

Deploying SiteAudit Hosted - Europe

September 2011

- SiteAudit Hosted Architecture
- Prerequisites and Installation
- Network Traffic and Security
- Testing Alert Communication

Overview

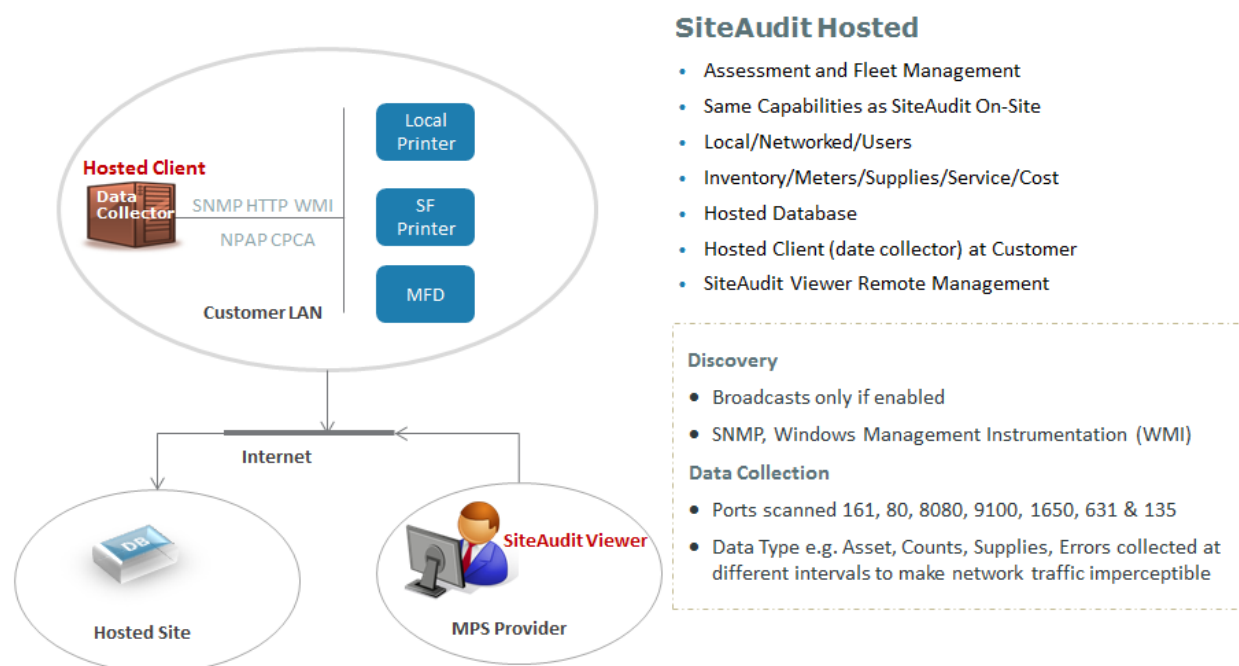
SiteAudit Hosted is a hosted application for assessments and fleet management. Discussed below is how to deploy SiteAudit Hosted and the architecture it uses.

Current Version: v4.4.0.3 released 15 June 2011

SiteAudit Hosted Overview

SiteAudit Hosted provides the same capabilities as SiteAudit On-Site except the database is hosted outside the customer's LAN/WAN. SiteAudit Hosted consists of the following software:

- Hosted Client installed at the customer site that collects data and displays an inventory view
- SiteAudit Viewer(s) installed at the MPS Provider's site(s) for configuration, analysis, alerting & reporting
- Hosted SQL database



The Hosted Client is licensed using a key file. It contains the license code to allow the client to collect data to hosted database and is sent to the customer by the MPS provider. After installation the hosted client prompts the user for the key file and the user simply points to it.

The SiteAudit Viewer is installed at the MPS provider and licensed once a machine ID has been processed into a license key. The Viewer is the same as the SiteAudit On-Site viewer with the same capabilities. The

viewer must be configured to point to the hosted database, which requires the name of the hosted database and the SQL owner credentials.

The database is hosted at a Netaphor infrastructure partner site in the Netherlands. Discovery and data collection of local and networked printers is accomplished without desktop agents and uses secure HTTPS to transfer data to the hosted site.

Deployment Prerequisites

The Hosted Client and SiteAudit Viewer run on Windows and require NET Framework 3.5 SP1. The recommended system for Hosted Client is below.

