

## Local Printer Discovery

August 2011

### In This Article:

- Windows Firewall Settings
- COM Configuration

SiteAudit provides discovery and management of printers attached to Windows hosts via USB or Parallel ports. This operations document is about Windows Firewall settings to allow SiteAudit to manage these printers.

### Windows Firewall

By default Windows Firewall settings on Windows XP SP2, Windows 2003 SR1 (and above) do not allow SiteAudit to discover and manage printers attached to. Several settings need to be changed in order to allow this management. This document describes the manual process needed to make this possible. The steps outlined below could be combined in a script and pushed out to each host in the network using a tool such as Group Policy Management Console.

### Remote Administration/WMI Exceptions

**Description** Windows Firewall must be enabled on each host to allow Remote Administration.

**Default Option** This option is not enabled by default

**Steps** 1. Using the Command prompt

1. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. **netsh firewall set service RemoteAdmin enable**

For Windows 7 and newer operating systems, use the following command instead:

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

2. Using the Group Policy editor

1. Click **Start**, click **Run**, type **gpedit.msc**, and then click **OK**.
2. Under the **Local Computer Policy** heading, double-click **Computer Configuration**.
3. Double-click **Administrative Templates, Network, Network Connections**, and then **Windows Firewall**.

4. If the computer is in the domain, then double-click **Domain Profile**; otherwise, double-click **Standard Profile**.
5. Click **Windows Firewall: Allow remote administration exception**.
6. On the **Action** menu, select **Properties**.
7. Click **Enable**, and then click **OK**.

## DCOM

<b>Description</b>	Distributed COM (DCOM) must be enabled.
<b>Default Option</b>	This option is the default.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Click <b>Start</b> click <b>Run</b>, type <b>DCOMCNFG</b>, and then click <b>OK</b>.</li> <li>2. In the <b>Component Services</b> dialog box, expand <b>Component Services</b>, expand <b>Computers</b> and then right-click <b>My Computer</b> and click <b>Properties</b>.</li> <li>3. In the <b>My Computer Properties</b> dialog box, click the <b>Default Properties</b> tab.</li> <li>4. Check the box for <b>Enable Distributed COM on this computer</b>.</li> </ol>

## Launch Permissions

<b>Description</b>	Windows Firewall must allow the credentials being used to allow Remote Launch Permissions
<b>Default Option</b>	This option should be the default if the credentials of a user that is the member of the Local Administrators group is being used.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Click <b>Start</b> click <b>Run</b>, type <b>DCOMCNFG</b>, and then click <b>OK</b>.</li> <li>2. In the <b>Component Services</b> dialog box, expand <b>Component Services</b>, expand <b>Computers</b> and then right-click <b>My Computer</b> and click <b>Properties</b>.</li> <li>3. In the <b>My Computer Properties</b> dialog box, click the <b>COM Security</b> tab.</li> <li>4. Under <b>Launch and Activation Permissions</b>, click <b>Edit Limits</b>.</li> <li>5. In the <b>Launch Permission</b> dialog box, follow these steps if your name or your group does not appear in the <b>Groups or user names list</b>:             <ol style="list-style-type: none"> <li>1. In the <b>Launch Permission</b> dialog box, click <b>Add</b>.</li> <li>2. In the <b>Select Users, Computers, or Groups</b> dialog box, add your name and the group in the <b>Enter the object names to select</b> box, and then click <b>OK</b>.</li> </ol> </li> </ol>

6. In the **Launch Permission** dialog box, select your user and group in the **Group or user names** box. In the **Allow** column under **Permissions for User**, select **Remote Launch** and select **Remote Activation**, and then click **OK**.
7. When connecting to a target machine with a **local account** in Windows Vista and later, the user must explicitly be given full allow **Launch and Activation Permission**.
8. When connecting to a to a target machine with a **domain account** in Windows Vista and later, the domain user must be either explicitly added to the **Administrators** group of the machine, or a member of the domain's **Domain Admins** (and the Domain Admins group is a member of Administrators). Verify the Administrators group has full **Launch and Activation Permission** allowances.

