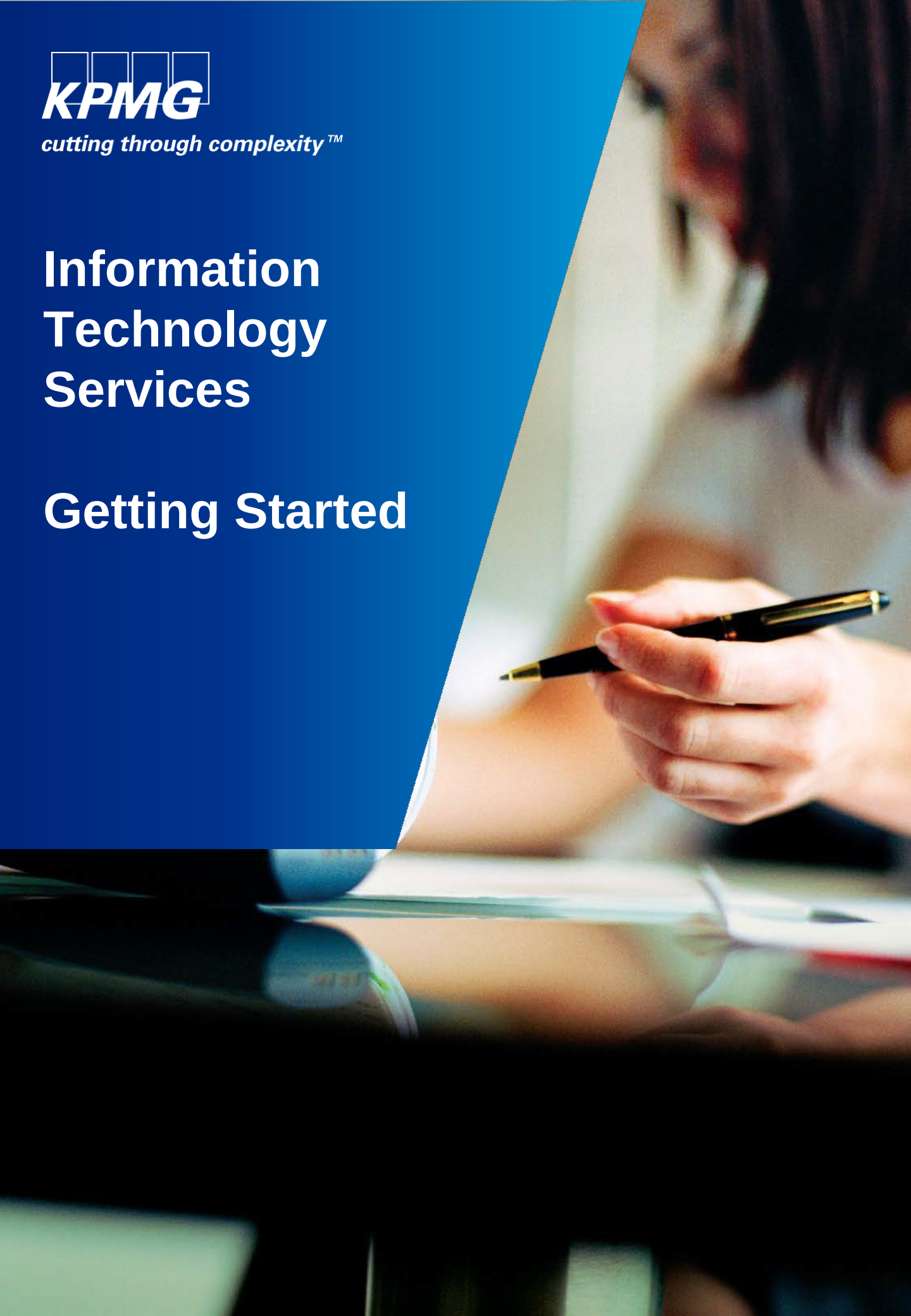
KPMG

cutting through complexity™

Information Technology Services

Getting Started



KPMG
cutting through complexity™

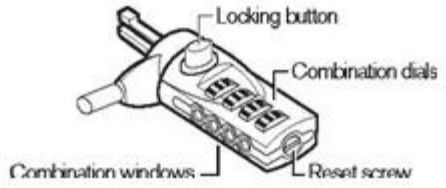
CONTENTS

Using of Cable Lock

The Cable Lock is a serialized lock with a pre-set number combination and it provides a computer security solution for complete asset protection. It is 6.5 feet of cut-resistant, galvanized steel cable that loops around any secure object and easily attached to your laptop lock slot.

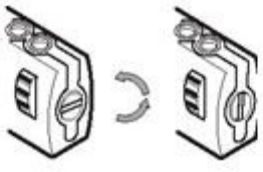
Setting the combination code

1. Locate the combination dials and windows on the lock.

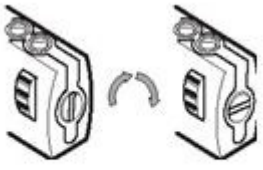


Cable Lock

2. If you are setting the combination for the first time, the preset combination is set as "0000". The combination appears in the windows.
3. Using a small flat-head screwdriver or similar object, push in and rotate the reset screw 90 degrees clockwise so that the screw's groove is positioned horizontaly.



Locking the combination lock



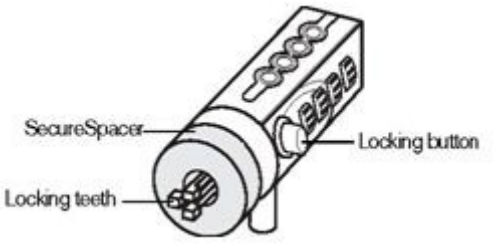
Unlocking the combination lock

4. Using the dials enter the new combination.
5. Rotate the reset screw 90 degrees counter clockwise, back to its original vertical position, to save the new combination.
6. Record the combination and place it in secure, easy-to-find place.

Locking your cable lock to your notebook computer

Tip: Hold the Cable Lock with both hands for additional stability while inserting or removing the lock.

1. Using the dials enters the correct combination. The combination appears in the windows.



NOTE: For the locking button to depress completely you must enter the correct combination.

2. Press and hold the locking button to align the locking teeth.
3. Insert the Cable Lock into your notebook computer's lock slot and release the locking button.
4. Turn the dials to conceal your combination.

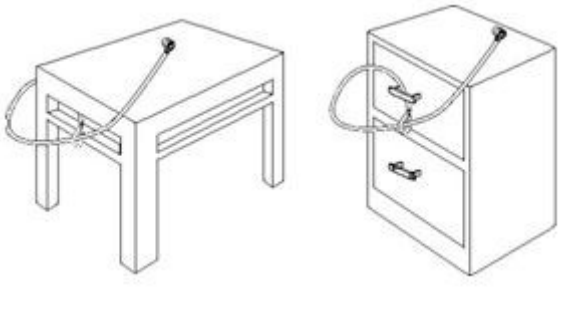
Note: You are responsible for the security of the laptop you are entrusted with. A routine check will be conducted by ITS randomly. Users who leave their notebook unattended will be confiscated and action will be taken.

Testing the combination and place it in secure, easy-to-find place.

1. Turn the dials to disguise the combination.
2. Return to the combination you set.
3. Check that the locking button depresses completely.

Securing your cable lock

1. Select an object in the room to which you will secure your notebook computer with the Cable Lock. Choose a large, heavy piece of furniture such as a table or desk, or an immovable fixture such as a closet hanging bar. Take the looped end of the cable and wrap it around the selected object.
2. Feed the lock through the looped end of the cable as shown..



NOTE: Wrap the cable around a part of the object that will deter an intruder from slipping the cable off (for example, a table or desk leg with a cross bar or a drawer handle).

Boot Up Your Machine

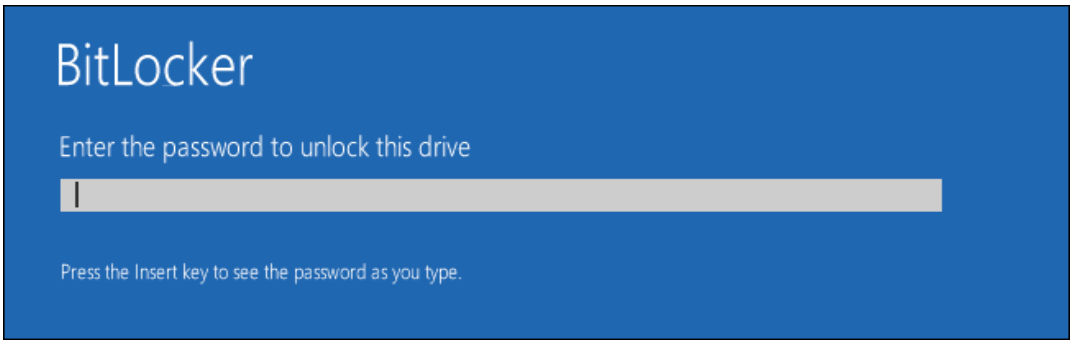
BitLocker encryption protect your data in the event the computer is lost or stolen. It encrypts the hard drive so that when someone has physical access to the drive, the drive is unreadable.

BitLocker is pre-installed in all KPMG computers. You will see the BitLocker logon screen when computer starts.

