SECMON1

Information Security Guideline

Operating System Patching

THIS PAGE INTENTIONALLY LEFT BLANK

Operating System (OS) patching refers to applying updates to operating systems. It is absolutely critical for ensuring system security. Time is of the essence in patching. It is ideal to apply patches within 48 hours of release.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what operating system patching is and why it is an essential security measure.

In this document we are going to provide some basic operating system patching steps for the most consistently vulnerable operating systems (Microsoft and Apple) as well as provide you with some interesting and important links where you can educate yourself further on this topic and discuss other available options.

There are also some vendor-provided operating system patch management solutions available. Below are just a few of them and by no means is it an exhaustive list:

- Cloud Management Suite
- Kaseya VSA
- SolarWinds Patch Manager
- Ivanti
- Automox

Implementation Guidance

When patching, organisations may be concerned about the risk of a patch breaking systems or applications and any outage this may cause. While this is a legitimate concern, and should be considered when deciding what actions to take in response to security vulnerabilities, many vendors perform thorough testing of all patches prior to their release to the public. Often the immediate protection afforded by patching an extreme risk security vulnerability far outweighs the impact of the unlikely occurrence of having to roll back a patch

The following are the recommended deployment timeframes for patches based on the outcome of risk assessments for security vulnerabilities:

Extreme Risk: Within 48 hours of a patch being released

High Risk: Within 2 weeks of a patch being released

Moderate-Low Risk: Within 1 month of a patch being released

In situations where resources are limited, organisations are encouraged to prioritise the deployment of patches. For example, patches could be applied to workstations of high risk users (eg, workstations used by executive officers and their support staff, HR staff, FOI staff and public relations staff) within 48 hours, followed by all other workstations within 2 weeks.

Note: Some patching may require you to restart your computer. Most system restarts after patches can be deferred for up to 3 days.

It is advised to restart your computer at least once per week to allow patch installations to complete.

Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

How-To Guide

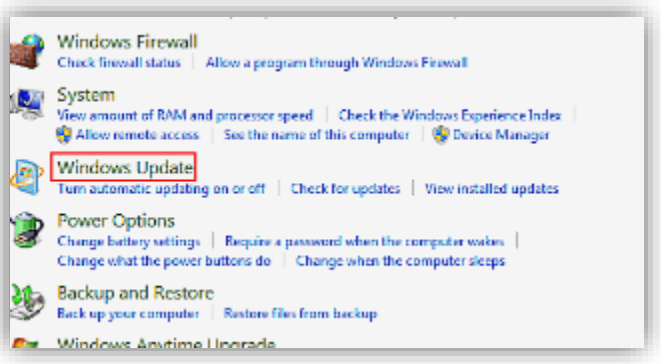
Microsoft Security Updates

Security updates are released on the second Tuesday of each month by Microsoft. Most computers are configured to receive these patches automatically via Windows Update, and it is strongly recommended to leave this feature enabled. However, companies can possibly wait about a week before applying them remotely if manual updating is preferred.

How to Get Updates in Windows 7 and 8

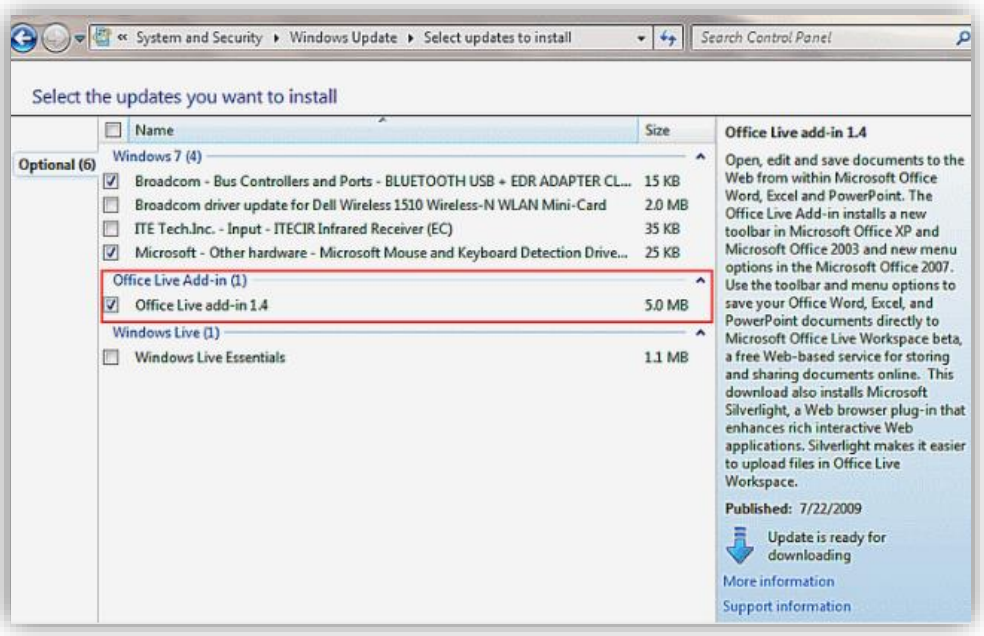
1. Click the **Start** button, then click **Control Panel** on the right side of the menu. This brings up the main Control Panel screen. (**Note**: In Windows 8, you will need to select **Settings** before the Control Panel option is displayed)
2. Click **System and Security** (outlined in red)

