510 Rockfield Blvd., Suite C-100  
Irvine, CA 92618 USA

Phone: +(949) 470 7955  
Fax: +(949) 470 4966

Toll free: 1-877-638-2479 – USA only

[www.netaphor.com](http://www.netaphor.com)

## SiteAudit technical support

---

To receive reseller technical support for SiteAudit:

Email: [support@netaphor.com](mailto:support@netaphor.com)

Please include the person's name, version (such as 4.4), a problem title, and a problem description with supporting information.

## SiteAudit sales

---

Phone: +1 (949) 232 9170

Email: [sales@netaphor.com](mailto:sales@netaphor.com)

## SiteAudit License Keys

---

Phone: +1 (949) 470 7955

Email: [licensing@netaphor.com](mailto:licensing@netaphor.com)