Using the software

1. Power on / Restart the computer.

2. The BitLocker login screen will appear.



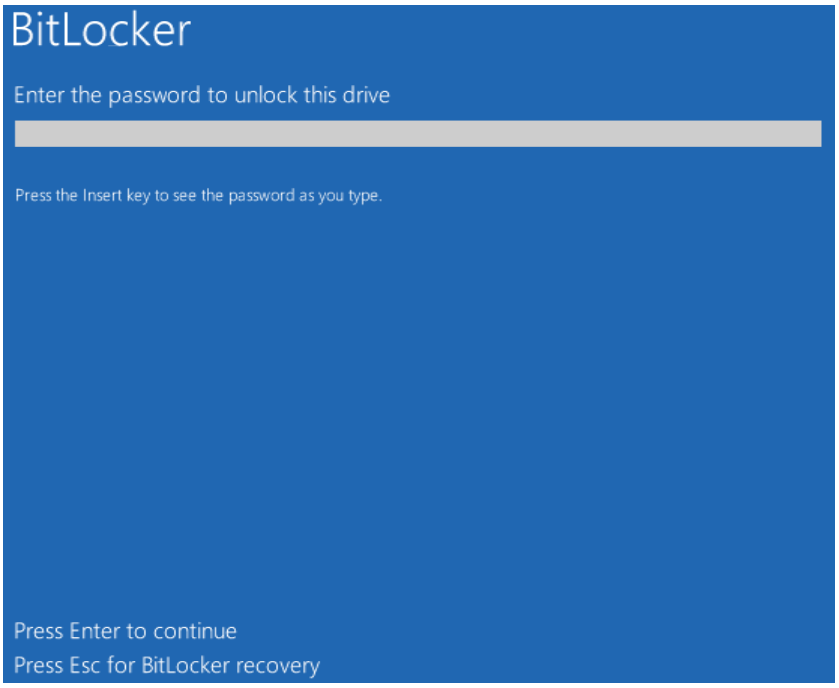
3. Enter your password.
   Tip: If this is your first logon, your password is 2266. Press "ENTER".

4. After that, you are require to change your BitLocker password in the Windows.

Continue to <Reset BitLocker Pin> guide on page 10 for instructions on how to change your BitLocker password …

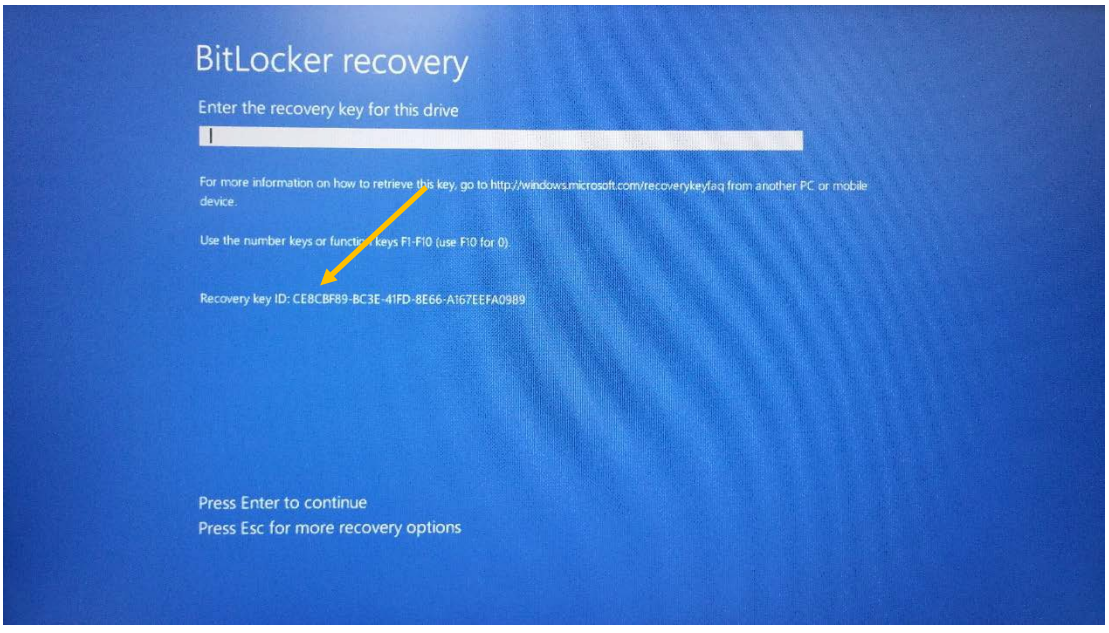
Forgot password/locked out

1. Press Esc key for BitLocker recovery



2. Call BSG Hotline (6213 2266) and press Option 1 for ITS Call Centre.

3. Provide the first 8 characters of the Recovery key ID from your screen to the engineer.



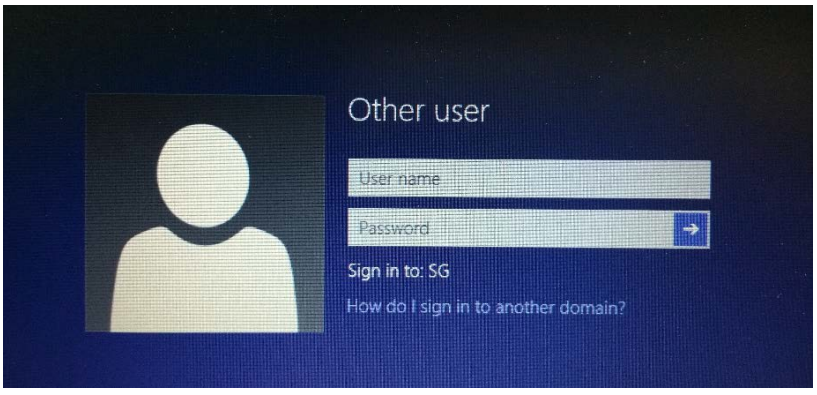
Log on to KPMG network

To gain access to the KPMG network, you will need to have a logon username and password. On your first day of work in KPMG, you will be provided with a default *username* and default *network password.*

How to login to KPMG network

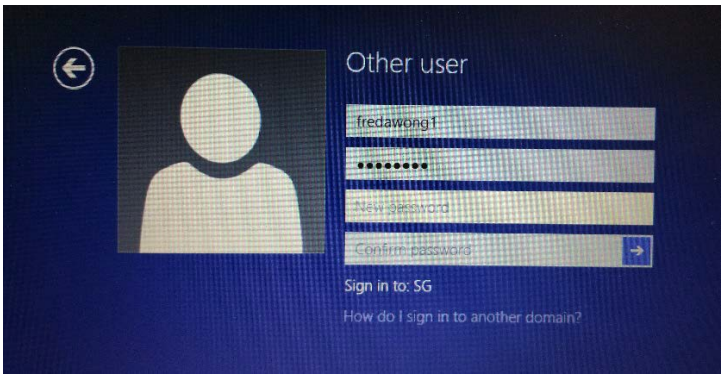
Tip: You are required to plug-in a network cable (a.k.a LAN Cable) for the first login.

1. Enter your username and password provided to you by the IT administrator.



2. If you are logging into the windows for the first time, system will prompt you to change the password.

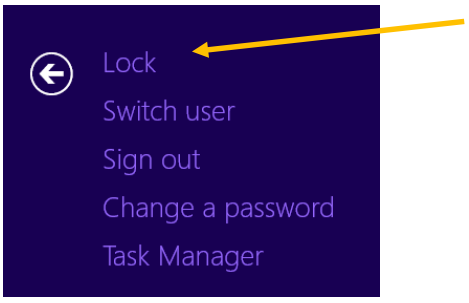
3. At the change password screen, enter your old password, new password and confirm new password. Press "ENTER" when you are done.



Secure your computer

Please make sure you secure your computer when you are away from your computer. To secure your computer, please follow below steps:-

1. Press "CTRL + ALT + Delete" button on your keyboard.
2. Click on "Lock". Your computer system is now locked, preventing everyone except you from unlocking your system and viewing any open files or programs.



Password and security guide

To ensure security, passwords must be used carefully. These recommendations will help protect your password.

- Never write down your password.
- Never share password with anyone.
- Never use your network logon password for another purpose.
- Change your network password every 180 days.
- Change your password immediately if you think it has been compromised. You should also be careful about where you save your password on your computer. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember your password. Do not select that option.

Password Tips

- Account will be lockout after 3 bad attempts.

Continue to Password Tips guide on page 9 for more tips…

Password Tips

This guide will help you create good, strong passwords that are hard to guess or break. Read through the following tips and check your own password

Password Tips

- Be at least eight characters long.
- Contain characters from each of the following 4 groups:-
  - ✓ Letters (Uppercase) – E.G: A, B, C, …
  - ✓ Letters (Lowercase) – E.G: a, b, c, …
  - ✓ Numeric – E.G: 0, 1, 2, 3, …
  - ✓ Symbols – E.G: !, @, #, $, %, ^, &, …
- Password is case-sensitive.
- Expire in 60 days.
- After changing your password, you need to wait for 24 hours before you can change it again.

Creating strong passwords

Good computer security includes the use of strong passwords for your network logon on your computer. For a password to be strong and hard to break, it should

- Long enough to be hard to guess.
- Not a famous quotation from literature and etc.
- Hard to guess by intuition – even by someone who knows the user well.
- Not contain your name or username.

What you should know?
What action to be taken before password expired?

- Change your password immediately if you are prompt to do so.
- Change your password if you know it going to expire soon.

Why change password before it expired?

