

Set Up a Client Computer

The instructions in this topic presuppose that your network runs Active Directory and that you use Group Policy to manage your network. For more information about Group Policy, see the Group Policy home page at <http://go.microsoft.com/fwlink/?linkid=109523>.

You can configure one or more computers by including them in a Group Policy object (GPO). Microsoft recommends that you create a new GPO that contains only Windows Server Update Services (WSUS) settings. Link this WSUS GPO to an Active Directory container appropriate for your environment. In a simple environment, you link a single WSUS GPO to the domain. In a more complex environment, you might link multiple WSUS GPOs to different organizational units (OUs).

Important

Microsoft recommends that you do not edit the Default Domain or Default Domain Controller GPOs.

The following four procedures are involved in setting up client computers:

- Load the WSUS Administrative Template.
- Direct the computers to the WSUS server.
- Configure the behavior of Automatic Updates.
- Set the contact frequency between computers and the WSUS server.

▶ To load the WSUS Administrative Template

1. In Group Policy Object Editor, right-click either of the **Administrative Templates** nodes. Click **Add/Remove Templates**.
2. Click **Add**.
3. In **Policy Templates**, click **wuau**, and then click **Open**.
4. Click **Close** to dismiss the dialog box.

▶ To direct the computers to the WSUS server

1. In Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the **Details** pane, double-click **Specify intranet Microsoft update service location**.
3. Type the URL of the WSUS server in both **Set the intranet update service for detecting updates** and **Set the intranet statistics server**. For example, type **http://servername** in both text boxes, where *servername* is the name of your WSUS server.
4. Click **OK**. After directing the computers to the WSUS server, you should configure the behavior of Automatic Updates.

Note

A client computer can be set to communicate with only one WSUS server at a time. If you later specify a different WSUS server, the client computer stops contacting the first WSUS server. However, the client computer will remain on the list of computers and computer groups on the first WSUS server, which will report the last time the client computer contacted it. To remove the computer from the WSUS server, see [Remove a Computer from a WSUS Server](#).

▶ To configure the behavior of Automatic Updates

1. In Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the **Details** pane, double-click **Configure Automatic Updates**.
3. In the **Properties** for **Configure Automatic Updates**, on the **Setting** tab, select **Enabled**, and then select one of these options from the **Configure automatic updating** drop-down list:
 - **Notify for download and notify for install**. This option notifies a logged-on

Think it is ↓
on WSUS server?
← can't find on regular Windows client computer

administrative user before the download begins and before the installation of the updates.

- **Auto download and notify for install.** This option automatically begins downloading updates and then notifies a logged-on administrative user before installing the updates.
- **Auto download and schedule the install.** This option automatically downloads and installs updates. You must also set the day and time for the installation.
- **Allow local admin to choose setting.** This option allows local administrators to use **Automatic Updates** in Control Panel to select a configuration option of their choice. For example, they can choose their own scheduled installation time. Local administrators are not allowed to disable Automatic Updates. The **Allow local admin to choose setting** option appears only if Automatic Updates has updated itself so that it is compatible with WSUS.

► **To set the contact frequency between computers and the WSUS server**

1. In Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane of Group Policy Object Editor, double-click **Automatic Updates detection frequency**, and set the option to **Enabled**.
3. The exact time between contacts will actually be the number of hours you specify here minus 0–20 percent of the hours specified. For example, if this policy is used to specify a 20-hour contact frequency, then all clients to which this policy is applied will check for updates anywhere between 16 and 20 hours. If the status is set to **Disabled** or **Not Configured**, Windows will check for available updates at the default interval of 22 hours.

Additional considerations

- To complete this procedure, you must have Edit setting permission to edit a GPO. By default, members of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group have Edit setting permission to edit a GPO.
- If you want a WSUS server to receive updates, you must also treat it like a client computer. Therefore, you should perform these procedures for the WSUS server; for example, in reference to the procedures in this topic, you would include the server in the domain GPO.
- WSUS client computers require that Automatic Updates be WSUS compatible. In most cases, you do not need to worry about this requirement. Automatic Updates will update itself when the client computer makes its first contact with the WSUS server (if you have performed a default server installation, WSUS is installed on the default Web site). However, if you are running the version of Windows XP without any service packs, Automatic Updates will not be able to update itself automatically.
- Administrator-defined configuration options (whether set with Group Policy for a domain-based GPO in an Active Directory environment, or by configuring the registry or Local GPO in a non-Active Directory environment) always take precedence over user-defined configuration options. When you use administrative policies to configure Automatic Updates, the Automatic Updates user interface is disabled on the client computer.

See Also

- [Set Up and Manage Computers and Groups](#)
-

up to date: micky

SEARCH:
type: gpedit.msc

go to :
Under Computer configuration
ADMIN TEMPLATES
WINDOWS Components
WINDOWS UPDATE

Check for the
SPECIFY INTRANET LOCATION
type://ntcserver
(In both)

Go Through any other, hit EXPLAIN for definitions.

Last step:

Bring up CMD

type: wuauclt.exe /detectnow
wuauclt.exe /reportnow

not necessarily
in this order
Hilary typed
When we were doing
a remote
connection
on engine room
computer

> gpupdate

> wuauclt

> wuauclt

/force

/reportnow

/detectnow

product ID 55041-008-168 6983-860077

remote desktop connection from Hilary

Windows Key - MKXHM-

26089-6 MF2W

HBRRD

harpo

Windows updates

Specify intranet ms update service location
intranet update server

<http://ntcserver.ship.atlantis.who.edu>

set intranet statistics server:

<http://ntcserver.ship.atlantis.who.edu>

product ID 00371-619-
Alvinmech 8083943-
85866
↑ not windows updating