3. Click on **Windows Update** (outlined in red).



4. Windows Update's main screen gives you a number of important bits of information. First, in the middle of the screen, it tells you if there's any "important", "recommended" or "optional" updates. The meanings behind these are as follows: Important Updates: Normally these are fixes for security issues, or to fix a problem that could cause system instability. They should be installed immediately. Recommended Updates: These are often additional new features or functionality. It's a good idea, but not a necessity, to install them. Optional Updates: These are often take-or-leave updates. They can be driver updates to help some devices work better with Windows or they could be trial software from Microsoft.

5. Clicking on the link for available updates brings up the screen below. You can choose to install some, all or none of the options by clicking the check-box to the left of them. If you are unsure of what an update does, click on it and a description will appear in the pane (in blue) on the right. This allows you to make a more informed decision on what to install (or not).

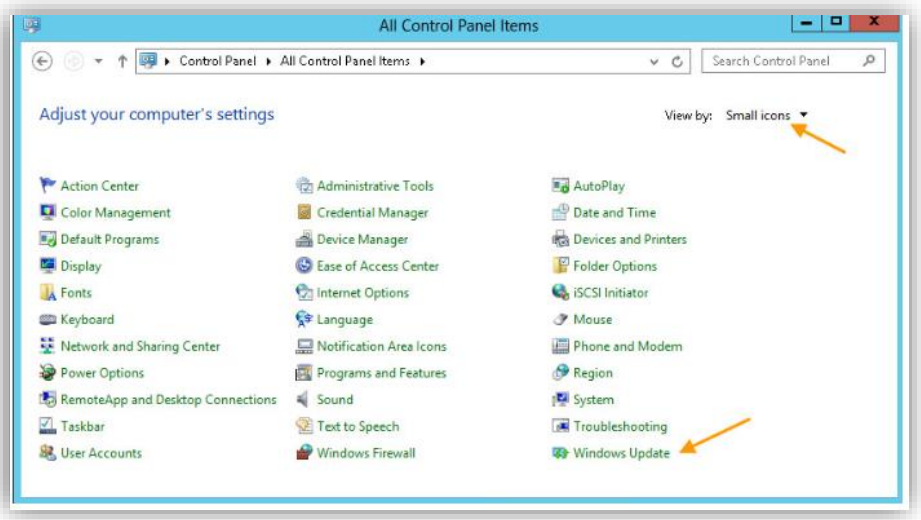


6. When the updates you choose to install are selected, click **OK**.

For an FAQ on updates for Windows 7-8, please go here.

How to Get Updates in Windows Server 2008 or Windows Server 2012

1. Log onto your Windows server via Remote Desktop (or if you are able to directly access your server, do so)
2. On a Windows 2008 Server, click **Start > Control Panel > Windows Update**. If necessary, switch the **View** settings to **Small Icons**
3. On a Windows 2012 Server, press the Windows key and type **Control Panel**. If necessary, switch the **View** settings to **Small Icons**
4. Click **Windows Update**



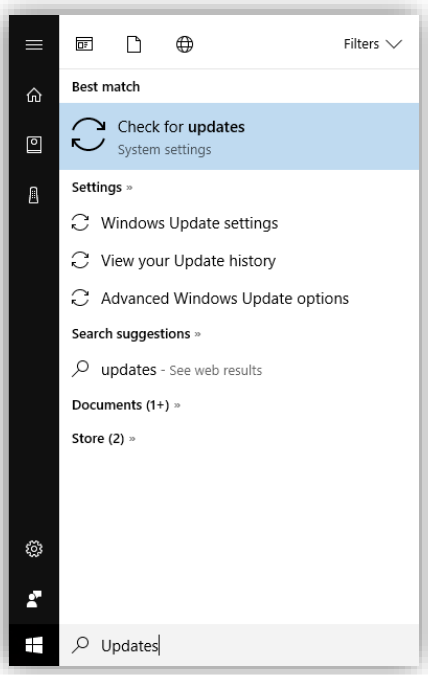
5. Click Check online for updates from Microsoft Update
6. Click on the Install now button
7. Windows will download and begin installing updates.

Note: Depending on the number of updates needed, your server may need to restart more than once.

