



Deployment Check List

In This Article:

- Platform Requirements
- Windows Settings
- Discovery Configuration

October 2007

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:

- Make sure that the platform requirements are as follows:

SiteAudit Monitor:

Operating System	Hardware
Windows 2003/2008 Server	<ul style="list-style-type: none">• Pentium 4 3.2 GHz or better• 4 GB available RAM• 200 MB free hard disk space

SiteAudit Viewer:

Operating System	Hardware
Windows XP with SP2	<ul style="list-style-type: none">• Celeron 2.8 GHz or better• 4 GB available RAM• 200 MB free hard disk space

SiteAudit Monitoring for > 250 printers requires Windows 2003/2008 server. For environments with < 250 printers Windows XP may be used.

2. Software:

- SQL Server 2005/2008 required for environments with > 250 printers
- SQL Server Express 2005/2008 may be used for environments < 250 printers
- .NET 3.5 Framework must be installed on all hosts where SiteAudit will be installed.

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.
- 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.

4. Other Platform/Environment Considerations

SNMP

- MUST be enabled on all of the networked printers that are to be managed by SiteAudit
- MUST not be blocked by a firewall
- Community strings accepted by the printer must be provided to SiteAudit

Job Tracking

- Job Log MUST be enabled. See <http://netaphor.com/products/support/documentation/kb/JobAnalysis.pdf> for details on how this can be done.
- Credentials MUST be provided.

Windows Services

5. 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
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

6. 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.

7. 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.

8. 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.

9. 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.