NETAPHOR SOFTWARE, INC.

SiteAudit™ Deployment Guide

Customer Use

December 2010

Pioneering Printer Asset Management

Contents

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.

About this guide

This guide describes how to install and configure Netaphor SiteAudit™ in your enterprise network.

For a brief overview of installation and configuration tasks, see the checklist on page 34.

Device discovery

SiteAudit can discover networked devices by scanning the network, using default settings or settings that you specify. You can also manually enter the IP addresses of subnetworks and devices.

Automatic discovery with the default settings does the following:

- Broadcasts to the local network and find all devices that respond to the broadcast.
- Finds all routers that respond to SNMP and RIP, finds each network that each router is connected to, and performs discovery on each discovered network. This process is recursive.
- Walks the set of all possible IP addresses for all known networks. Since all devices may not respond to broadcasts, it is necessary to probe the devices individually. For each known network, the list of IP addresses is computed using the network number and the subnet mask.

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
- **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, licensed separately, 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.

Deployment Decisions

Before you install and configure SiteAudit, you must make the following decisions:

- Where to deploy SiteAudit components
- Which hardware, operating system, and database server platform SiteAudit will run on
- How to represent, in SiteAudit's views and reports, the structure of your enterprise

Where to deploy components

SiteAudit Viewer

You should install SiteAudit Viewer on the computers for all users who would benefit by seeing the data that SiteAudit collects and the results SiteAudit's analyses. Examples include users who perform asset management, procurement, or IT tasks related to printers and printing.

SiteAudit Monitor

SiteAudit Viewer is installed wherever the SiteAudit Monitor service is installed. SiteAudit Viewer is used to start and stop the service and to configure the discovery and database settings. The SiteAudit Monitor service should be installed on a machine that can access and collect data from printers.

SiteAudit Reporting Web Site

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. The SiteAudit Viewer is also used to view, edit, customize reports that can be viewed on the Reporting Web Site.

Hardware, Windows version, and SQL Server version

SiteAudit is supported on Windows XP, and Windows Server 2003, Windows Vista, Seven, 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.

Number of Printers	Windows Operating System	Host Machine running Monitoring Service	SQL Server	IIS
< 250	XP SP3, Vista, Windows 7	**4 GB RAM** Dual Processor Quad Core or better **200 MB** Free hard disk space	SQL Server(or Express) 2005, 2008, or 2008R2; may run same Host as monitoring service Additional Disk Free space equal to 1/2 MB per month per printer. **1500MB/year**plus additional for backups	IIS 6, 7, 7.5 Additional 10MB Free space
250 - 1000	2003, 2008, 2008R2	**4 GB RAM** Dual Processor Quad Core or better **400 MB** Free hard disk space	SQL Server 2005, 2008, or 2008R2; may run on same Host as monitoring service Additional **10 GB** Disk free space/year	IIS 6, 7, 7.5 Additional 10MB Free space
1000 - 5000	2003, 2008, 2008R2	**4 GB RAM** Dual Processor Quad Core or better **400 MB** Free hard disk space	SQL Server 2005, 2008, or 2008R2; may run on same Host as monitoring service Additional **30 GB Disk** free space/year Additional **4GB** RAM if SQL Server is on same host as Monitoring Service	IIS 6, 7, 7.5 Additional 10MB Free space
5000 - 10000	2003, 2008, 2008R2	**8 GB RAM** Dual Processor Quad Core or better **400 MB** Free hard disk space	SQL Server 2005, 2008, or 2008R2; may run on same Host as monitoring service Additional **60 GB** disk free space/year Additional **8GB** RAM if SQL Server is on same host as Monitoring Service	IIS 6, 7, 7.5 Additional 10MB Free space
10000 - 25000	2003, 2008, 2008R2	**16 GB RAM** Dual Processor Quad Core or better **400 MB** Free hard disk space	SQL Server 2005, 2008, or 2008R2; may run on same Host as monitoring service Additional **150** GB disk free space/year Additional **16GB** RAM if SQL Server is on same host as Monitoring Service	IIS 6, 7, 7.5 Additional 10MB Free space

Note: Hosting Web reports requires IIS 6 or later, supported by Vista, Windows 7 and Server 2003/08 platforms. SiteAudit supports both 32 and 64 bit operating systems and SQL server versions. SQL database log files can grow significantly, especially during an upgrade from a prior version. One must be sure enough disk space exists to perform upgrades. The approximate space needed to perform the upgrade should be determined by the size of the database and be approximately twice the size. It is strongly recommended that the log file be shrunk after an upgrade and periodically thereafter as part of regular database maintenance.

Prerequisites

The following are things to do, or make sure of, before you deploy SiteAudit.

General

Previous installation of SiteAudit

If an existing installation of SiteAudit is present, back up the database. The backup mechanism in SiteAudit should be used for small test databases only. For production backups, use Microsoft SQL Management Studio to create the backup.

If upgrading from SiteAudit versions prior to 4.0, first uninstall SiteAudit and then upgrade to the post 4.0 version.

Database server

If a supported version of SQL Server is installed on the network, make sure that it is reachable and that you have the ***sa*** password. (In case SQL Server is not yet installed, the installation instructions appear later in this chapter.)

Creating a database and installing a schema for it requires administrator privileges. Once the schema has been set up, SiteAudit can use an account that it creates and that does not have administrator privileges.

Windows services

Remote discovery of directly connected (USB or LPT) printers requires that various services are enabled. Configure the startup type of these services as follows:

1. **Start > Run**
2. Type `services.msc` and press **Enter**.
3. For each service whose startup type you want to change:
    - Double-click the service name.
    - On the **General** tab, in the **Startup type** list, click either **Automatic** or **Manual** as recommended in the table below.

Service	Where needed	Startup type
COM+ Event System	SiteAudit Monitor	Automatic on servers
	Targets that need to be scanned	Manual on workstations

Service	Where needed	Startup type
Remote Access Auto Connection Manager	SiteAudit Monitor *or* SiteAudit Viewer	Manual
Remote Access Connection Manager	SiteAudit Monitor *or* SiteAudit Viewer	Manual
Remote Procedure Call (RPC)	SiteAudit Monitor *or* SiteAudit Viewer	Manual
Remote Procedure Call (RPC) Locator	SiteAudit Monitor *or* SiteAudit Viewer	Manual
Remote Registry	SiteAudit Monitor	Automatic
Server	SiteAudit Monitor *or* SiteAudit Viewer	Automatic
Windows Management Instrumentation	SiteAudit Monitor Targets that need to be scanned	Automatic
Windows Management Instrumentation Driver Extensions	SiteAudit Monitor	Manual
Workstation	SiteAudit Monitor *or* SiteAudit Viewer	Automatic

Host credentials

To scan hosts for directly connected printers and print queue information, SiteAudit requires Windows credentials that permit this action. The credentials must be those of a user who is a member of the "local" administrators group. Typically, in the case of hosts that are part of a Windows domain, the domain administrators group is also a member of the local administrators group. In this case, providing the credentials of a user who is a member of the domain administrators group is sufficient.

If the same username/password combination can be used for all hosts, you can provide SiteAudit with ***\username** and a password as credentials, and SiteAudit will substitute the name of each host as needed. This is typically the case in workgroup environments.

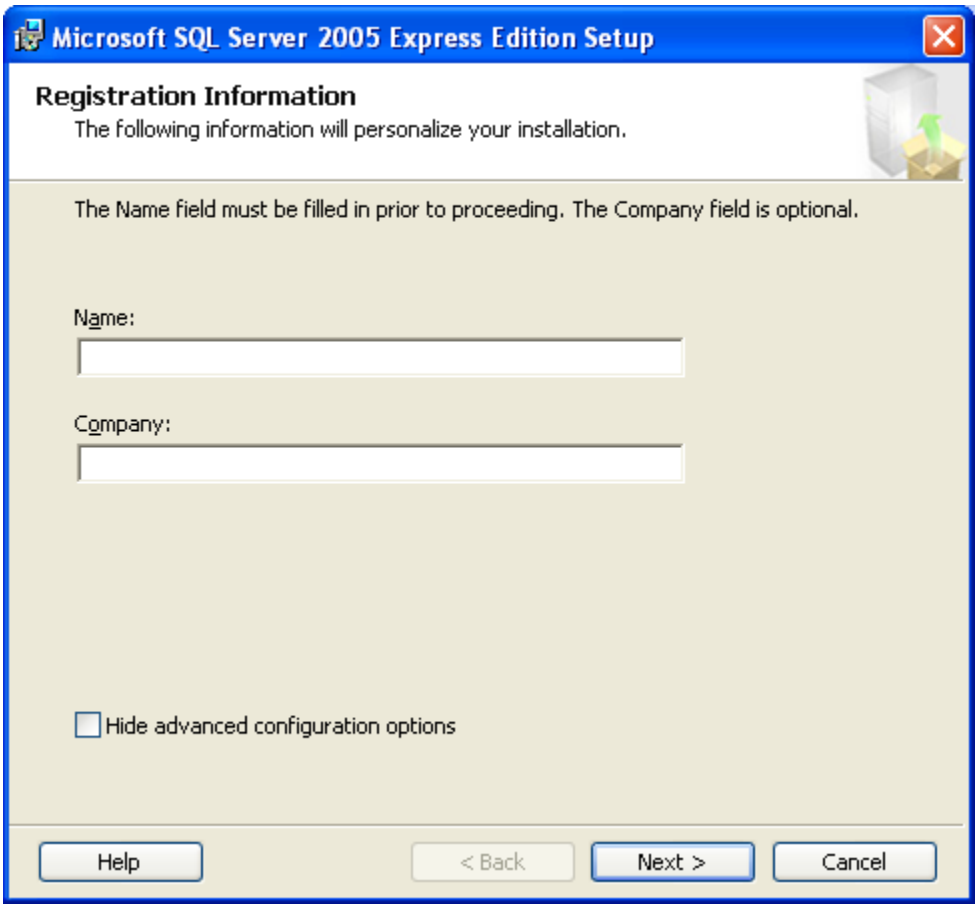
Install and configure SQL Server

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.

