



Deployment Check List

March 2012

In This Article:

- Platform Requirements
- Windows Settings
- Discovery Configuration

Before deploying SiteAudit it is recommended to review the information below. This will ensure efficient installation and operation of SiteAudit.

Platform Requirements

You should review this checklist before and after deploying SiteAudit.

1. Platform:

Operating System	Hardware	SQL Server
Windows 2003/2008/2008R2	<ul style="list-style-type: none">• Dual Quad or better• 4 GB available RAM• 400 MB free hard disk space	SQL Server 2005/2008/2008R2

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

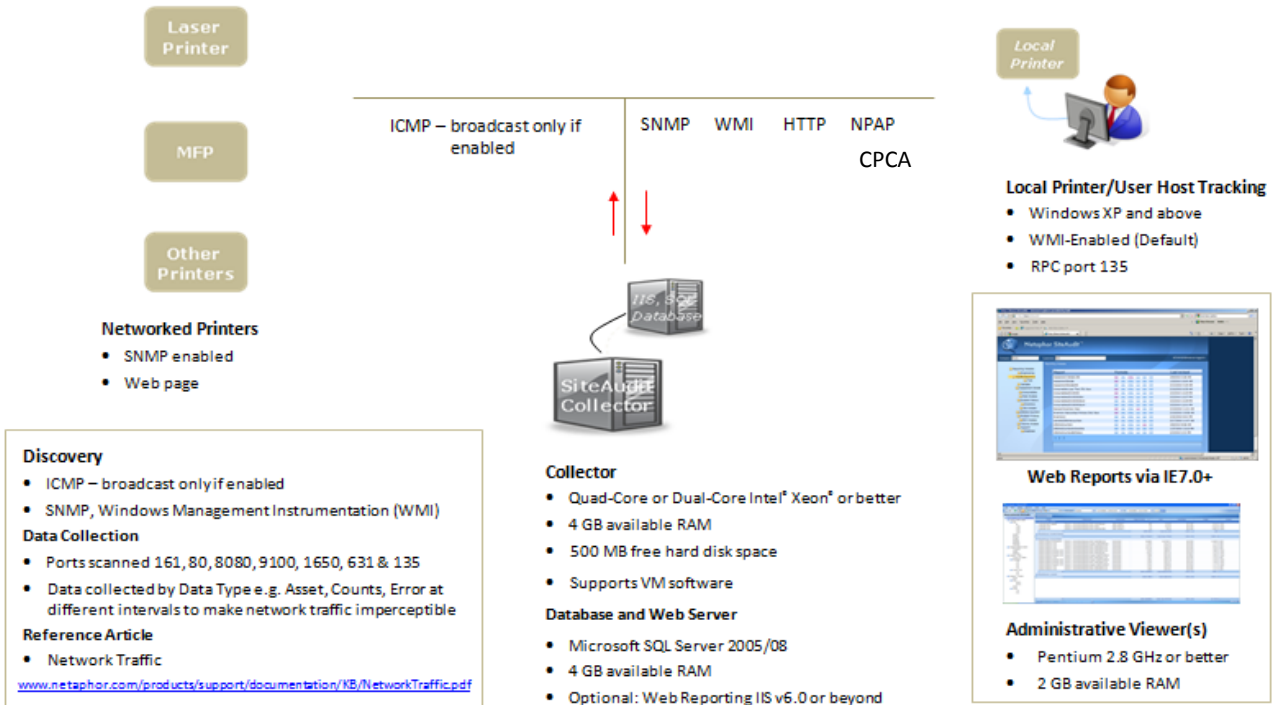
Operating System	Hardware	SQL Server
Windows XP with SP3/Vista/Windows 7	<ul style="list-style-type: none">• Dual Quad or better• 2 GB available RAM• 200 MB free hard disk space	SQL Server Express 2005/2008/2008R2

Note: To host web reports must support 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.

2. Database:

- If SQL Server is installed on the network, make sure it can be used and that there is a database for data collection.
- The minimum required privileges for database operations are Owner. Users with Owner privileges can update database schemas, backup and restore the database (from within SiteAudit) and discard the data. At least one person who will be using SiteAudit should have this privilege.

- ❑ To create a database (from within SiteAudit) the user must have sa privileges (if SQL security is being used) or administrator privileges if integrated security is being used.
- ❑ SQL Express 2008 supports database sizes up to 4GB whereas SQL Express 2008 R2 supports sizes up to 10GB



Netaphor Software Inc. – 2011

Windows Services

3. Windows services settings:

- ❑ Make sure that the services listed below are started or able to be started.

Service	Where needed	Startup type
COM+ Event System	SiteAudit Monitor Targets that need to be scanned	Automatic on servers Manual on workstations
Remote Access Auto Connection Manager	SiteAudit Monitor and SiteAudit Viewer	Manual
Remote Access Connection Manager	SiteAudit Monitor and SiteAudit Viewer	Manual
Remote Procedure Call (RPC)	SiteAudit Monitor and SiteAudit Viewer	Manual

Service	Where needed	Startup type
Remote Procedure Call (RPC) Locator	SiteAudit Monitor and SiteAudit Viewer	Manual
Remote Registry	SiteAudit Monitor	Automatic
Server	SiteAudit Monitor and 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 and SiteAudit Viewer	Automatic

- 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.

Discovery Configuration

4. Network discovery:

- Collect the list of networks over which discovery needs to be performed. The network address and mask are required for each network.
- Collect the list of networks over which discovery should NOT be performed. The network address and mask are required for each network.
- Collect the list of ranges that need to be included or excluded
- Decide whether broadcasts should be used. If broadcasts are not to be used add the broadcast addresses to the list of devices not to be scanned
- 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.

5. SNMP:

- Make sure that all needed community strings are available.
- 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.

6. 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.

7. Security:

- ❑ Check to see whether security software needs to be configured to white list SiteAudit to prevent false positives from being registered when SiteAudit is scanning the network and collecting data.

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 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:

Port	Protocol	Description
161	UDP	SNMP to see if SNMP is available. SNMP is used to collect data
80	TCP	HTTP to see if there is an embedded web server. HTTP is used to collect data
9100	TCP	Print protocol for printers, used to collect data
1650	TCP	Same as 9100
135	TCP/UDP	RPC, used to detect a Windows host for directly connected printers

Directly (Local) 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.