Fleet sizes greater than 250 printers use a Windows server with Windows 2005/08 Server and 4GB RAM

Operating System	Hardware	Bandwidth
Windows 2003/08 Server	<ul style="list-style-type: none">• Dual Quad or better• 4 GB available RAM	>1Mbps

Fleet sizes less than 250 printers use a Windows PC with XP/Vista/W7 and 2GB RAM

Operating System	Hardware	Bandwidth
Windows XP with SP2/Vista/Windows 7	<ul style="list-style-type: none">• Pentium 4 or better• 2 GB available RAM	>1Mbps

Local and networked printers are discovered by the Hosted Client.

Discovery configuration is added by the MPS provider using the SiteAudit Viewer. Discovery may include or exclude networks, ranges and IP addresses. The MPS provider can setup any other configurations such as: Thresholds, Notifications, Mail Server, Costs, Service Level Agreements, etc. It is important to that the SMTP server be accessible from the Hosted Client since it is the SiteAudit monitor service that sends notifications.

The discovery configuration can be imported through the Tools menu. Once the discovery configuration has been added, the monitoring is started by the Hosted Client.

Setup tip: obtain the discovery parameters from the customer prior to installing the Hosted Client. Enter the discovery configuration using SiteAudit viewer and then ask the customer to start monitoring: Tools menu → Start Monitoring.

- ✓ Networked printers must have SNMP-enabled
- ✓ Windows Management Instrumentation (WMI) is used to monitor local printers

As a general benchmark of discovery performance SiteAudit Hosted discovers 1,500 printers in one hour.

Note: Outbound SQL port must be open at SiteAudit Viewer installation (MPS Provider) and for the customer. Netaphor will inform you when the Key File is sent which port must be used for this purpose.

SiteAudit Hosted Installation Process

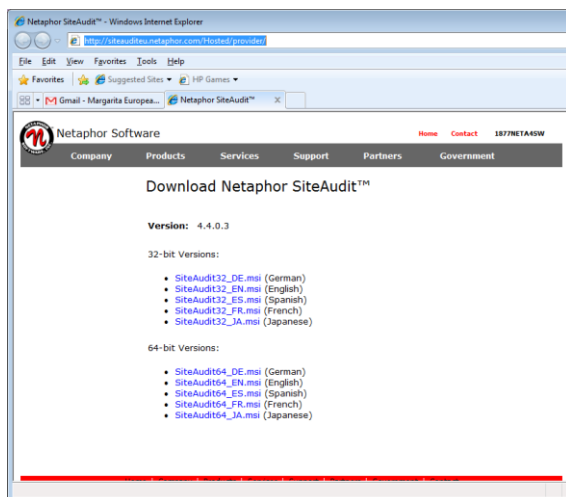
The installation process includes installing the SiteAudit viewer and the Hosted Client.

Basic Steps:

- 1) Partner provider asks for Hosted Deployment from Netaphor
- 2) Netaphor creates Customer database and provides key file and DB access information to partner
- 3) Partner accesses DB to setup discovery and other information (e.g. thresholds, notifications etc.)
- 4) Partner installs Hosted Client at the customer site and starts monitoring

Installing the SiteAudit Viewer

MPS Provider can download the viewer from from: <http://siteauditeu.netaphor.com/Hosted/provider/>



Install the Viewer only (View and setup reports only) and request a viewer license at licensing@netaphor.com

After installing the viewer do the following:

- 1- Connect to the hosted database
- 2- Add the discovery configuration

Connecting the hosted database:

Setup discovery and other settings in the viewer

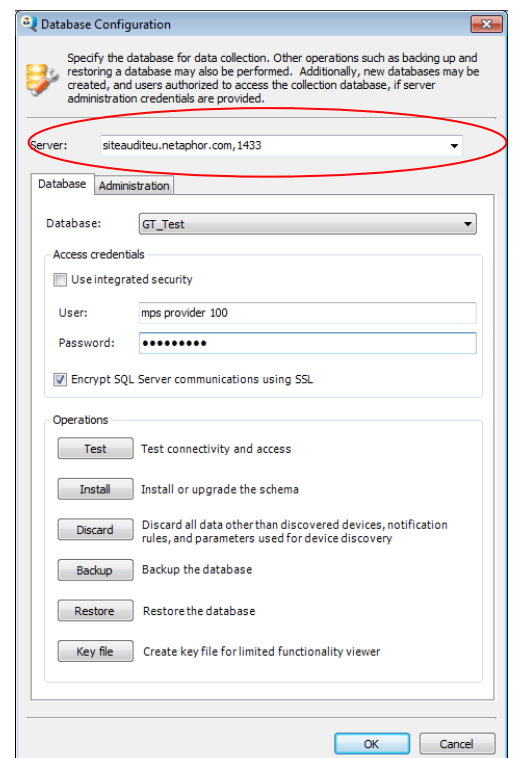
- a. Setup Database
- b. Server name¹ is siteauditeu.netaphor.com,1433
- c. Uncheck "Use Integrated Security"
- d. Check "Encrypt SQL Server Communications"
- e. Enter the credentials see below
- f. Select the DB (**customerX**)
- g. Click OK
- h. Set up the Discovery from Setup -> Discovery