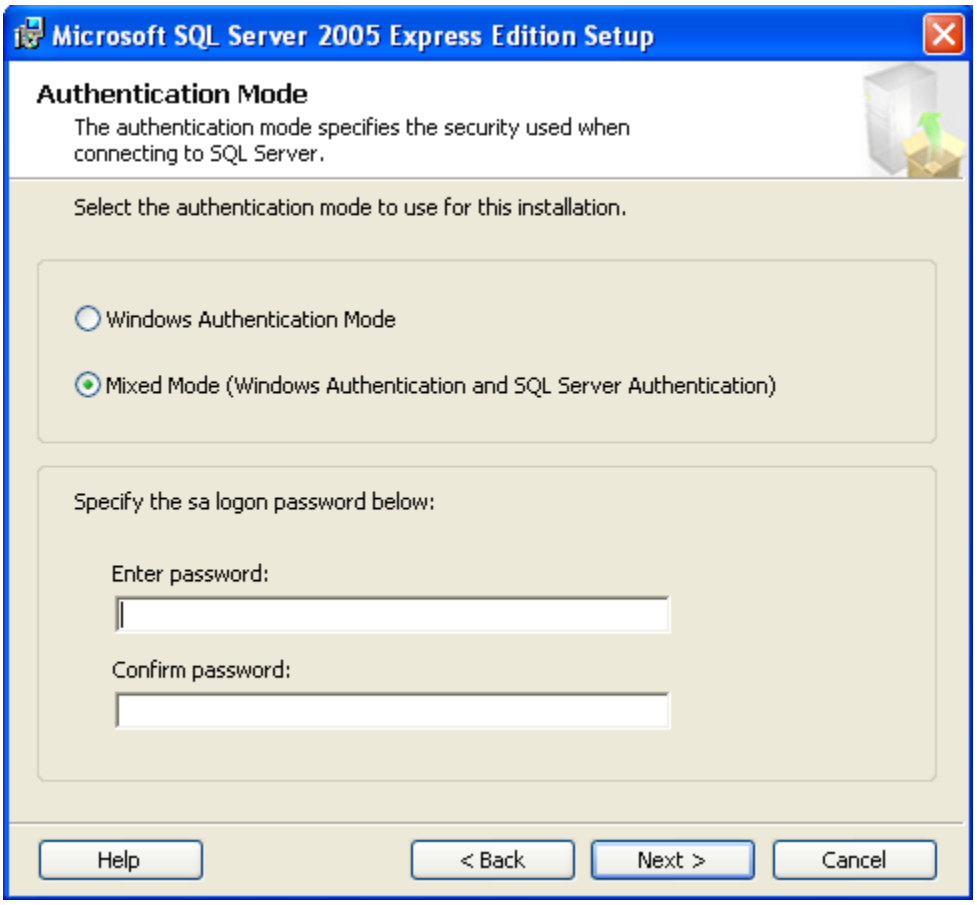
SQL Server 2005 Express Edition

For information about installing SQL Server Express, consult the documentation that accompanies SQL Server Express. SiteAudit requires that you make the following choices during installation:

- On the Registration Information screen, clear the Hide advanced configuration options check box.



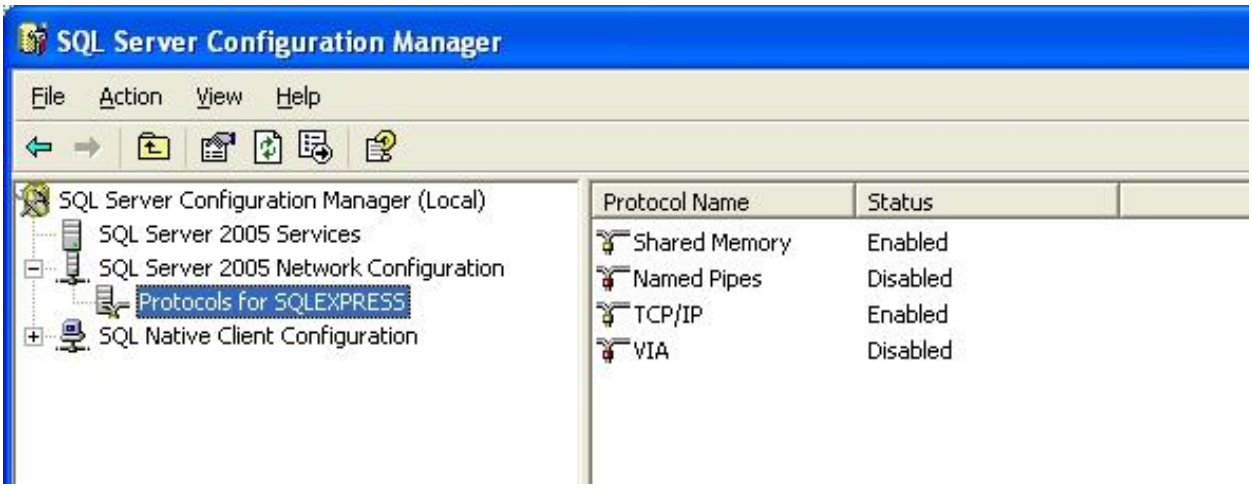
- On the **Authentication Mode** screen, select the **Mixed Mode (Windows Authentication and SQL Server Authentication)** option and provide the sa password.



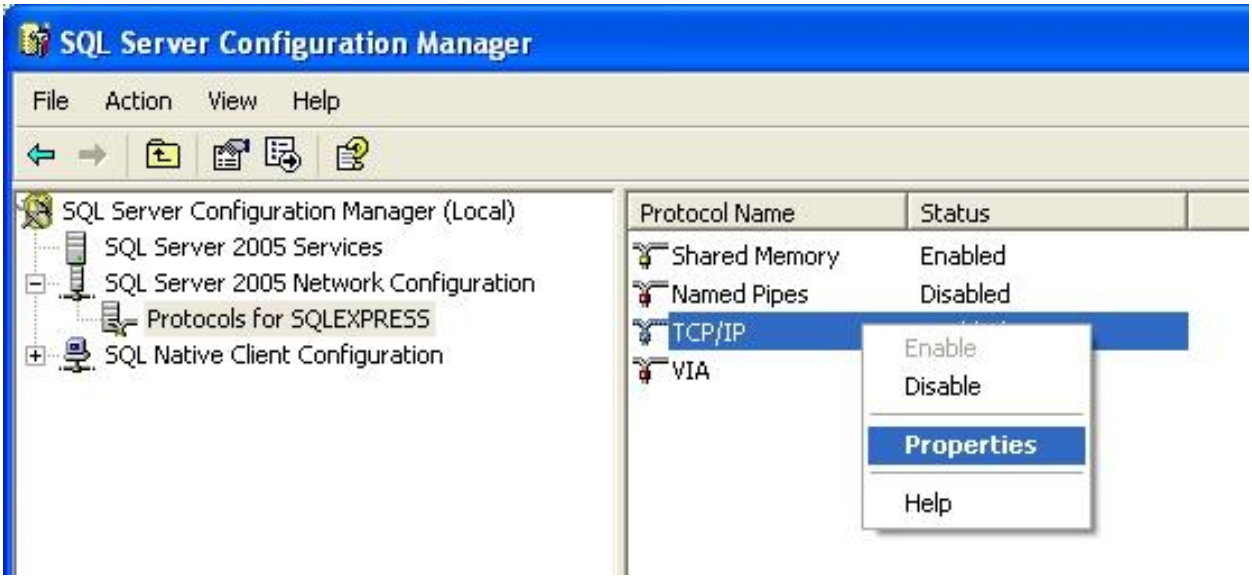
SQL Server Express must be configured with an sa password and with networking (TCP/IP). You can enable TCP/IP after SQL Server Express is installed.