- It is not possible to change password outside of office (Unless you are connected to VPN)
- Reset of password by the administrators will not be possible when you have:-
  - ✓ Forgotten your password outside the office or
  - ✓ Password is expired outside the office.

Tip: Changing of password can only be done in the office as windows password needs to be synchronized using the office network.

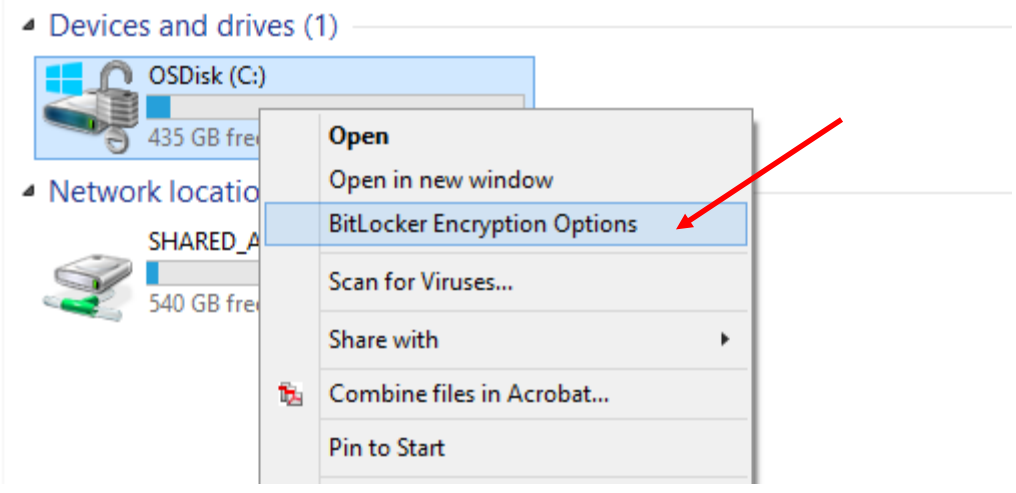
Reset Bitlocker PIN

Enabling BitLocker on computer is greatly beneficial to protect hard drive data. Consequently, a large number of people use BitLocker to encrypt the computer hard disks. This guide will show you how to change BitLocker password on Windows 8 by use of the following steps.

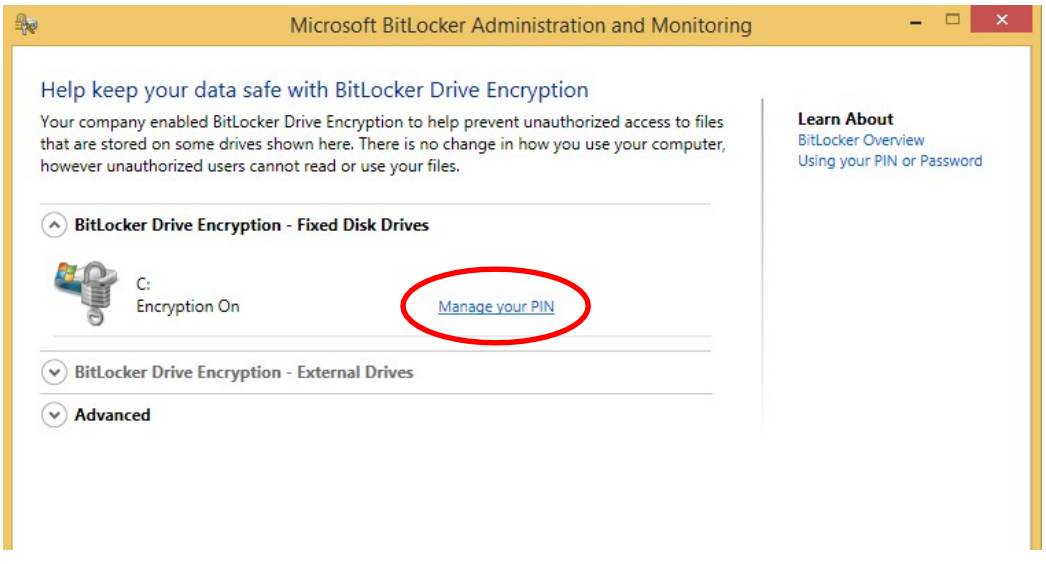
To reset your Bitlocker Pin

1. Enter Desktop from the Start menu, then click on **File Explorer** icon located on your system bar.

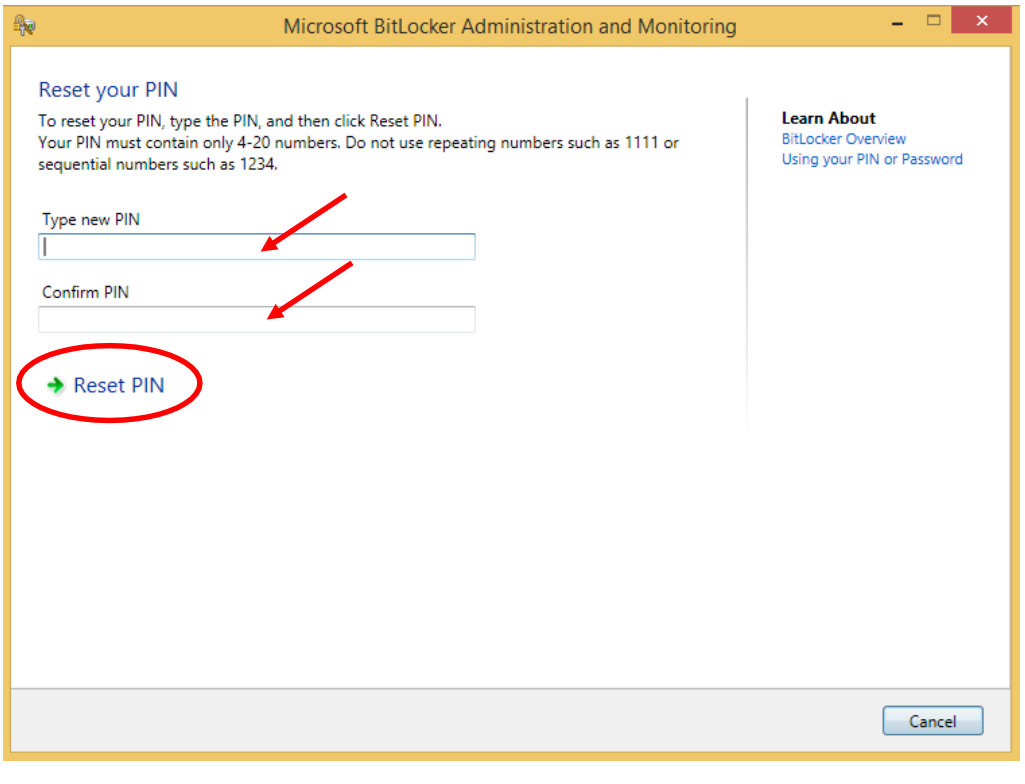
2. Right-click on **OSDisk (C:)** Drive and select **Bitlocker Encryption Options**.



3. Click on **Manage your PIN**.



4. Type and Confirm New Pin, then press **Reset PIN**. (Note: The PIN must contain only 4 – 20 numbers)



5. Click **Close**. Your new PIN is now set.

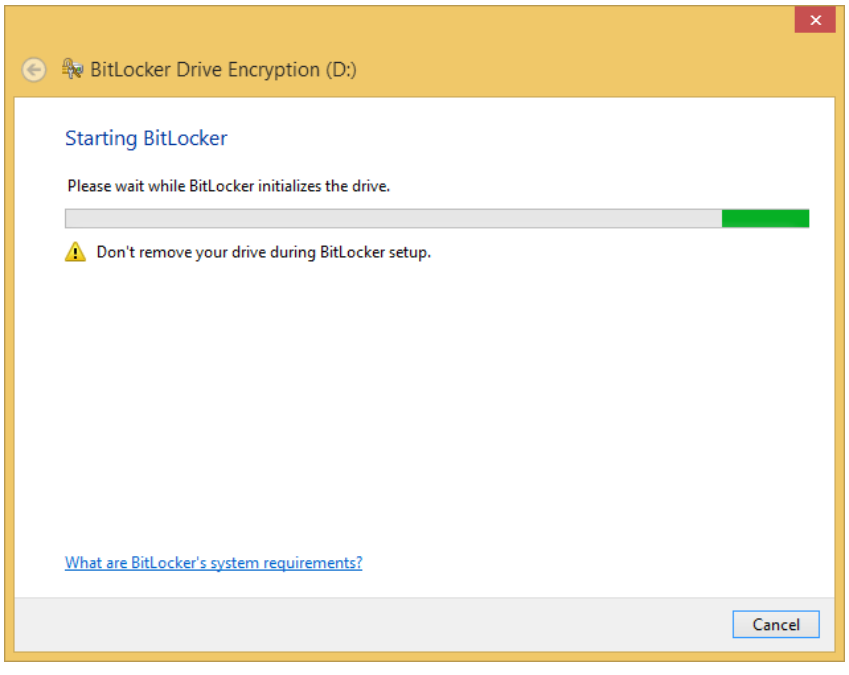
Using External Drive

When you first connect an external device such as a thumb drive to your KPMG machine, you will be prompt to encrypt your device with BitLocker To Go, and you can set it to unlock by using a password.
Password encryption requires that you enter an 8-character password during the setup process. This password does not expire. You will not need to reset or change the password unless you want to.