Credentials for the MPS Provider:

User Name: **mps credential**

Password: **mps credential**

Database: **customerX**



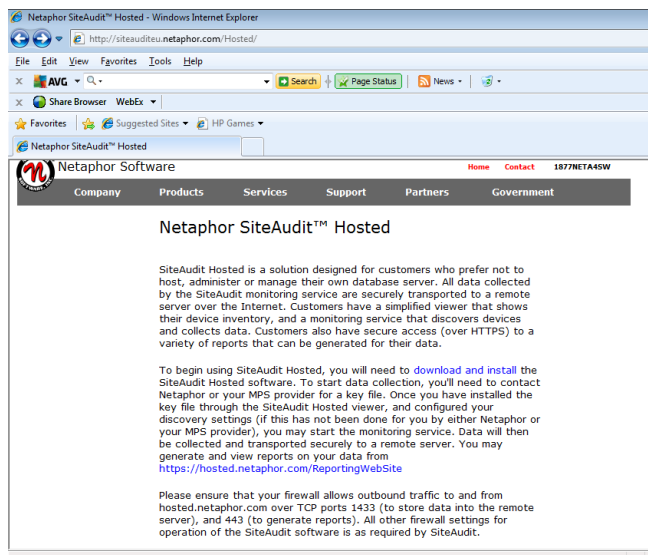
¹ Netaphor will inform on server and port number

Installing the Hosted Client

Customer or MPS Partner goes to <http://siteauditeu.netaphor.com/Hosted/>
Select and download the installation package for your system, 32 or 64 bit.

- Email Key File to customer; saves on desktop
- Customer installs SA Hosted Client
- Customer points SA Hosted Client @ key file (attached)
- Customer starts monitoring

Key File: **CustomerX.sakey**



Hosted Client

Start Discovery Tools → Start Monitoring



Note: SA Hosted Client cannot be installed on the same computer as the SiteAudit Viewer. The Hosted Client only provides an Inventory view.

Note: Outbound SQL port must be open at SiteAudit Viewer installation (MPS Provider) and for the customer. Netaphor will inform you when the Key File is sent which port must be used for this purpose.

Network Traffic

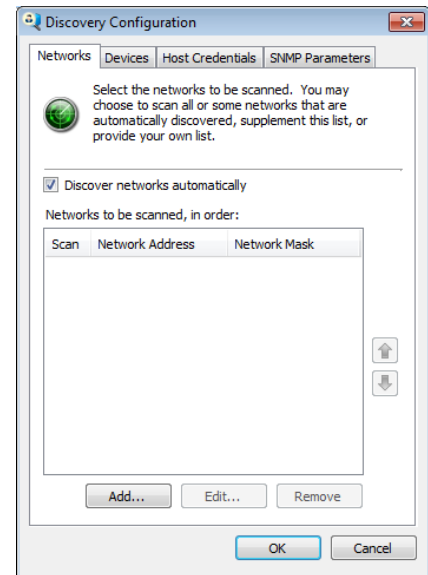
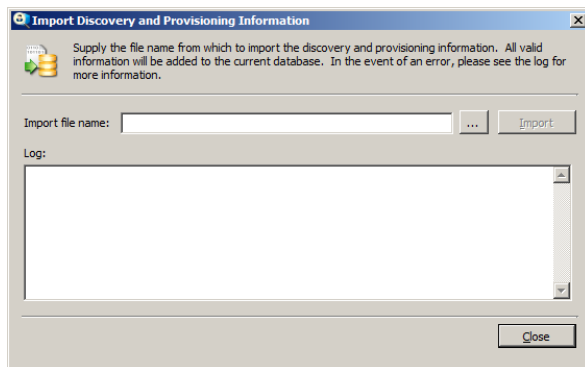
SiteAudit Hosted has minimal traffic as a result of its design.

- What is the traffic impact?

During data collection 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 Hosted data collection can be characterized as a *slow, steady receipt of packets*. This results in a smaller percent of the network bandwidth being used.

If 'Discover Networks Automatically' is selected, SiteAudit Hosted 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 Hosted*. SiteAudit Hosted 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 Hosted 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 string

SiteAudit Hosted 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.

- 6) If it supports the Standard Printer MIB then it is a networked printer
- 7) If it supports SNMP, not the Standard Printer MIB, it supports Port 9100 it is a networked printer
- 8) If it responds to ICMP but is not a networked printer determine if it serves Port 135

Local Printers:

- 1) If it supports Port 135 attempt to connect using WMI and one of the provided credentials
- 2) If the credentials worked, determine if there are any local printers or print queues on this host
- 3) The discovery process also scales to use multiple threads and connections depending on the host that it is running on and the resources available

- **Monitoring Traffic:**

It depends on the type of the device and the number of counters 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.