1. **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**

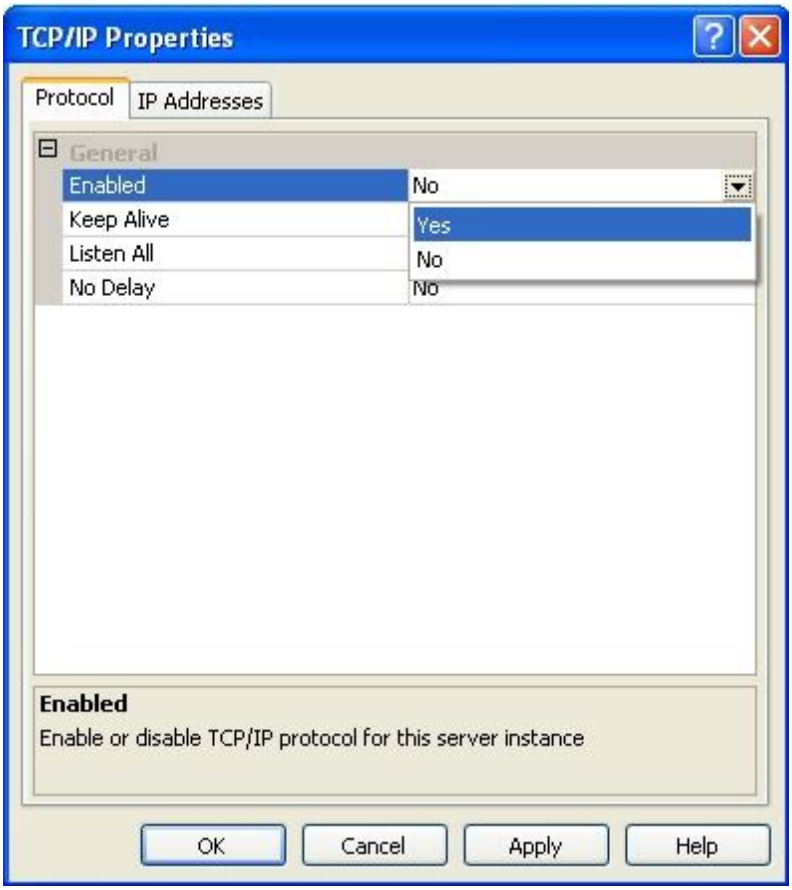
2. In the left pane, click **Protocols for SQLEXPRESS**.



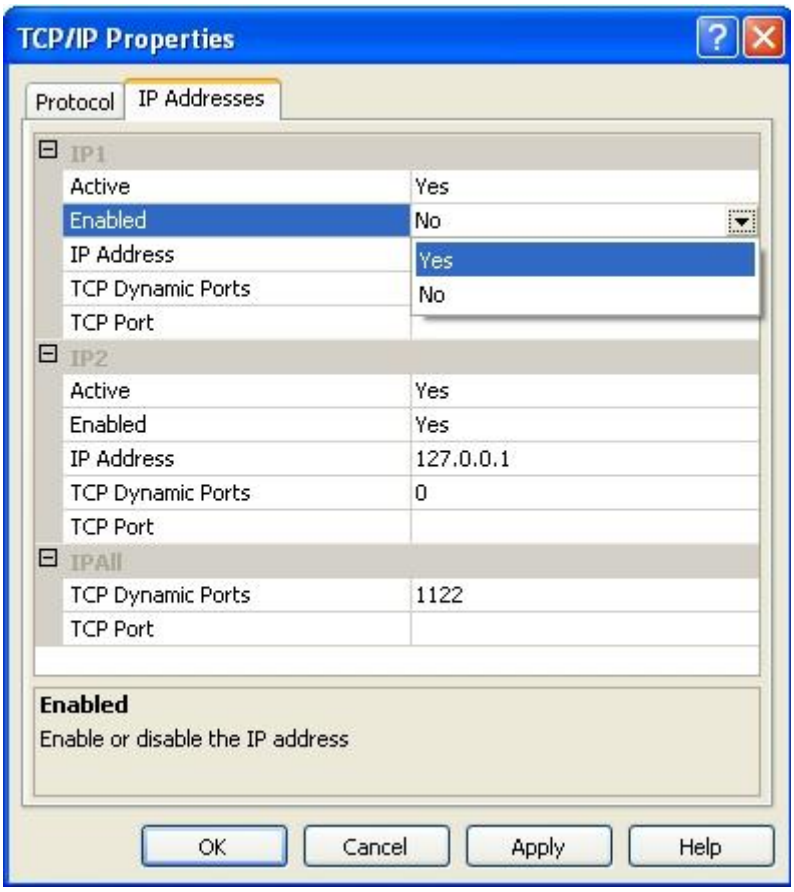
3. In the right pane, right-click **TCP/IP** and click **Properties**.



4. On the **Protocol** tab, set **Enabled** to **Yes**.



5. On the **IP Address** tab, for every IP address, set **Enabled** to **Yes**.

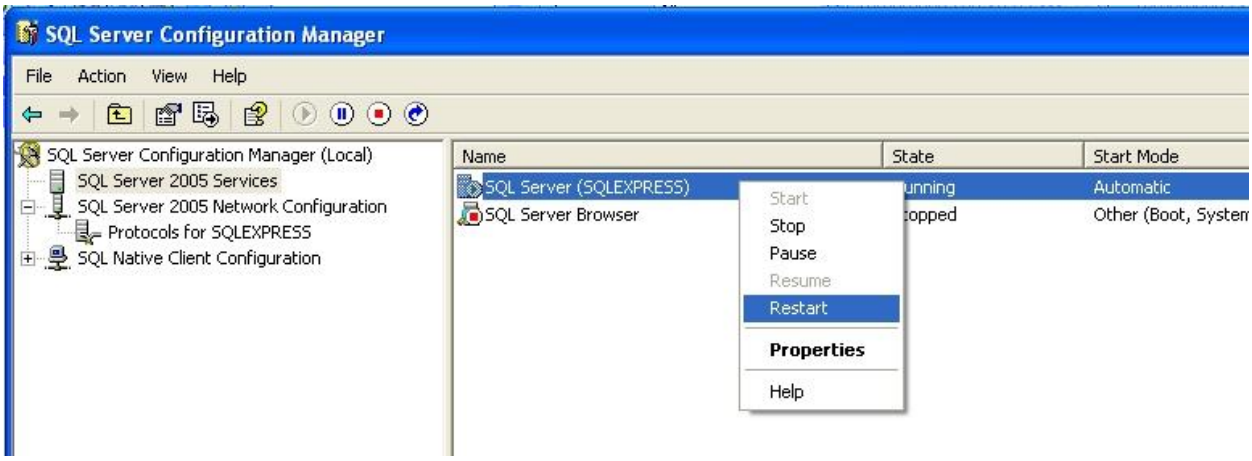


6. Click **Apply**.

   The following message appears:

7. Click **OK**.
8. In the left pane, click **SQL Server 2005 Services**.

9. In the right pane, right-click **SQL Server (SQLEXPRESS)** and click **Restart**.



After the restart, you can configure SiteAudit to connect to the database. For details, see *Database* on page 30.

About 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

A very rough benchmark for calculating your memory requirements:

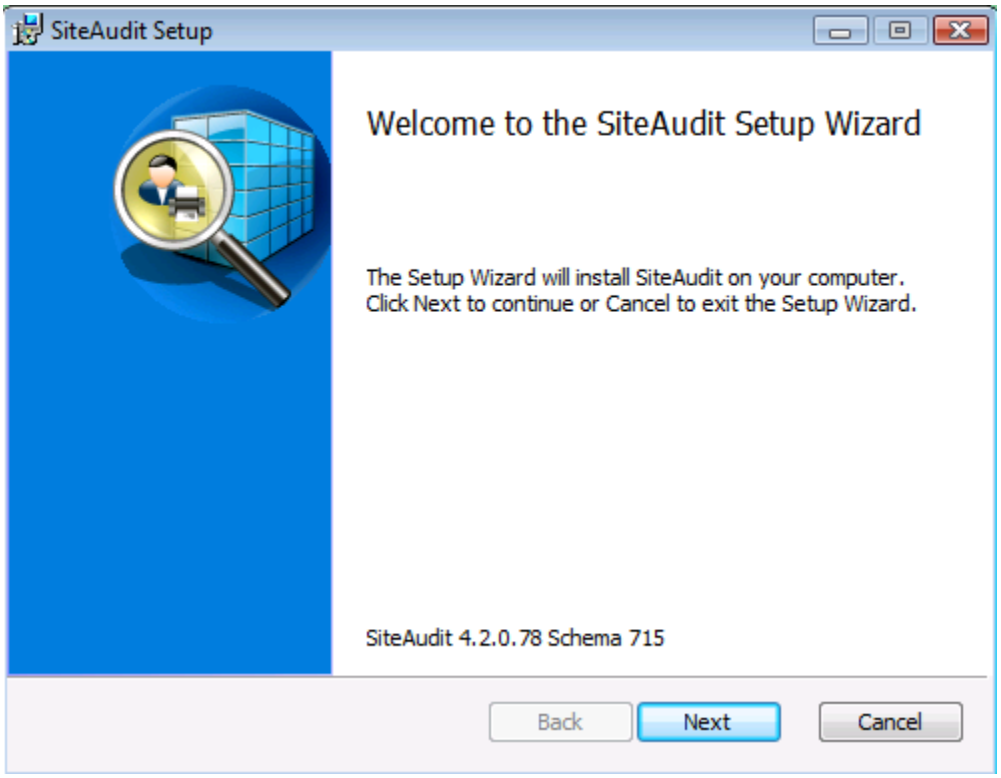
With 2000 active printers, and 220,000 incidents over four months, the total memory used is 1GB, and for a one-year period, the total memory used is 3GB to 5GB.