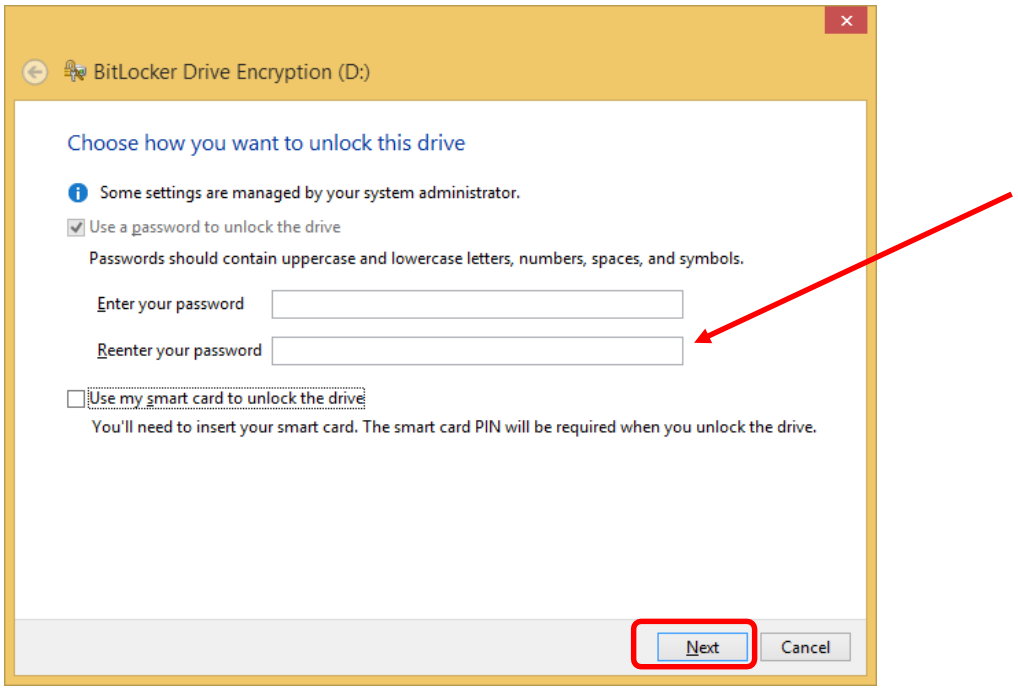
Encrypt your portable drive

1. First, plug in your portable drive. Once Windows recognizes it, you will receive the following prompt.

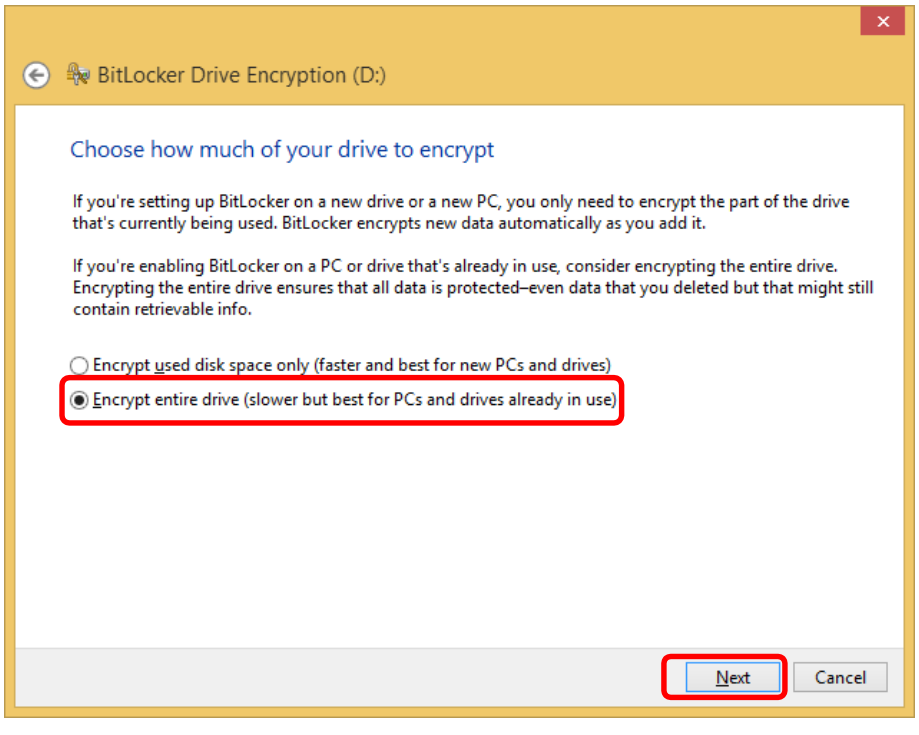
2. Choose the first option "**Encrypt this drive using BitLocker Drive Encryption**" in order to save or copy files from the portable drive. The BitLocker will then starts initializing the drive.



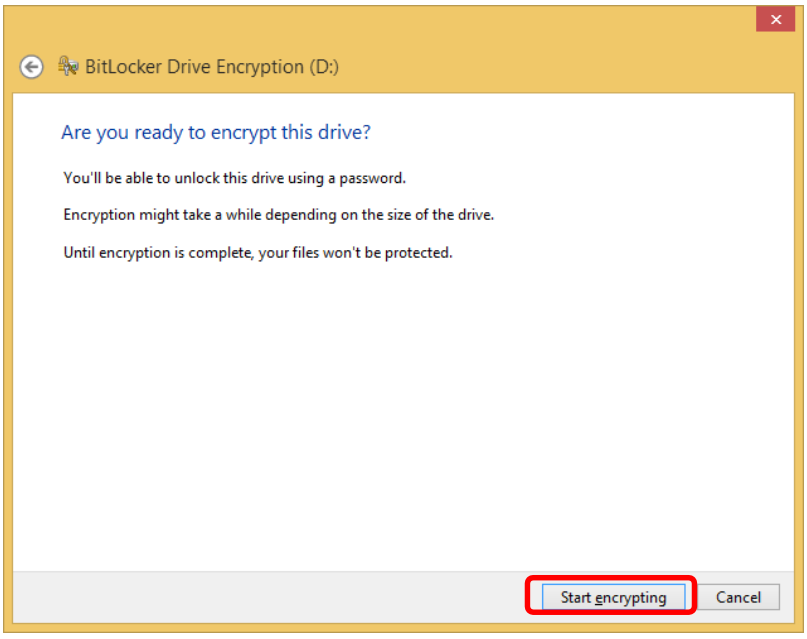
3. Type in your password twice. Click "**Next**".

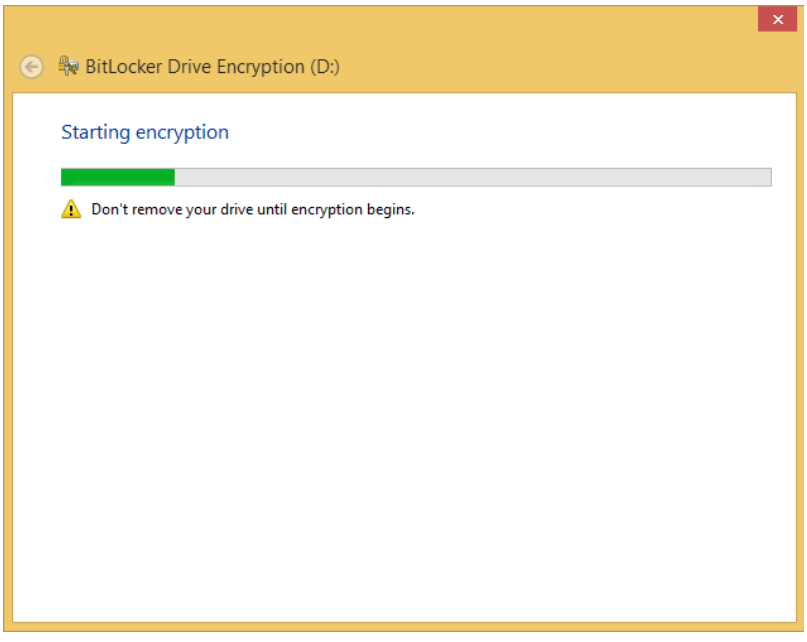


4. Select the second option "**Encrypt entire drive**". That way even deleted data, that's possibly recoverable is encrypted too.

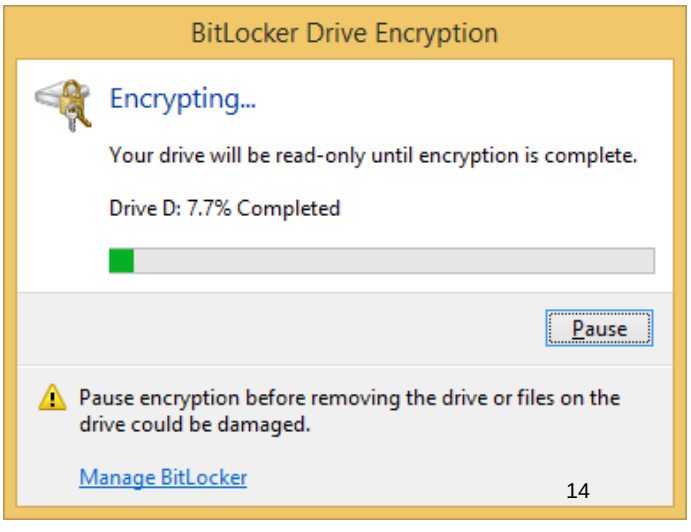


5. Click on **"Start encrypting"**.

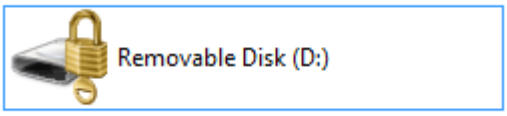




6. You'll be able to monitor the progress while your drive is encrypted. The amount of time it takes will vary depending on the amount of data on your drive and its size. The following window will disappear after encryption completes.