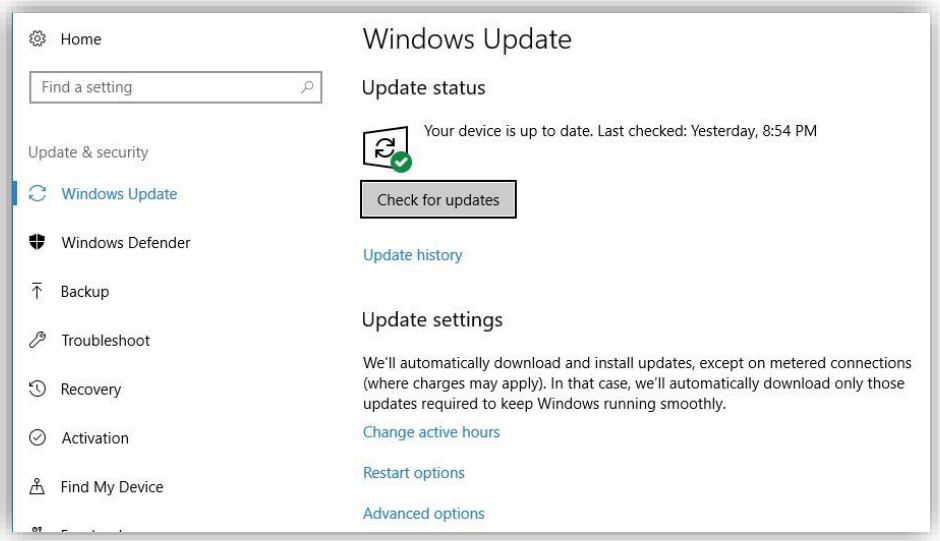
For an FAQ on updates for Windows Server 2008 and 2012, please go here.

How to Get Updates in Windows 10.

1. Click the Start menu and type Updates in the search bar



2. Click **Check for updates**

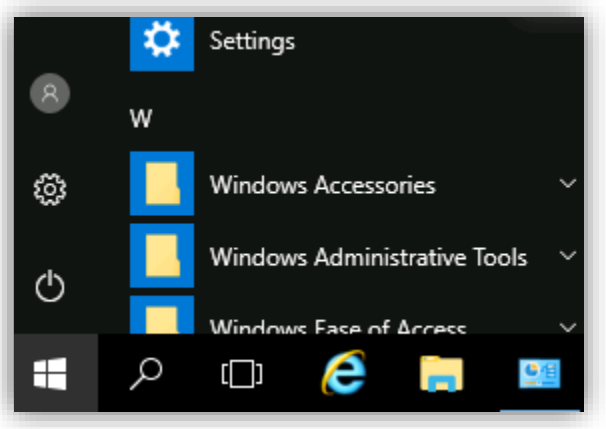


3. If there are updates to install, they will be installed automatically. In Windows 10, Microsoft has taken away the ability to pick and choose which updates to install (or not). However, you can change when updates are checked and when restarts to apply them occur. For more info on this aspect, please go here.

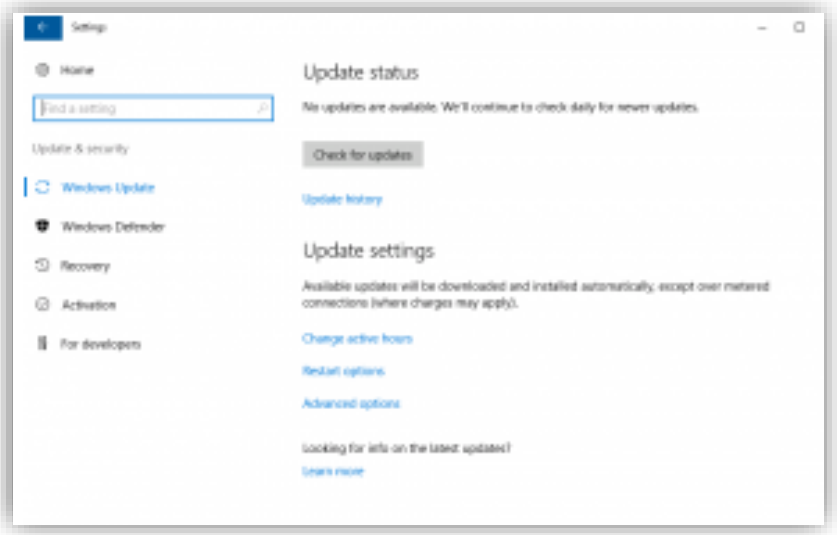
For an FAQ on updates for Windows 10, please go here.

How to Get Updates in Windows Server 2016

1. Log onto your Windows server via Remote Desktop (or if you are able to directly access your server, do so) and select **Settings**



2. Click **Update & Security**, which will open the following screen.



Everything regarding updates can be done via this screen. You have the option to **Check for updates**, which will check for the latest updates and automatically download and install them. If some updates require reboot, Windows will schedule it accordingly. It is possible to set these

hours by selecting **Change active hours** where a timeframe will be given in which Windows will not reboot the device automatically. It is possible to further customize the day and time for reboot utilizing the **Restart options** link.

Further information on Windows Server 2016 patching can be found here.

Apple Security Updates

OS X and security updates from Apple are usually deployed within a few days of release. OS X update versions may be delayed for compatibility testing. You can manually install Apple software updates without interfering with the managed update process.

Further information on Apple updates can be found here.

How to Get Updates in Mac OS X

1. Open the App Store app on your Mac. The App Store app button appears as the following:

2. Click **Updates** in the toolbar. If updates are available, click the **Update** buttons to download and install them.

Final Note

SECMON1 are available to review your operating system patching strategies with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement operating system patching for your company.

Please feel free to visit our website at www.secmon1.com.

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com.