SiteAudit Installation

Installation of SiteAudit on a server or workstation requires a local account running as a service.

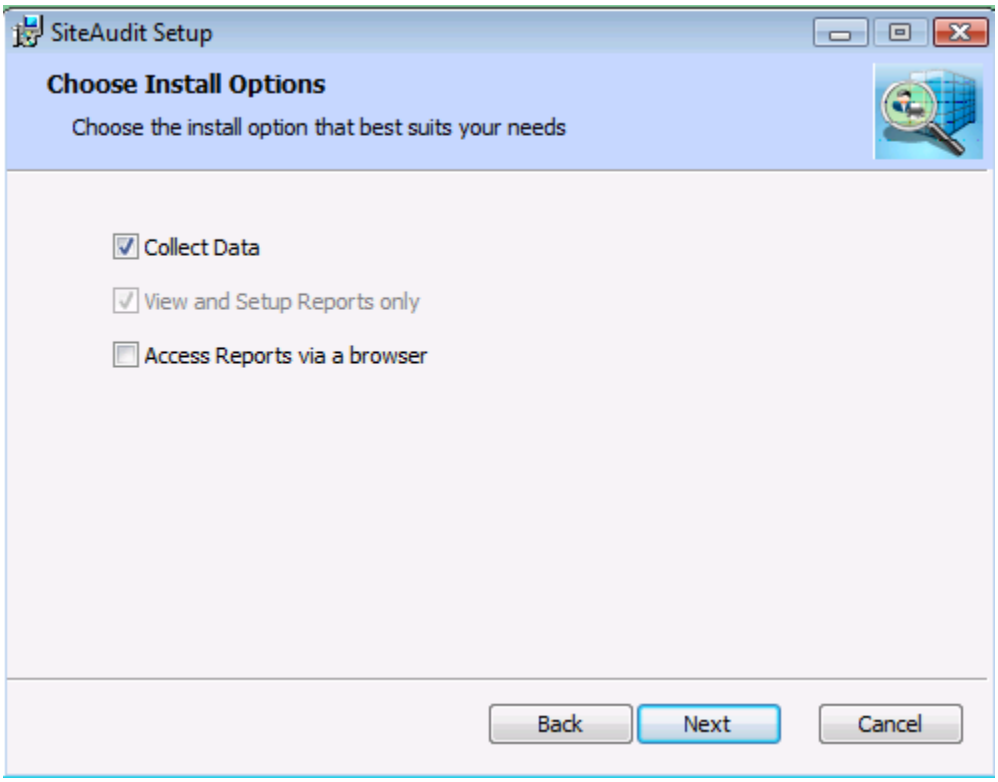
> **About addition Microsoft components**
>
> The following assumes that Microsoft .NET Framework 3.5 and Windows Installer 4.1 is already installed. If they are not, install the prerequisites first, which are available at the same location as the SiteAudit installation.

1. Run setup.exe from the installation source file. The introduction screen shows the version and schema for the SiteAudit installation

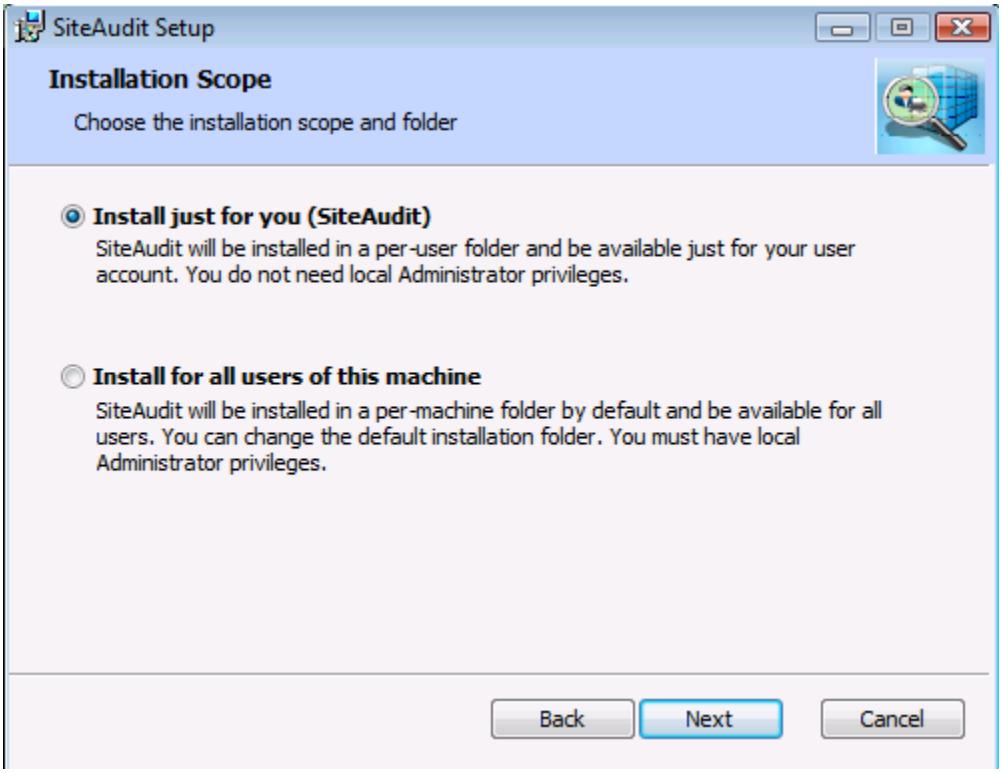


2. Click **Next**.

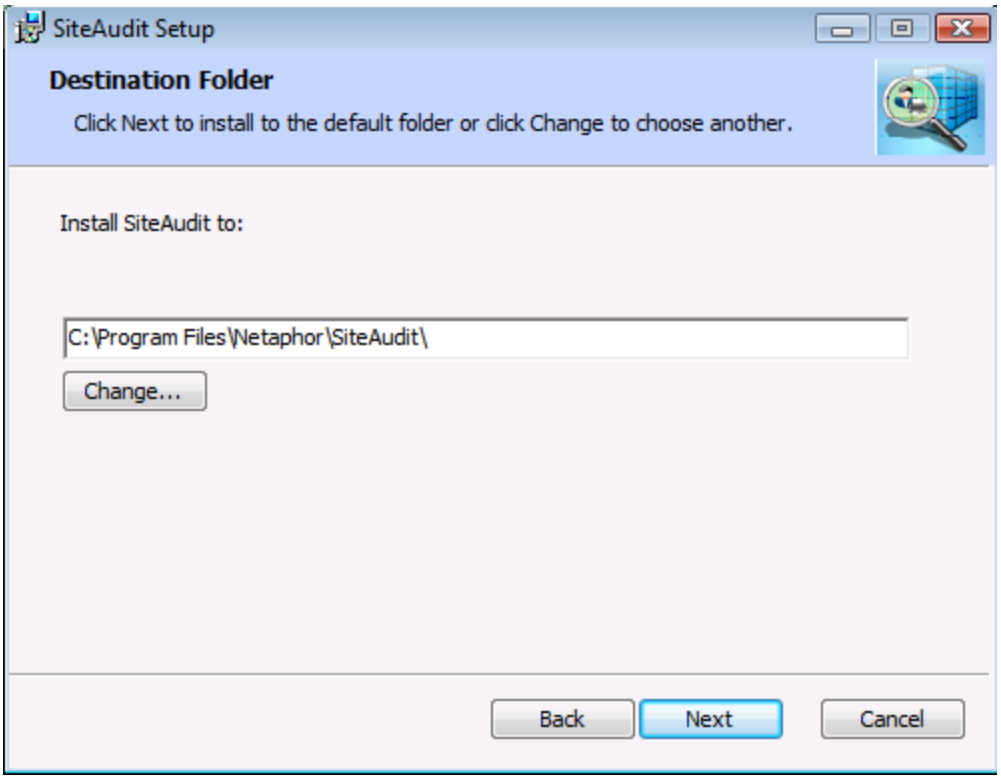
3. Accept the license agreement, and click **Next**.