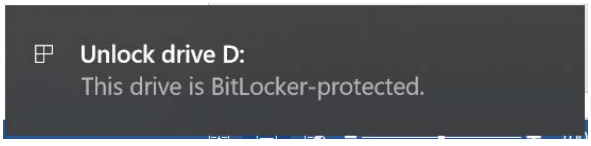


7. After the drive is encrypted, you'll see a lock icon on the drive listed in computer.

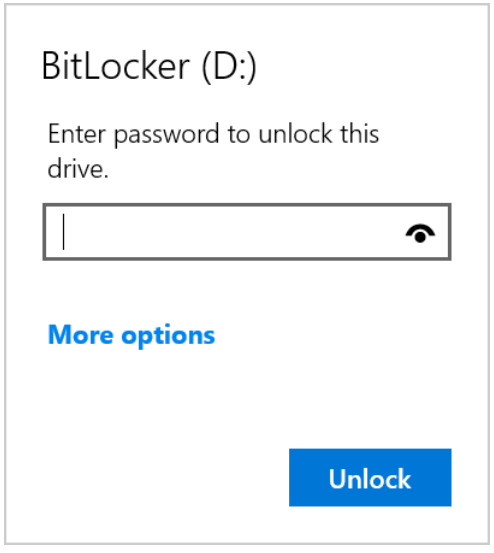


Unlocking your portable drive

1. When you insert a BitLocker portable drive into a Windows 10 computer, you will receive the following prompt. *(On Windows 8, the box looks a little different)*



2. Click on the above prompt, and you will be required to enter the password which you have set previously to unlock the drive before you can access it.

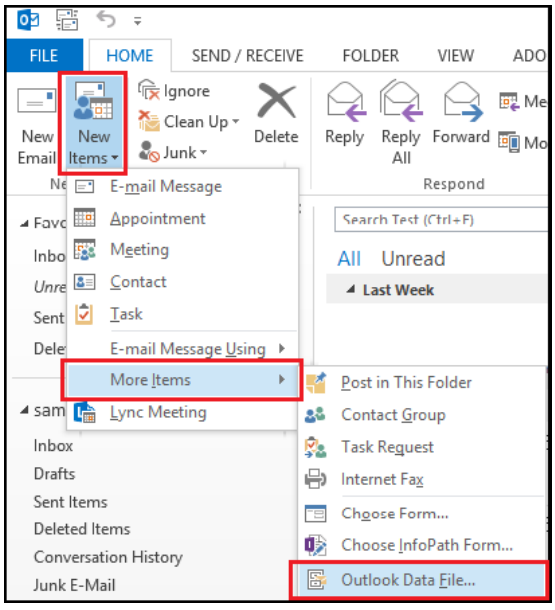


Personal Folder

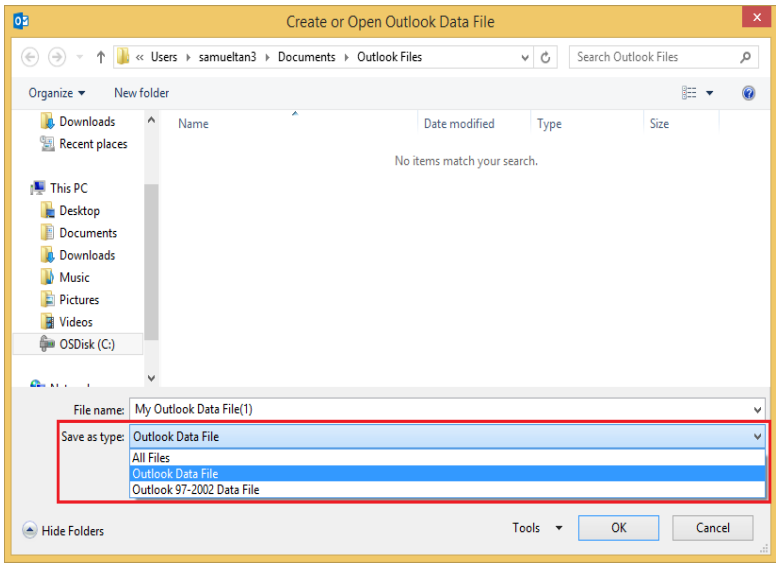
A personal folder, also known as Outlook data file in the 2013 version or .pst, is a media used for storing emails created in Outlook. It compresses your emails similar to a zip file allowing you to save hundreds of emails along with their attachments. Personal folder need to be setup manually in order to save those wanted emails into the folder. The default personal folders location will be located on your hard drive.

Create Personal Folder

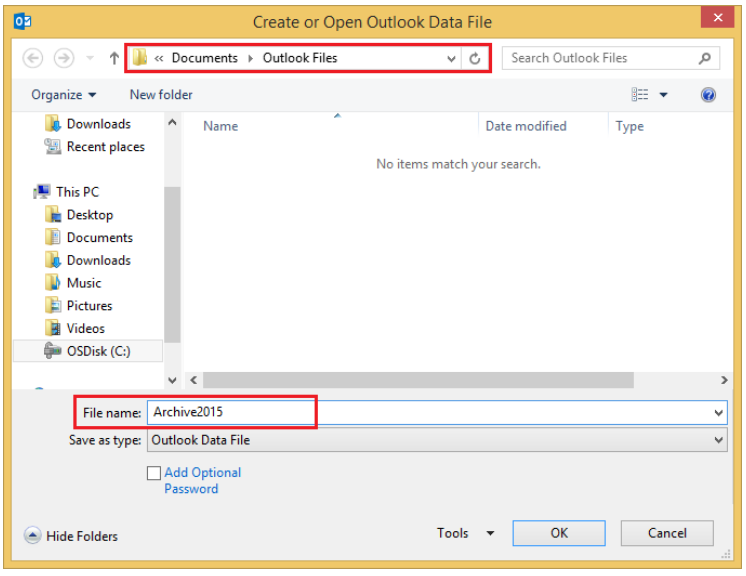
1. Select "Home" tab from your Outlook and select "New Items", then "More Items", then "Outlook Data File..".



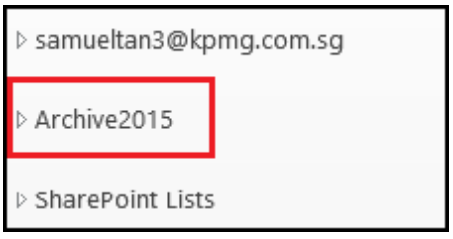
2. At 'Save as type', you may use the default setting "Outlook Data File" (.pst).



3. Choose the location to save the Personal Folder or leave it as default under *C:\Users\<username>Documents\Outlook Files*. Then rename the personal folder for easy referencing or leave it as default.

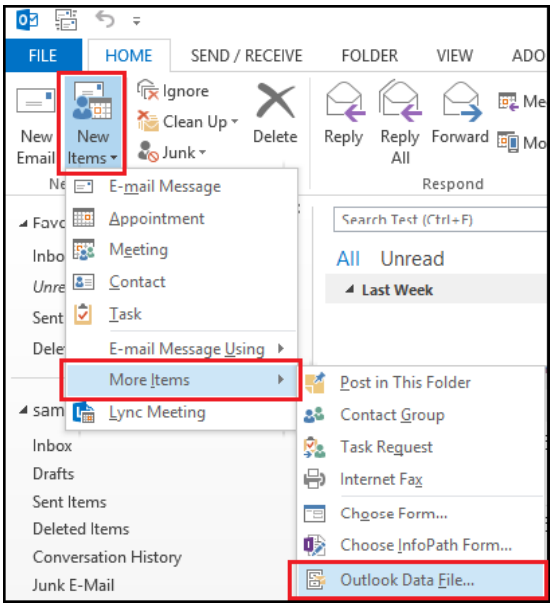


4. The Personal folder you created will appear on the left pane of your Outlook Folder List.

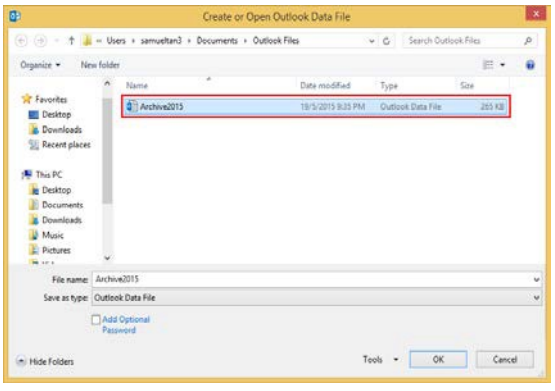


Open Personal Folder

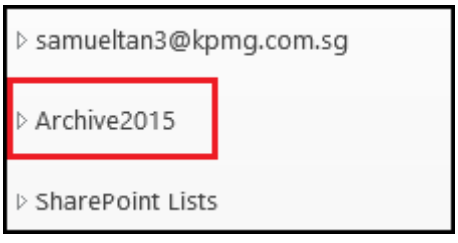
1. Select “Home” tab from your outlook and select “New Items”, then “More Items”, then “Outlook Data File..”.