## Access Permissions

**Description** Windows Firewall must allow the credentials being used to allow Remote Access Permissions. These permissions are only required if the host where SiteAudit is running is in a different domain or workgroup from the target domain or workgroup

**Default Option** This option is not the default.

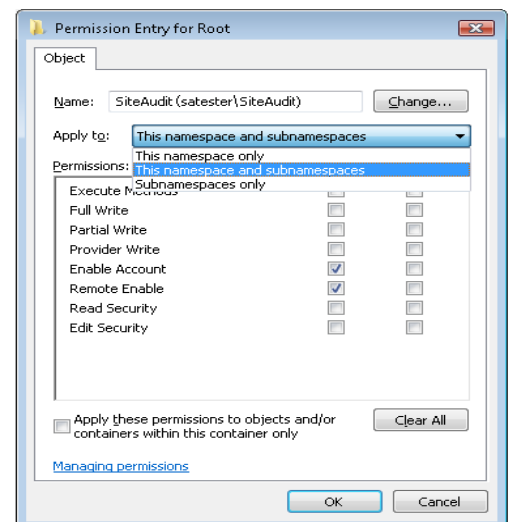
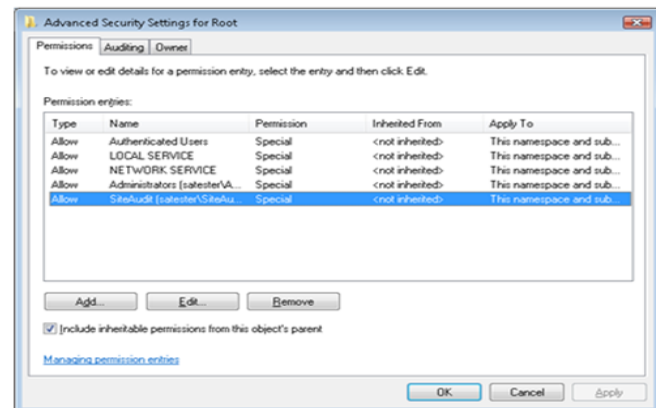
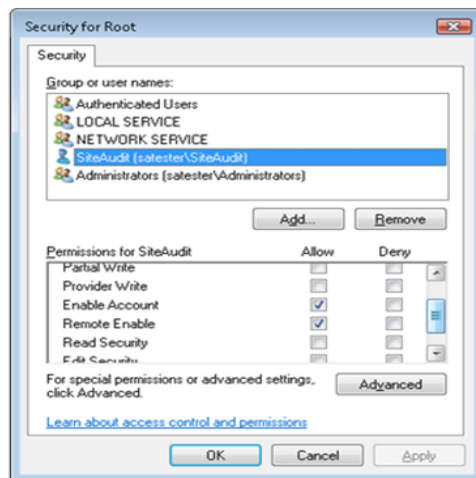
- Steps**
1. Click **Start** click **Run**, type **DCOMCNFG**, and then click **OK**.
  2. In the **Component Services** dialog box, expand **Component Services**, expand **Computers** and then right-click **My Computer** and click **Properties**.
  3. In the **My Computer Properties** dialog box, click the **COM Security** tab.
  4. Under **Access Permissions**, click **Edit Limits**.
  5. In the **Access Permission** dialog box select **ANONYMOUS LOGON** name in the **Group or user names** box. In the **Allow** column under **Permissions for User**, select **Remote Access**, and then click **OK**.

## Namespace Permissions

**Description** WMI must allow the credentials being used to have full access.

**Default Option** This option should be the default if the credentials of a user that is the member of the Local Administrators group is being used.

- Steps**
1. In the **Control Panel**, double-click **Administrative Tools**.
  2. In the **Administrative Tools** window, double-click **Computer Management**.
  3. In the **Computer Management** window, expand the **Services and Applications** tree and double-click the **WMI Control**.
  4. Right-click the **WMI Control** icon and select **Properties** and then select the **Security** tab.
  5. Click on the **Security** button.



6. Ensure that the credentials which you will be using (typically the local Administrators group) will have full control, and that the namespace privileges apply to the current and

all sub namespaces. **Remote Enable** must be selected as a minimum. When connecting to a target machine with a **local account** in Windows Vista and later, the user must be listed explicitly.

## Remote Credentials

**Description** On Windows XP Professional make sure that remote logons are not being coerced to the GUEST account ("Force Guest", which is enabled by default computers that are not attached to a domain).

**Default Option** This option is not the default.

- Steps**
1. Click **Start** click **Run**, type **Secpol.msc**, and then click **OK**.
  2. Select **Local Policies** and then select **Security Options**.
  3. Find the setting **Network access: Sharing and security model for local accounts**. Make sure it is set to **Classic**.
  4. If you change the setting you must restart your computer.