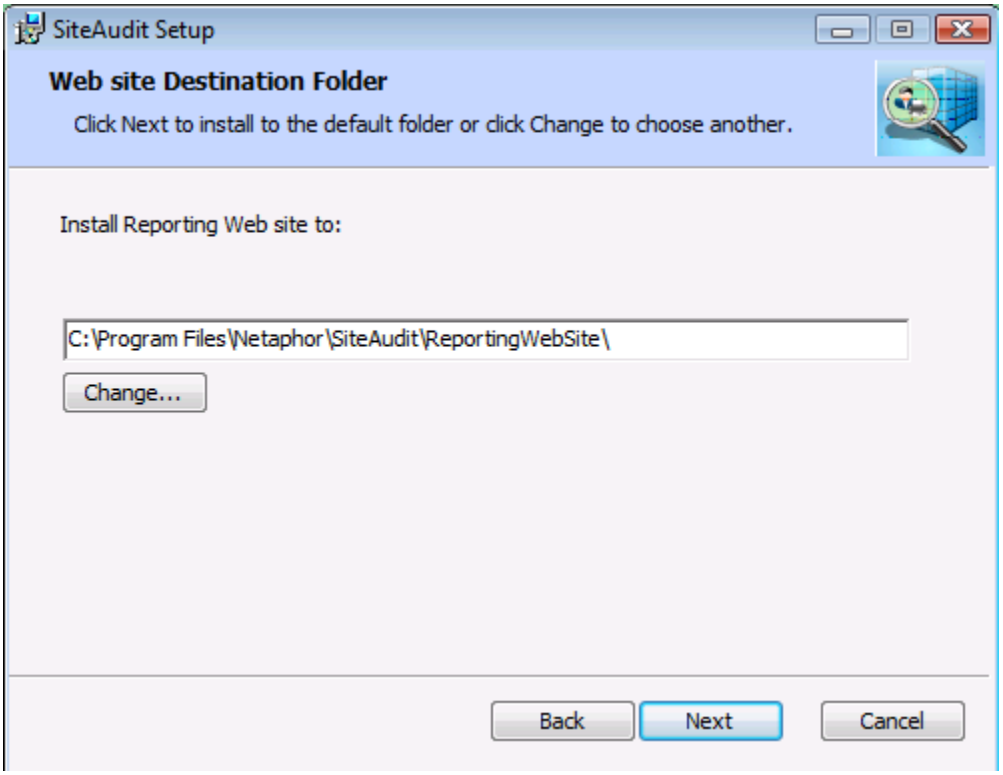
4. Select the components to install. To install the SiteAudit Viewer only, deselect the *Collect Data* component and select *View and Setup Reports only*. The SiteAudit Viewer is installed automatically If *Collect Data* or *Access Reports via a browser* is selected. Select both *Collect Data* and *Access Reports via a browser.*



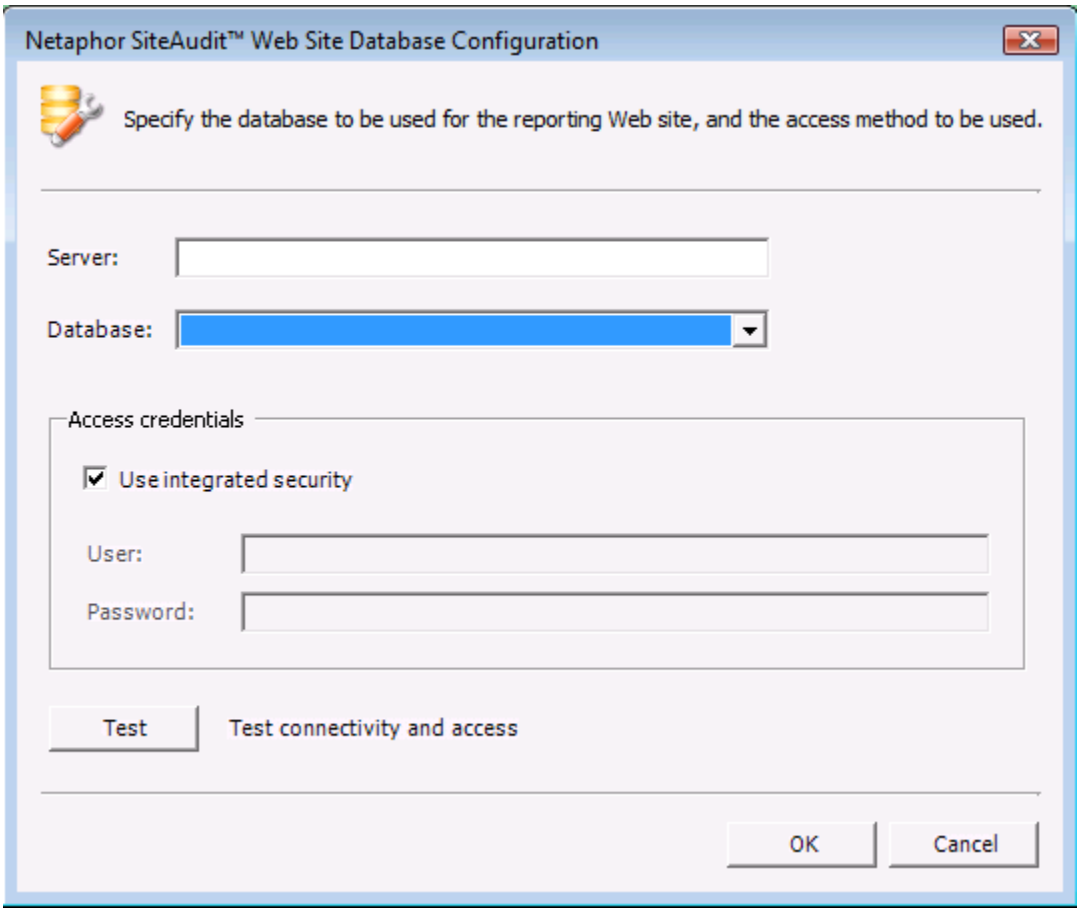
5. Click **Install for all users of this machine**, and click **Next**.



6. Specify an installation folder for SiteAudit, and click **Next**.

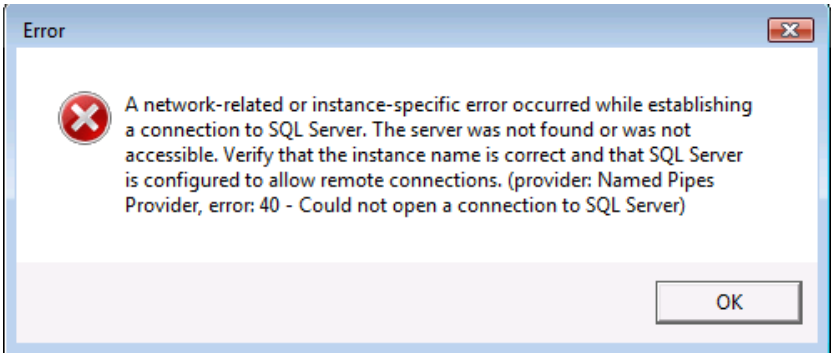


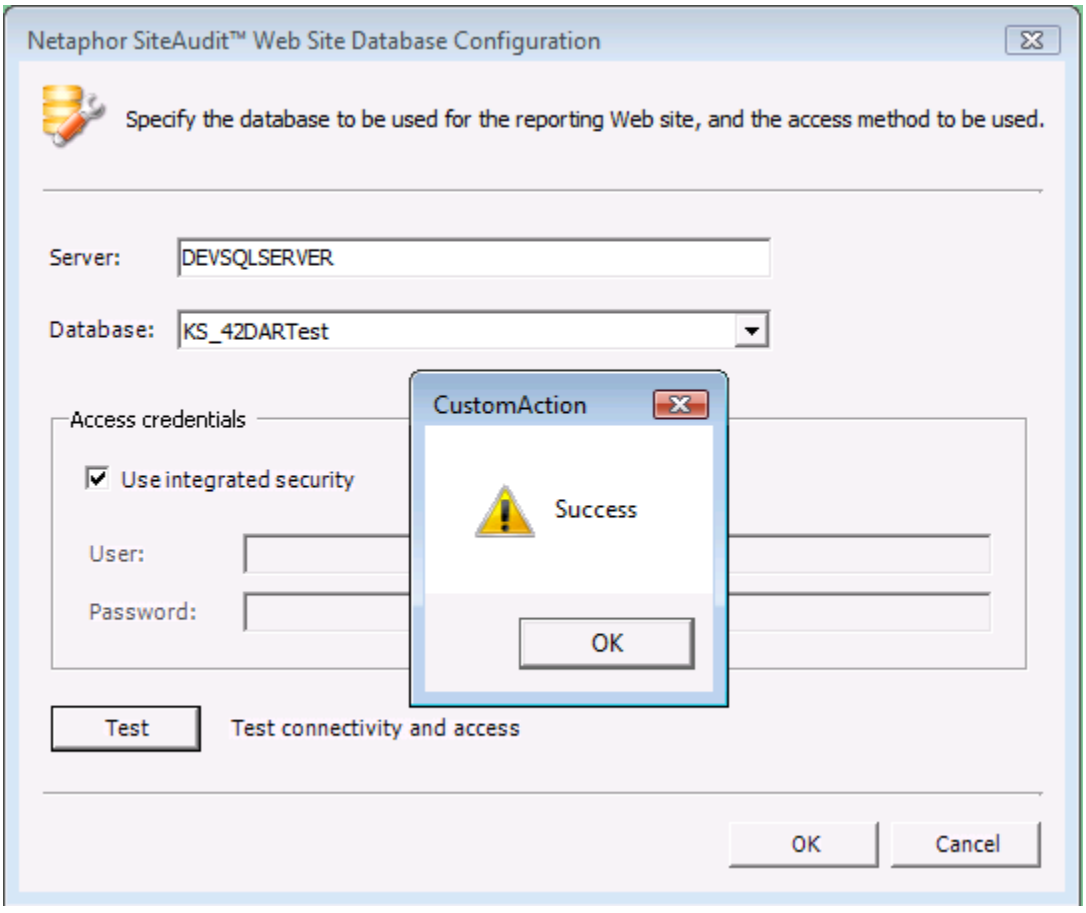
7. Enter the installation folder for the SiteAudit Reporting Web site and click **Next**