2. Select the Personal Folder file (.pst), which you would like to open, from the “Create or Open Outlook Data File” dialog box.



3. The Personal folder will appear on the left pane of your Outlook folder list.



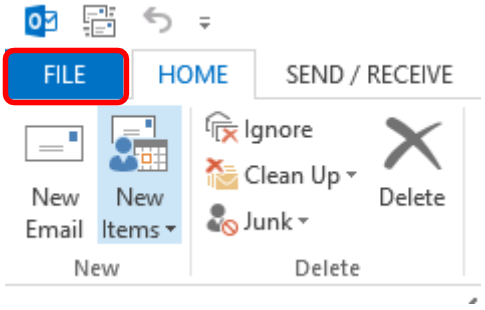
How to archive your Outlook emails

Have you ever received an e-mail message stating that your Outlook mailbox was full, and you were unable to receive or send e-mail messages? There is a limit to the outlook mailbox size. Once this limit is reached, mail cannot be sent or received until space is freed up. The best way to do this is by archiving your old e-mail. When you archive your e-mail, it is moved from the Microsoft Exchange Server to a file on your hard drive. This frees up space in your mailbox, and gives you the ability to access all your old mail.

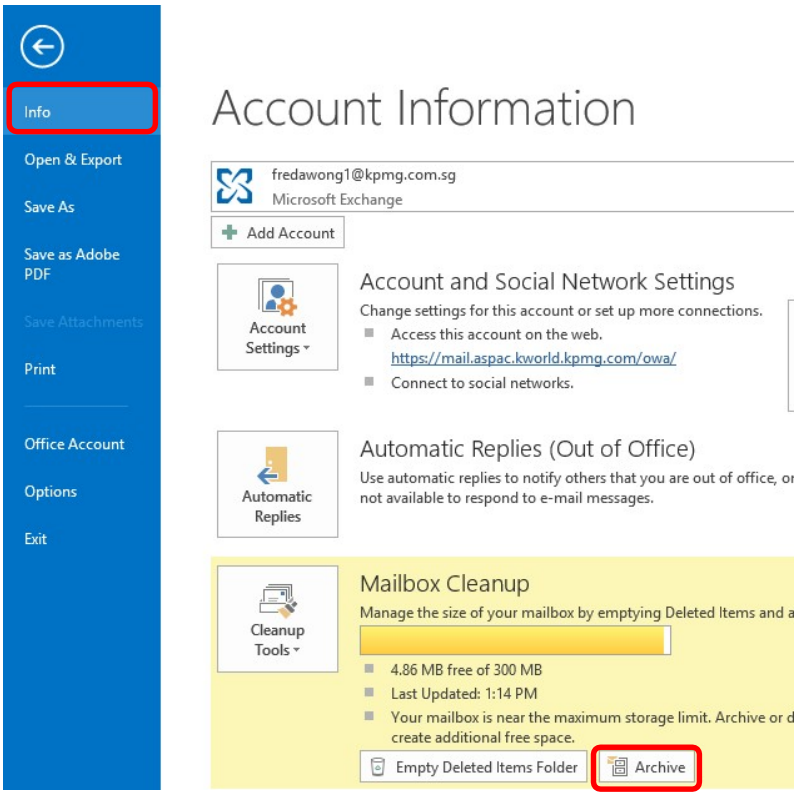
How to manually archive emails

Manual archiving provides flexibility, and allows you to specify exactly which folders are included in the archive, and which archive Outlook Data File (.pst) is used.

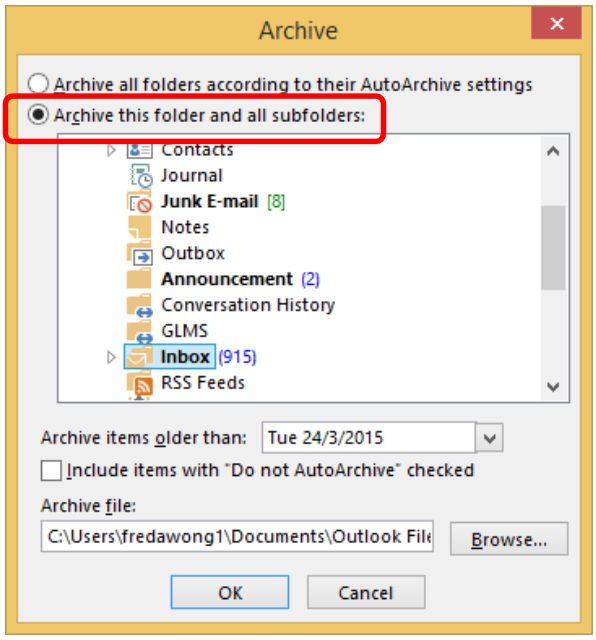
1. Click the "File" tab on the top left of your Outlook.



2. Go to "Info", then click on "Archive" under Mailbox Cleanup.



3. Click on the option 'Archive this folder and all subfolders'.



4. In the Archive items older than list, choose a date from the date picker. In this example, items in the folder created before March 24, 2015 are archived.

5. To include items that you previously selected not to archive, select the Include items with "Do not AutoArchive" checked check box.

   Note: To see if items have the Do not AutoArchive this item check box selected, open the item. On the File menu, click Properties. On the General tab, verify that the Do not AutoArchive this item check box is selected.

6. To archive the folder to a file other than the default Archive.pst file, click Browse, and then specify a different file name, such as Home Networking Archive.pst, and a location, such as My Documents.

   Note: The default location for Archive.pst is C:\Users\<username>\Documents\Outlook Files\.

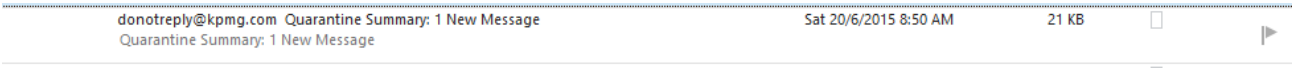
7. Click OK.

Managing Your Spam Mail

ProofPoint external email content filtering tool protects the email communications infrastructure by providing comprehensive email intrusion prevention that prevents spam, viruses and SMTP attacks from ever reaching the enterprise gateway.

Receive Quarantine Summary Message

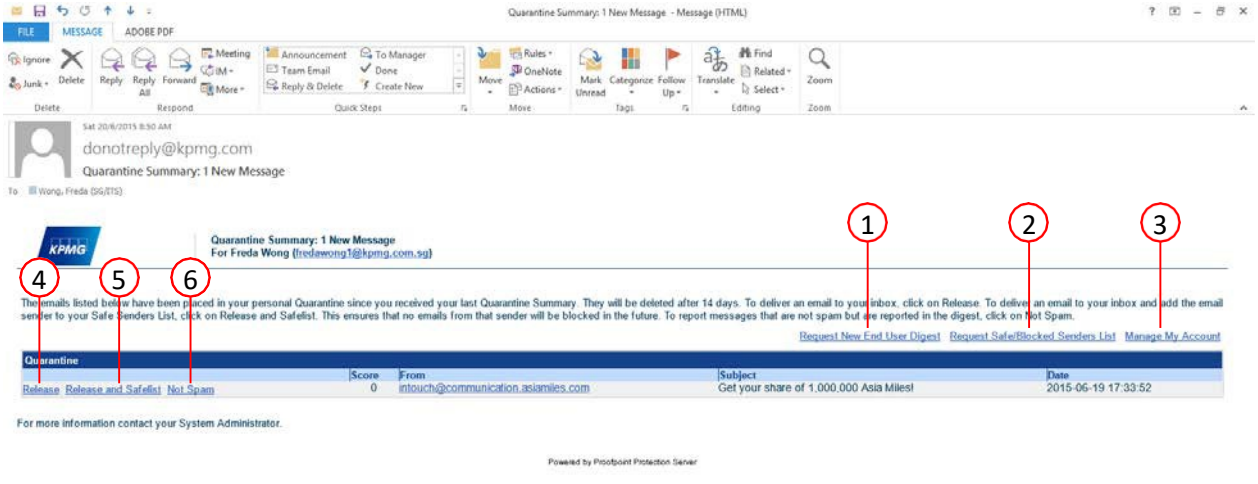
Users of the KPMG Message Centre will receive a "Quarantine Summary" message in his inbox daily.



How to use the new Quarantine Summary email

The quarantine email provides the following functionality:

1. Request New End User Digestto have a refreshed quarantine summary emailed to you.
2. Request Safe / Blocked Senders List to have the safe/blocked sender list emailed to you.
3. Manage My Account to add or remove email addresses from your safe/blocked senders list and change other preferences. This link opens the message center in a browser window.
4. Release quarantined emails to deliver message to your inbox.
5. Release and Safelist to deliver the email to your inbox and add the sender to Safelist.
6. Not Spam delivers the message to your inbox.



If all messages listed on the Quarantine Summary are spam, you do not have to take any action. These messages will be stored in the KPMG Message Centre where you can manage them later on.