- **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.

SNMP Access

The SNMP protocol includes a provision for access control using “community” strings. A community string is required to access a device. SiteAudit Hosted maintains a list of community strings that it uses to attempt to access SNMP data from a device.

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 Hosted
- Disable the authentication failure traps on the device

Host Credentials

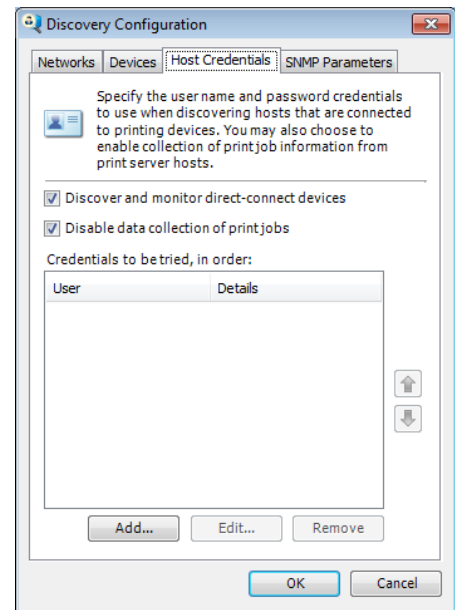
SiteAudit Hosted discovery requires credentials in two instances:

- 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.

Security

Some of the key security points are listed below.

- The Hosted server is certified with a VeriSign® SSL Certificate
- Hosted server is authenticated by a valid certificate; it is not self certifying (less secure)
- Hosted client and viewer connections are over secure HTTP/SSL (HTTPS)
- All Data collected is transported over HTTPS (same security level as credit card transaction.)
- Data is hosted behind firewall, and access is protected with encrypted password
- Reports web site access is protected via firewall and encrypted passwords



Security Software

As part of the discovery process, the hosted client 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 Hosted monitoring software runs.

Testing Alert Communication

To verify the alert capability is setup properly make a test. The reason is the monitoring is running on the customer's network and if it uses an SMTP server on that network the MPS Provider cannot test sending email from its SiteAudit Viewer.

The MPS Provider should try and use an SMTP server on their network (using credentials authentication /encryption) similar to what happens with GMAIL. Alternatively GMAIL is an option to use. This way there are minimal requirements of the customer's IT group.

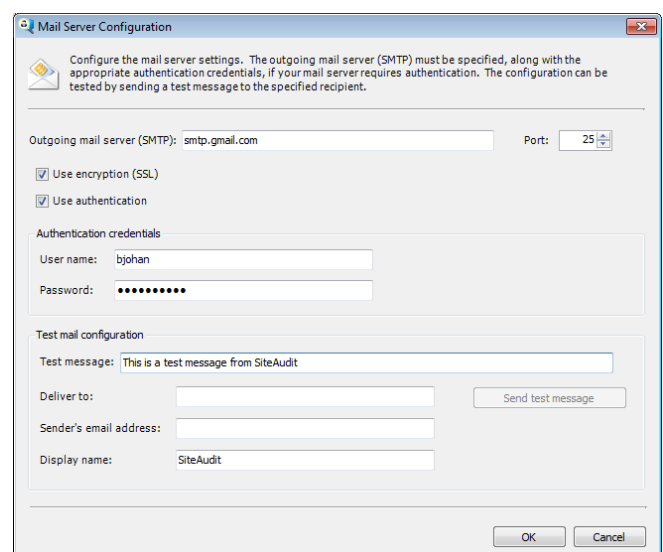
To setup GMAIL SMTP server:

Outgoing mail server (SMTP): smtp.gmail.com

Port: 25

Use encryption (SSL): selected

Use authentication: selected



Enter credentials of the user that has a GMAIL account.

Knowledge Base Articles

To read more about SiteAudit viewer capabilities click on or use the Knowledge Base links below:

Scheduling Reports

www.netaphor.com/products/support/documentation/KB/SchedulingReports.pdf

Working with Reports

www.netaphor.com/products/support/documentation/KB/WorkingWithReports.pdf

Consumables

www.netaphor.com/products/support/documentation/KB/Consumables.pdf

Alert Notifications

www.netaphor.com/products/support/documentation/KB/Notifications.pdf

Using Thresholds

www.netaphor.com/products/support/documentation/KB/Thresholds.pdf

Importing and Working with Organizations

www.netaphor.com/products/support/documentation/KB/WorkingWithOrganization.pdf