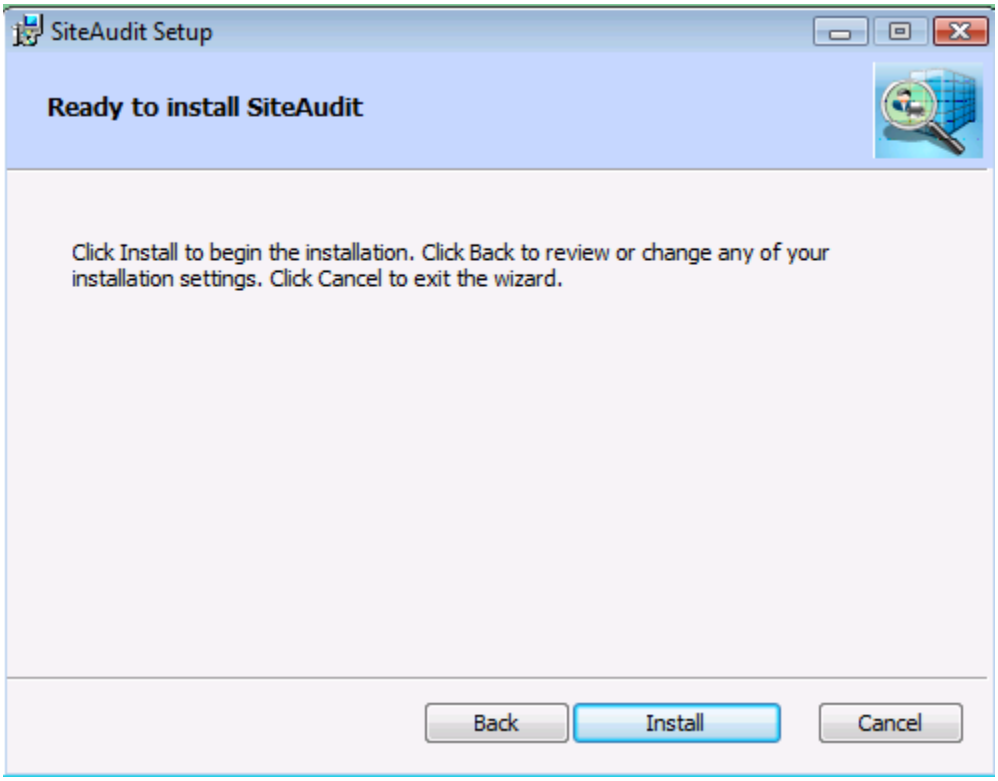
8. Enter the SQL server name and select the database where SiteAudit data will be stored. Specify the credentials used to access the database. It is NOT required to fill out this information during the installation process. The same dialog is available in the SiteAudit Viewer under the Setup/Website Database Configuration menu.

   If the credentials are invalid or the server cannot be accessed an error message will appear.

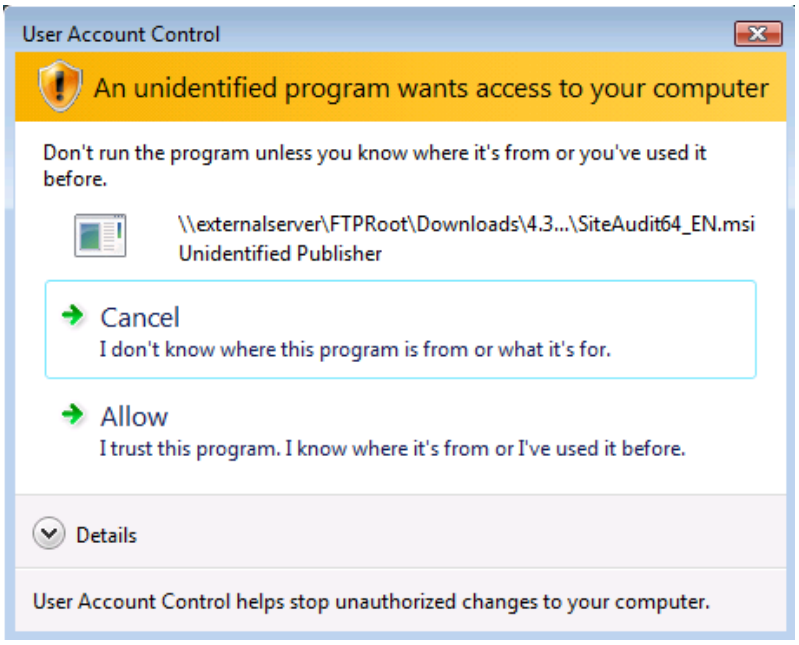


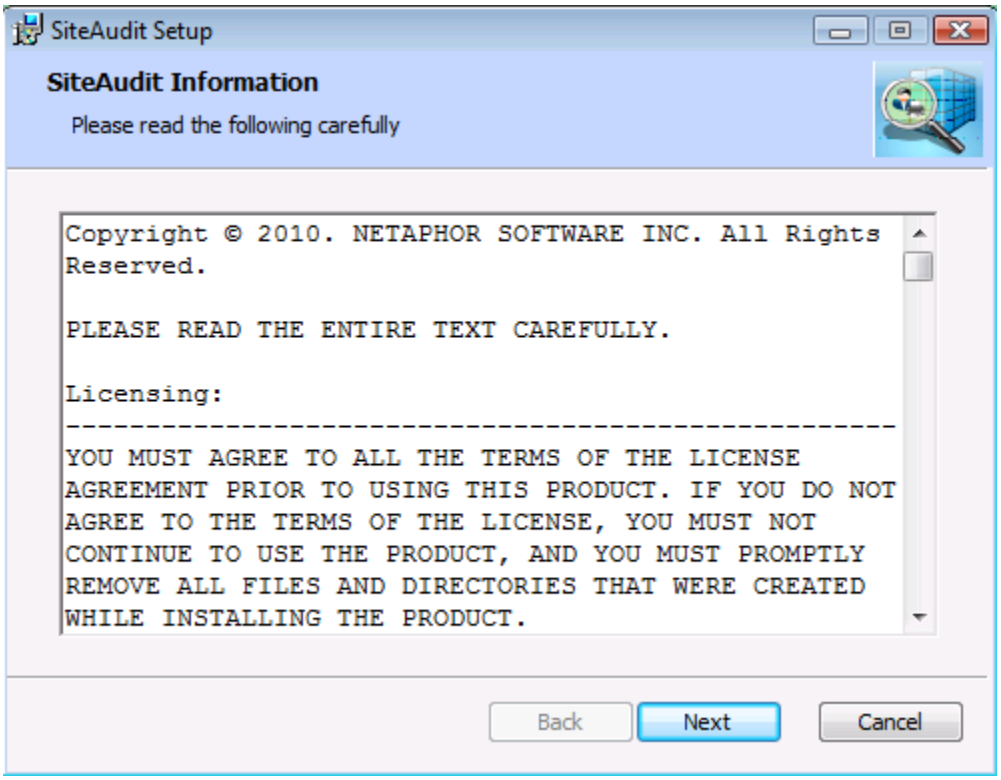


   If the correct credentials are entered and the **Test** button is clicked, a *Success* message should appear.