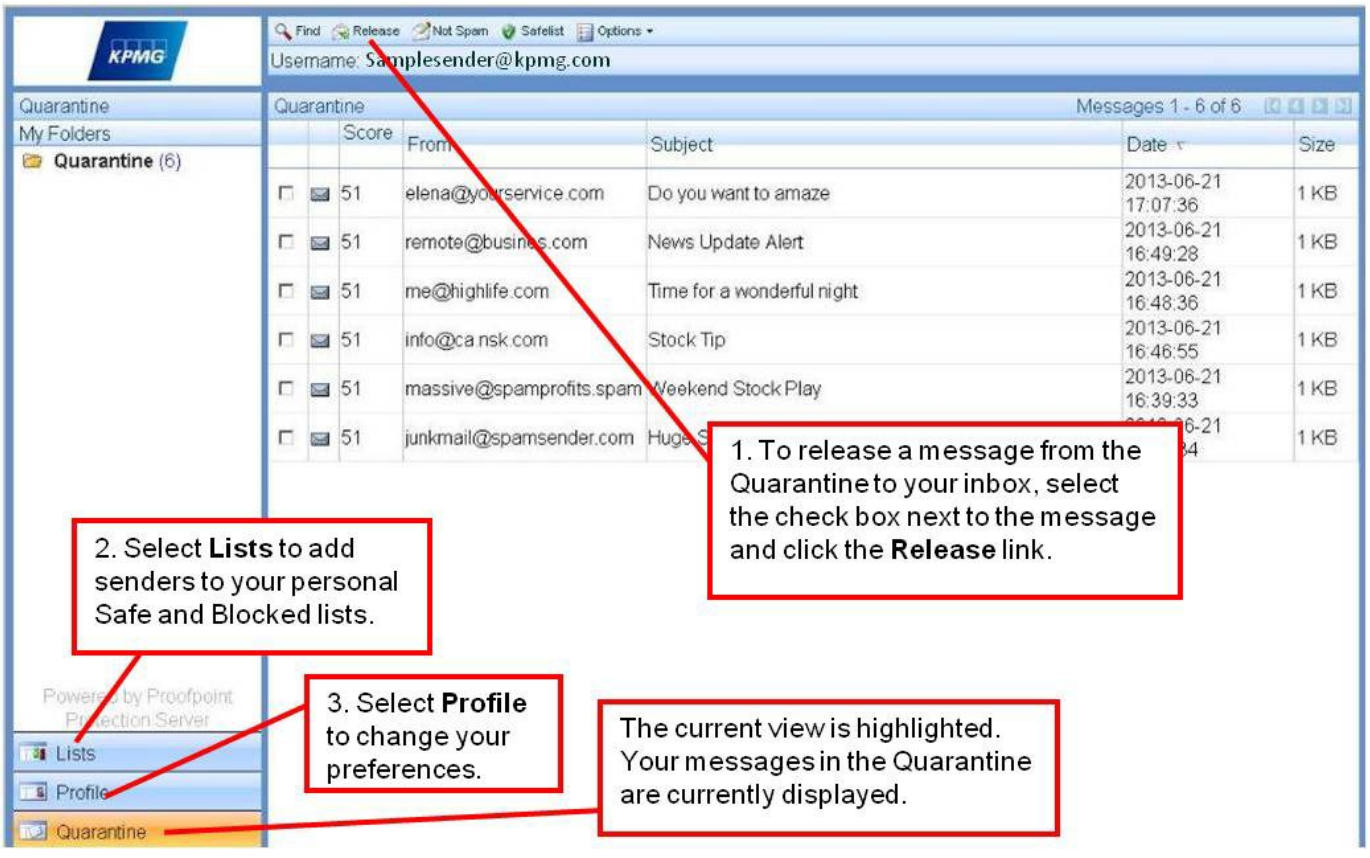
How to use the message center

The below illustration provides an example of the Message Center functionality.
You can access the Message Center by clicking the "Manage my account" link from your Quarantine Summary email.

To ensure the security of your emails, it is not possible to access your message center without your quarantine summary. You must use the link in the quarantine summary to access your message center. This link cannot be bookmarked.

After you access the Message Center, you can:

1. Release your email messages from the Quarantine
2. Add or delete senders in your Safe Senders and Blocked Senders lists
3. Change your quarantine preferences



NOTE: You need to be connected to the KPMG network (i.e. you can send and receive KPMG email) to release emails or access the message center

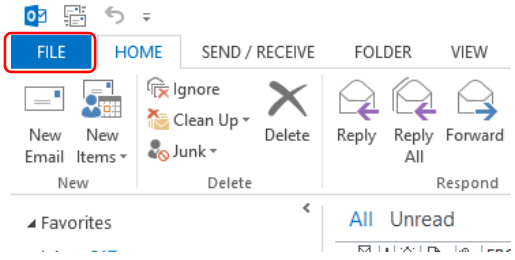
Data Loss Prevention

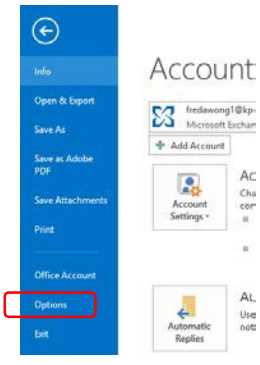
Have you ever sent your email to an unintended party? Our Data Loss Prevention (DLP) software is designed to prevent accidental sending of internal correspondence to external parties. It also identifies emails that may contain sensitive information and prompts the sender to pause and think before sending the email out.

To make full use of the DLP software, kindly amend your current "default" email signature or create a new default signature and include the phrase "KPMG Internal Use Only" (not case sensitive).

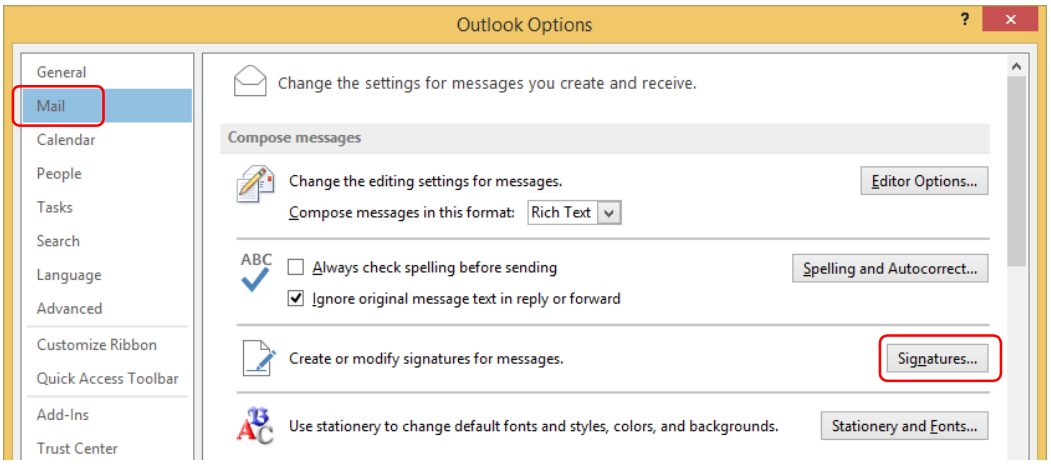
Creating/ Editing New Email Signature

1. Launch your Outlook and go to "File" on the top left corner. Then select "Options".

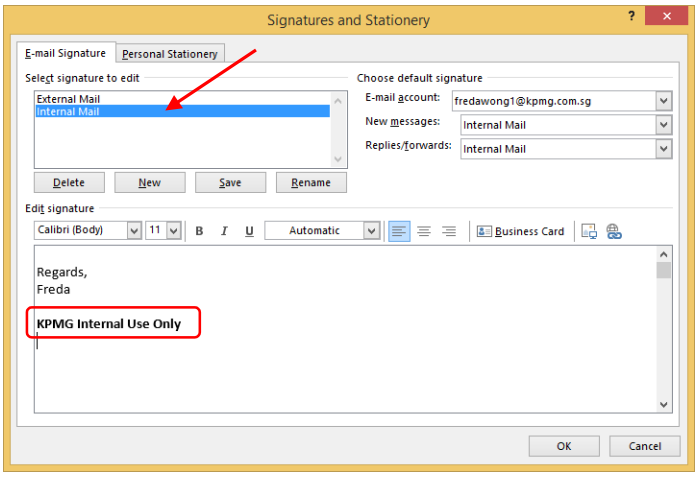




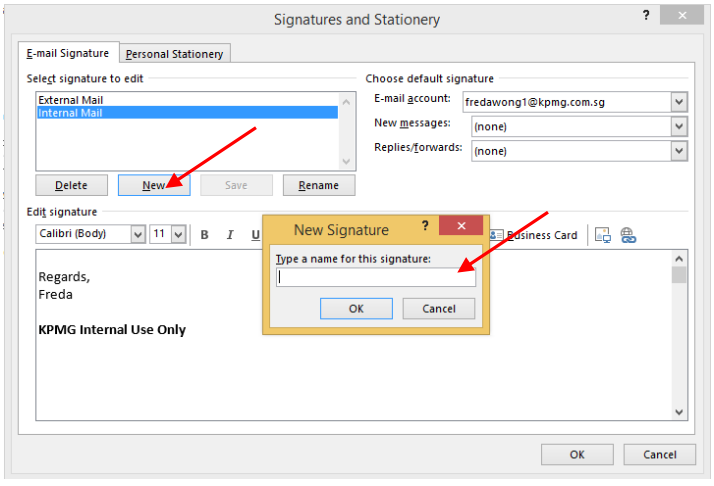
2. Go to "Mail", then select "Signatures".



