Make sure automatic updates is enabled:
Enable automatic updates

Set up WSUS server:
Log in > click on Manage in server manager > add Roles and Features > click next > select role-based or feature-based installation > next > choose which server you want to be the WSUS server > next > select Windows Server Update Services > click on Add Features > next > retain defaults > next > next > leave defaults and next > on content location page, choose a valid location to store updates (you can create a folder for the WSUS updates called “WSUS_database” if it helps) > next > in the Web Server Role (IIS) retain defaults and next > confirm installation selections and install > launch post-installation tasks > once successfully configured you can close it > Server Manager will want you to restart, so restart when ready

ALTERNATE WSUS INSTALL (POWERSHELL):
Open powershell > Get-WindowsFeature > Install-WindowsFeature > **Install-WindowsFeature -Name UpdateServices, UpdateServices-WidDB, UpdateServices-Services, UpdateServices-RSAT, UpdateServices-API, UpdateServices-UI**

Configure firewall to allow WSUS updates:
Open firewall > create inbound rules to allow ports 80 (HTTP) and 443 (HTTPS) to allow updates to go through WSUS > if using WSUS 6.2 and later (at least Windows Server 2012) then allow ports 8530 (HTTP) and 8531 (HTTPS) in the firewall rule

Configuration wizard for WSUS:
Server manager > dashboard > tools > click on Windows Server Update Services > do not join microsoft update improvement program > next > synchronize updates with microsoft update > next > if you’re not using a proxy server then you can just skip proxy settings > on the Connect to Upstream Server page, click start connecting > click next when it connects > on the choose languages page, choose languages for systems you know need to have a specific language, or just English if you don’t know if you need any extra languages besides this one > In the Choose Products page, review over which windows products you want updates for > on the Choose Classifications page, choose update classifications you want and hit next > manually sync on setting sync schedule > next > begin initial synchronization > finish

Creating WSUS computer groups:
Open WSUS Administration console > update services > expand WSUS server > expand Computers > right click All Computers > click on add computer Group > make a name for the computer group > add computers you want to the group > right click the computer names you selected and click Change Membership > in the Set computer group membership dialog box > select the test group and hit ok

Configure client updates:
If using an environment with active directory service, you can use Group Policy Objects or create one.
If using an environment without active directory, you can use the Local Group Policy editor to configure automatic updates and point to client computers.

To approve and deploy WSUS updates
On the WSUS Administration Console, click Updates. In the right pane, an update status summary is displayed for All Updates, Critical Updates, Security Updates, and WSUS Updates.
In the All Updates section, click Updates needed by computers.
In the list of updates, select the updates that you want to approve for installation in your test computer group. Information about a selected update is available in the bottom pane of the Updates panel. To select multiple contiguous updates, hold down the shift key while clicking the update names. To select multiple noncontiguous updates, press down the CTRL key while clicking the update names.
Right-click the selection, and then click Approve.
In the Approve Updates dialog box, select your test group, and then click the down arrow.
Click Approved for Install, and then click OK.
The Approval Progress window appears, which shows the progress of the tasks that affect update approval. When the approval process is complete, click Close.

To configure Automatic Approvals
In the WSUS Administration Console, under Update Services, expand the WSUS server, and then click Options. The Options window opens.
In Options, click Automatic Approvals. The Automatic Approvals dialog opens.
In Update Rules, click New Rule. The add Rule dialog opens.
In add Rule, in Step 1: select Properties, select any single option, or combination of options from the following:

When an update is in a specific classification
When an update is in a specific product
Set a deadline for the approval

In Step 2: edit the properties, click each of the options listed, and then select the appropriate options for each.
In Step 3: Specify a name, type a name for your rule, and then click OK.
Click OK to close the Automatic Approvals dialog.

WSUS detection commands:
Command prompt commands for refreshing what servers/computers need updates

```
Wuaclt.exe /detectnow
Wuaclt.exe /reportnow
```

Add-WsusComputer

Approve-WsusUpdate

Deny-WsusUpdate

Get-WsusClassification

Get-WsusComputer

Get-WsusProduct

Get-WsusServer

Get-WsusUpdate

Invoke-WsusServerCleanup

Set-WsusClassification

Set-WsusProduct

Set-WsusServerSynchronization