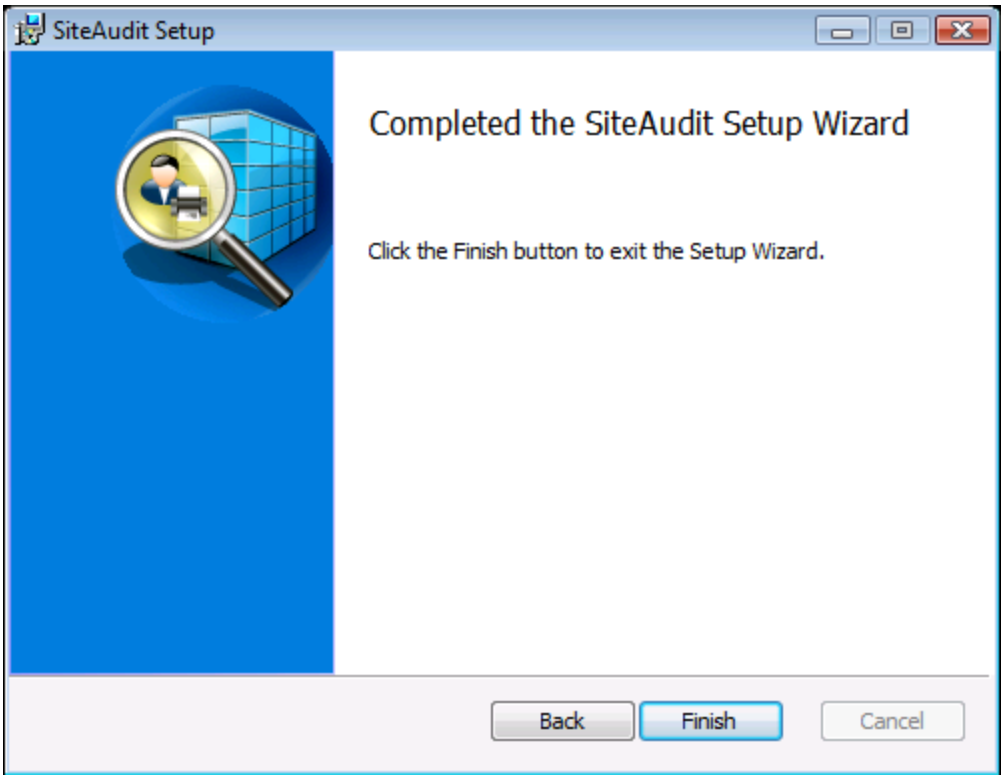

SiteAudit Setup
Ready to install SiteAudit
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

9. Click the **Install** button to start the installation. If installing on Vista or later OS, it may be required to elevate permissions to complete the installation. Click **Allow** to permit the installation.





10. Read the additional information, and click **Next**.



11. Click **Finish**.

SiteAudit Configuration

Once SiteAudit is installed, you should perform the following configuration tasks found on the **Setup** menu. Generally, these tasks need to be done only once.

Discovery

To configure SiteAudit's discovery of devices: **Setup > Discovery**

SiteAudit can discover and monitor both networked printers and directly connected (USB or LPT) printers. A networked printer is characterized by just an IP address. A directly connected printer is characterized by a combination of a host IP Address and a device ID that is unique for the host.

The **Connection** column in the inventory view (**View > Inventory**) or assessment details view (**View > Assessment Details**) identifies the printer as networked or direct connected.

Setup > Discovery opens the **Discovery Configuration** dialog box with its four tabs:

- **Networks** — the networks on which SiteAudit can discover devices. You can select the **Discover networks automatically (recommended if you have a small network)** check box to have SiteAudit find networks, and you can add networks manually with the **Add** button. For each network in the list SiteAudit may broadcast discovery packets. To enable broadcasts to a particular network that needs to be scanned add the broadcast address for the network to the "Devices" tab and check that device's check box. You can disable device discovery on a network by clearing that network's check box.

- **Devices** — the devices that SiteAudit monitors. You can select the **Discover and monitor devices automatically (recommended if you have a small network)** check box to have SiteAudit find devices, and you can add devices manually with the **Add** button. You can disable monitoring of a device by clearing that device's check box.

- **Host Credentials** — for each host with a directly connected printer, the user name and password of a user who is an administrator on that host. The host credentials of the domain administrator may in some enterprises be the administrator credentials on most or all host workstations on the network. If this is the case, only the domain administrator credentials are required. SiteAudit encrypts and stores these credentials. You can disable discovery of directly connected printers by clearing the check box for this option.

- **SNMP Parameters** — community strings to be used for remote access to devices by SNMP.

The following table gets you started with discovery tasks. Sections that follow the table provide details about key aspects of discovery.

Discovery Task	What you need to do
Discover devices using default settings	Nothing. Automatic discovery is enabled by default.
Prevent broadcast to local network	In the **Discovery Configuration** dialog box, on the **Networks** tab, clear the **Discover Networks Automatically** check box. On the **Devices** tab, clear the **Discover and monitor devices automatically** check box.
Exclude a network from scanning	In the **Discovery Configuration** dialog box, on the **Networks** tab, clear the check box for each network you do not want scanned. If the automatic settings for discovering networks are not being used, enter the network and clear its check box.
Scan specified networks only	In the **Discovery Configuration** dialog box, on the **Networks** tab, clear the **Discover Networks Automatically** check box. For each network that you want to scan, click **Add** and enter the network address and network mask. SiteAudit will broadcast to each added network and will attempt to contact every possible address using the network address and subnet mask provided.
Scan a specified set of devices only	In the **Discovery Configuration** dialog box, on the **Devices** tab, clear the **Discover and monitor devices automatically** check box. For each device IP address or ranges of addresses that you want to scan, click **Add**. For an individual address, simply enter that address in the **Starting IP address** box. For a range, select the **Specify a range** check box and enter The **Starting IP address** and **Ending IP address**.
Exclude a set of devices from scanning	In the **Discovery Configuration** dialog box, on the **Devices** tab, click **Add**, add an individual IP address or range of IP addresses, and click OK. In the **Scan** column, clear the check box for that address or range to exclude the devices from scanning.
Specify host credentials to be used when discovering host-connected devices	In the **Discovery Configuration** dialog box, on the **Host Credentials** tab, click **Add** to enter host user name and password information.
Prevent discovery of locally connected printer	In the **Discovery Configuration** dialog box, on the **Host Credentials** tab, clear the **Discover and monitor direct-connect devices** check box.
Provide SNMP community strings to be tried	In the **Discovery Configuration** dialog box, on the **SNMP Parameters** tab, click **Add** to enter a community string.
Rearrange the order in which SNMP community strings are tried	In the **Discovery Configuration** dialog box, on the **SNMP Parameters** tab, select a community string and use the up-arrow or down-arrow button to move the string within the list.

About networked printers

SiteAudit can discover networked devices by scanning the network, automatically or as you specify. Broadcast packets are of the following types: RIP, SNMP, and ICMP.

Automatic discovery with the default settings does the following:

- Broadcasts to the local network and find all devices on that network that respond to the broadcast.
- Finds all routers that respond to SNMP and RIP, finds each network that each router is connected to, and performs discovery on each discovered network. This process is recursive and thus finds networks within networks and devices in all of them.
- Walks the set of all possible IP addresses for all known networks. Since all devices may not respond to broadcasts, it is necessary to probe the devices individually. For each known network, the list of IP addresses is computed using the network number and the subnet mask. This process finds devices on all known networks.

On the **Networks** and **Devices** tabs, you specify whether, and over which IP address ranges, SiteAudit performs automatic discovery. You also specify which devices, if any, are added to or excluded from the list of those to be monitored within these ranges. That is, you completely define the IP address space over which you want discovery and monitoring performed. You can use network masks to include or exclude networks, ranges of IP addresses, and individual IP addresses.

Special circumstances to consider include the following:

- If discovery is to be performed over a range of IP addresses only, you should disable automatic discovery of networks and add the IP ranges manually.
- If certain networks are to be excluded from discovery and monitoring, you should allow SiteAudit to discover them and even add them manually if necessary, but disable discovery on them (clear their check boxes) before you start the discovery process.

About network traffic

During the first five minutes or so of automatic discovery, SiteAudit generates network traffic at about three to five percent during the first few minutes. *This small increase in network traffic is the peak of SiteAudit's impact.*

Once SiteAudit has created a full inventory of printer assets, it performs discovery every six days. Network impact is immeasurably small.

The design of your network, including sub-netting and routing, can impact traffic for any network application.

About directly connected printers

SiteAudit can discover and monitor locally connected (USB/LPT) printers. Discovery is limited to printers directly connected to hosts on network elements accessible to SiteAudit or on restricted segments that you define on the **Networks** and **Devices** tabs of the **Discovery Configuration** dialog box.

You can also manually enter the IP addresses of devices.

About importing discovery data

You can import discovery data in an XML file: **Tools > Import**

The file can specify

- Networks to include or exclude
- Network ranges to include or exclude
- Devices to include or exclude
- SNMP community strings to use

It can also specify device-specific information:

- Location
- Printer name
- Serial number
- Asset tag
- Acquired-on date
- Installed-on date
- MAC address
- IP address

The syntax of the file is as follows:

```
<root>

  <Import>

   <Discovery>

    <Networks>
     <Include>
                    IP addresses or address ranges to include in discovery
     </Include>
     <Exclude>
                    IP addresses or address ranges to exclude from discovery
     </Exclude>
    </Networks>

    <Ranges>
     <Include>
                    IP address ranges to include in discovery
     </Include>
     <Exclude>
                    IP addresses or address ranges to exclude from discovery
```

```
    </Exclude>
   </Ranges>

   <Devices>
    <Include>
                    IP addresses of devices to include in discovery
    </Include>
    <Exclude>
                    IP addresses of devices to exclude from discovery
    </Exclude>
   </Devices>

   <CommunityStrings>
                    Community strings to use
   </CommunityStrings>
  </Discovery>

  <Provisioning>
                    Device-specific information; for syntax, see example file below
  </Provisioning>

 </Import>

</root>
```

Only the <root> and <Import> tags are required. You can have multiple <Provision> and <Printer> tags.

Example file:

```
<?xml version="1.0" encoding="utf-8"?>
<root>
  <Import>

   <Discovery>
    <Networks>
     <Include>
      10.0.0.0 - 255.255.255.0, 192.168.0.0 - 255.255.255.0
     </Include>
     <Exclude>
      192.168.10.0-255.255.255.0
     </Exclude>
    </Networks>
    <Ranges>
     <Include>
      192.168.0.0 - 192.168.1.255
     </Include>
    </Ranges>
    <Devices>
     <Exclude>
      10.25.25.192,10.25.25.193
     </Exclude>
    </Devices>
    <CommunityStrings>
     public,private
    </CommunityStrings>
   </Discovery>
```

```
  <Provisioning>
   <Provision TYPE="MACAddress">
    <Printer>
     <MacAddress>
      AA-BB-CC-DD-EE-FF-00
     </MacAddress>
     <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
     <Location>
      <![CDATA[Irvine]]>
     </Location>
     <AssetTag>
      <![CDATA[QYYE234]]>
     </AssetTag>
     <AcquiredOn>
      <![CDATA[10/1/97]]>
     </AcquiredOn>
     <InstalledOn>
      <![CDATA[10/12/97]]>
     </InstalledOn>
    </Printer>
   </Provision>
   <Provision TYPE="SerialNumber">
    <Printer>
      <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
    </Printer>
   </Provision>
   <Provision TYPE="IPAddress">
    <Printer>
     <IPAddress>
      10.0.0.17
     </IPAddress>
     <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
    </Printer>
   </Provision>
  </Provisioning>

 </Import>
</root>
```

About host credentials

When attempting connection to a Windows host, SiteAudit tries each set of credentials on the **Host Credentials** tab until one set works or the list is exhausted. You should order the list so the most frequently used community strings are the first ones tried. You should configure the Windows users to ensure credentials do not get locked out after multiple failed attempts.

The SiteAudit "Unauthenticated Hosts" report provides detail on hosts that refuse access. You can add credentials to ensure complete discovery of directly connected print devices. A credential that works on all or a grouping of hosts is best.

If the credentials of the domain administrator do not provide administrator access on the host workstations in the network, you can provide each host's credentials individually. Alternatively, ***\username** is equivalent to **hostname\username**, with SiteAudit substituting the appropriate name for each host discovered.

Database

To configure SiteAudit's database connection: **Setup > Database**

When configuring the database in SiteAudit, for the server name you should use the following format:

HOSTNAME\INSTANCE_NAME

where HOSTNAME is the name of the host where SQL Server Express is installed and INSTANCE_NAME is the name of the SQL Server Express instance. You can use SQLEXPRESS for the instance name if you did not provide one during installation.

Version 1.6.1 allows users with owner permissions only to perform the database operations of setup/upgrade, backup and restore.

Database setup is described in the knowledge base article accessible online at http://www.netaphor.com/products/Support/Documentation/KB/DeploymentGuide.pdf.

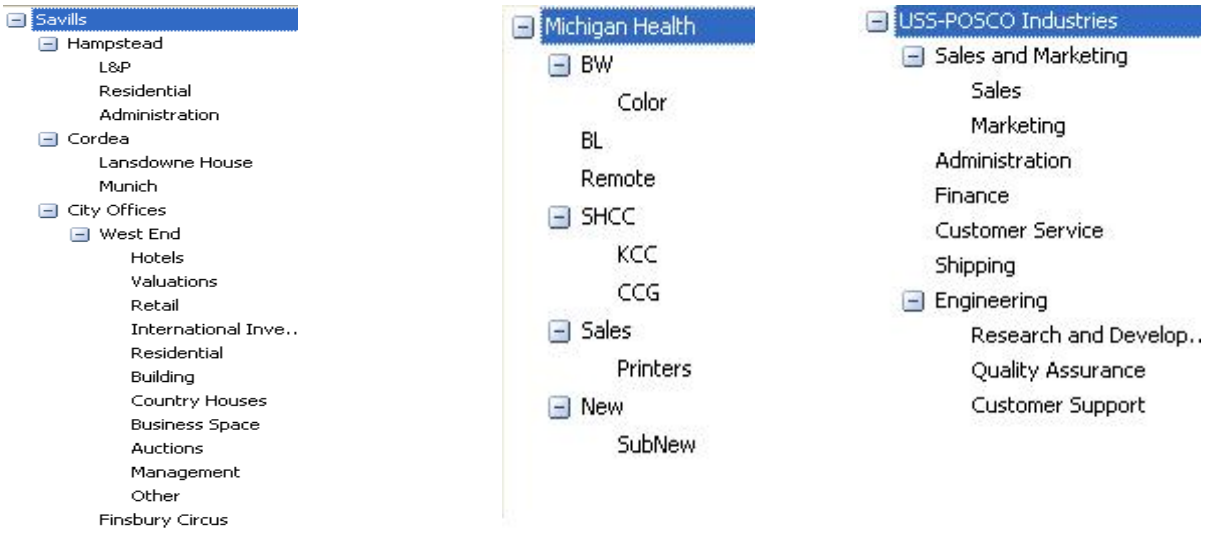
Company organization

To configure the hierarchical structure of the enterprise: **Setup > Company organization**

Within SiteAudit, you organize printers according to a scheme that addresses your needs. For example, if you want to track costs by department, you should organize the printers by department. This data can then be used to decide on printer acquisitions, to bill departments for printing costs, and for capacity planning.

Alternatively, you might organize printers by location (floor, building, or campus, for example). Views and reports can thus be generated geographically rather than by business unit.

See the examples below.



Printer assignment

Once you have specified your company organization, you assign printers to departments, cost centers, locations, or other units within the organization.

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 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.

Checklist

You should review this checklist before and after deploying SiteAudit.

1. Platform:

   - ☐ Make sure that the platform requirements are as specified beginning on page 5.

2. General prerequisites

   - ☐ If SiteAudit is already installed, back up the database.
   - ☐ If the installed SiteAudit is a previous version, uninstall it.

3. Database:

   - ☐ If SQL Server is installed on the network, make sure it can be used and that there is a database for data collection.
   - ☐ If SQL server will be used and you are using SQL security, make sure that you have the sa password. If you are using integrated security, make sure that the host account where SiteAudit monitoring will be run has database administrator access on the SQL Server database.

4. Windows services:

   - ☐ Make sure that the services listed under *Windows services* on page 7 are started or able to be started.
   - ☐ Make sure that Windows Management Instrumentation (WMI) access is enabled on every client computer that needs to be scanned and on the host where SiteAudit Monitor is running.

5. Network discovery:

   - ☐ Make sure that all networks over which discovery should be performed are listed, and their check boxes selected, on the **Networks** tab of the **Discovery Configuration** dialog box.
   - ☐ Make sure that all networks over which discovery should NOT be performed are listed, and their check boxes CLEARED, on the **Networks** tab of the **Discovery Configuration** dialog box.
   - ☐ Add any ranges that are not automatically discovered but need to be included or excluded, and select or clear their check boxes as appropriate.
   - ☐ On the Devices tab, add any devices that need to be added or excluded. Devices that should be excluded are UPS devices, DNS server(s), and other devices that should not be accessed.
   - ☐ Decide whether broadcasts should be used.

6. SNMP:

   - ☐ Make sure that all needed community strings are in the list.
   - ☐ Order the list to make sure that most frequently used community strings are the first ones tried.
   - ☐ Remove any community strings that will not be used.

7. Windows hosts:

   - ☐ Make sure that all needed credentials are in the list on the **Host Credentials** tab of the **Discovery Configuration** dialog box.
   - ☐ Make sure that any necessary firewall access has been configured.

8. Security:

   - ☐ Check to see whether security software needs to be configured as described beginning on page 32.

Troubleshooting

Issue: I would like data to help with debugging a problem

Using RegEdit, under HKLM\Software\Netaphor\PALM, add a key called Debugging. Under this key, add a DWORD value called EnableEventLog, and set this value to a non-zero value. This will cause SiteAudit to generate Windows Event Log events.

Issue: I am trying to access a database server over a WAN link, and it times out

Using RegEdit, under HKLM\Software\Netaphor\PALM\Database, add a DWORD value called CommandTimeout, and set this value to 2000 (decimal).

Issue: Database access is very slow

Consult with the database administrator to see whether the database needs to be compacted.

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

SiteAudit technical support

To receive reseller technical support for SiteAudit:

Email: support@netaphor.com

Please include the person's name, version (such as 1.3), a problem title, and a problem description with supporting information.

SiteAudit sales

Phone: +(949) 232 9170

Email: sales@netaphor.com