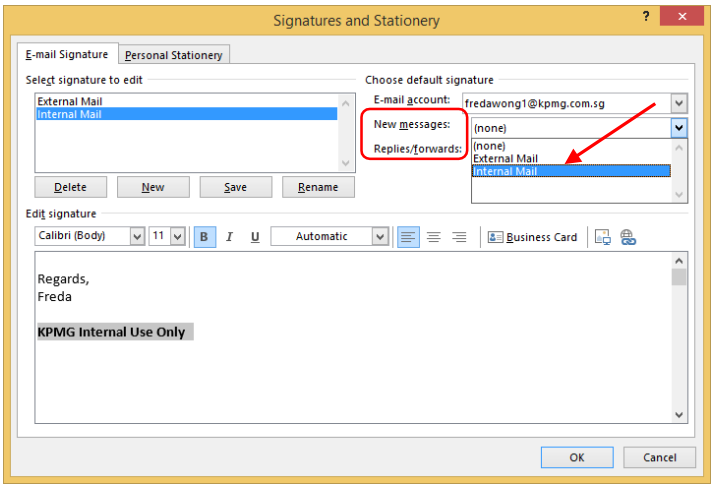
3. To Amend Signature: Select the signature which you like to edit and add "KPMG Internal Use Only" (not case sensitive) as shown in the example below.



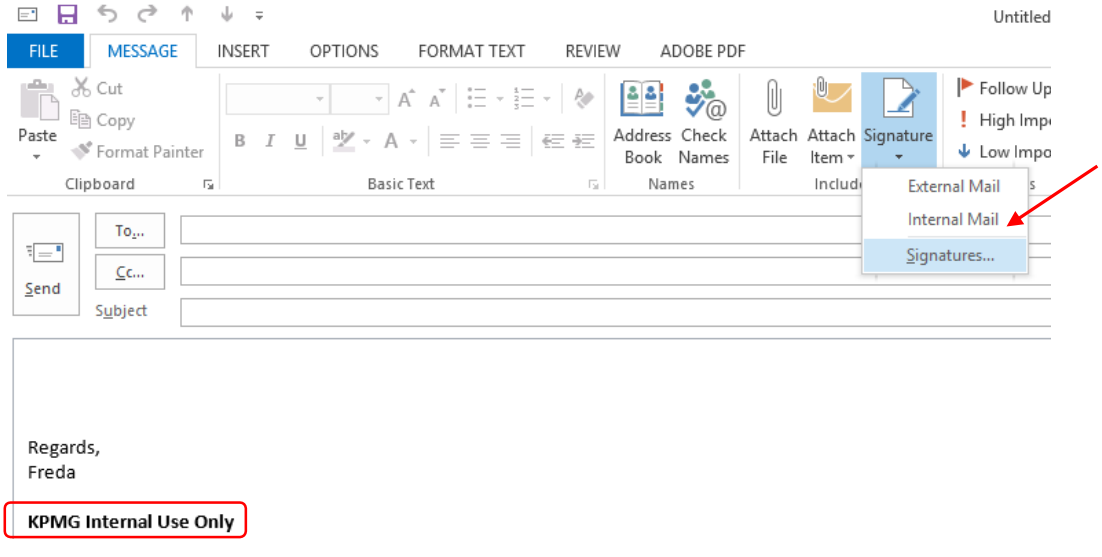
4. To Create New Signature: Click on the new button and name your signature and click on "OK". After the new signature is created, you can refer to step 3 to amend the signature.



5. To Set Default Signature: After you have amended or created the signature, select the "Internal Email" signature as default for New messages and Replies/forwards.



6. When Composing a New Email: When you compose a new email, the "Internal Email" signature which contain the phrase "KPMG Internal Use Only" will be appended on the email. You can also choose to use other signatures from the signature option on the new email as shown in the example below.



DLP Protection Rules

1. Internal Email Content Protection

If you have followed the instructions above to amend or create a new signature (containing the phrase "KPMG Internal Use Only") and have specified it as your default signature, then all new emails you create or reply to will have that phrase appended to it.

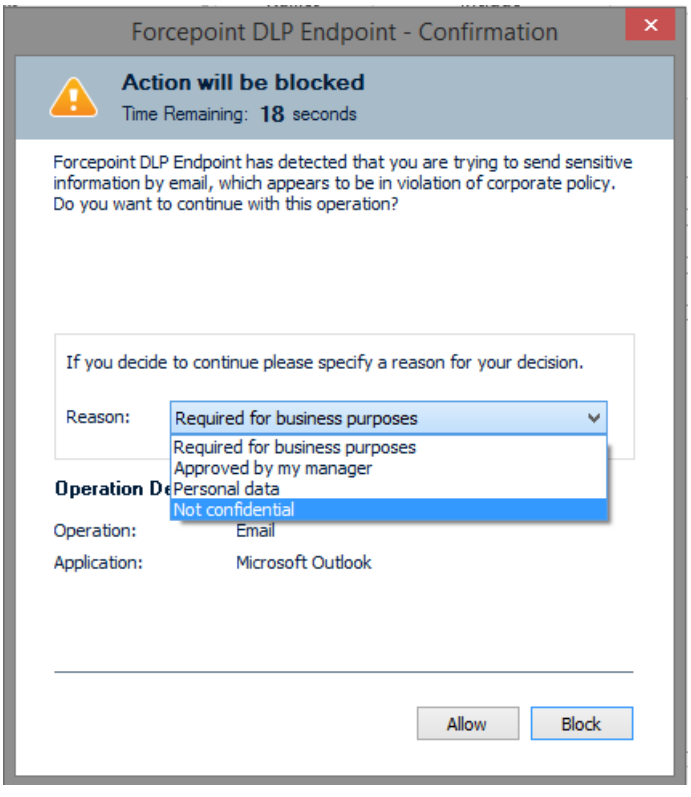
The DLP system will identify that the email (or its attachment) is meant for internal circulation only and will prevent accidental sending to non-KPMG email addresses. The following pop-up will appear on the bottom right hand corner of your screen.

2. Sensitive Information Protection

If your email or attachment contains potentially sensitive information, a pop-up will appear prompting you to click on "Cancel" to confirm your recipients or to select one of the following options and click on "OK" to send the email.

You are required to select one of the following justification:

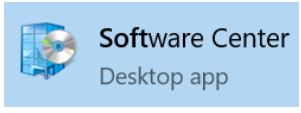
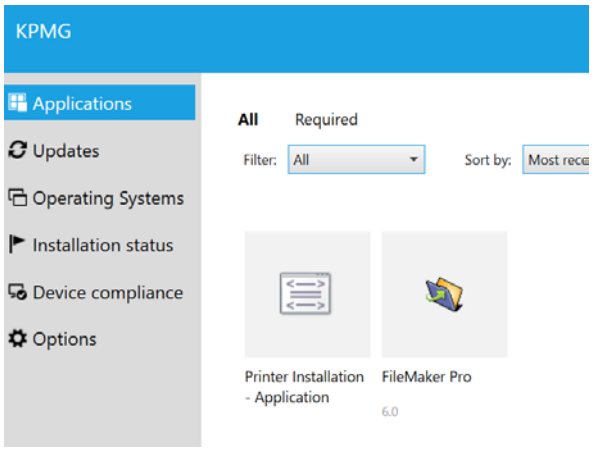
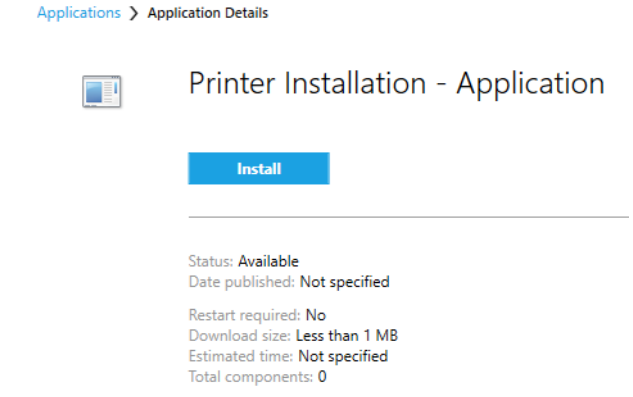
1. Required for business purposes
2. Approved by my manager
3. Personal data
4. Not confidential

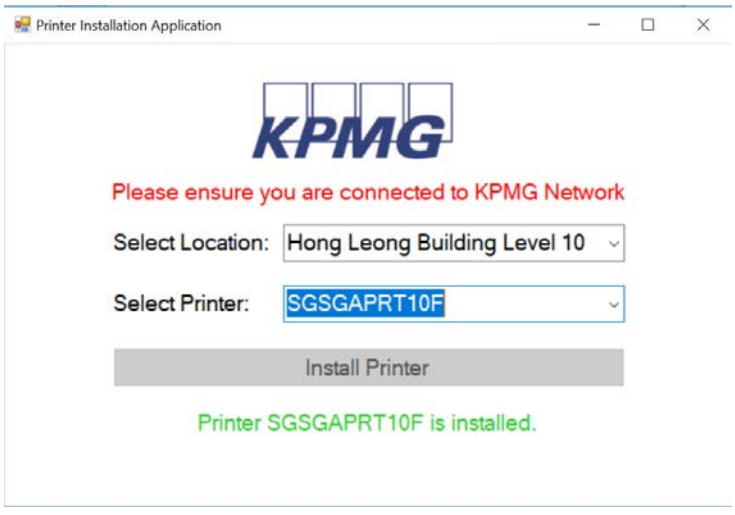


Adding of Printers

Before you install a network printer, you need to know the printer name. You can find the printer name on the physical printer.

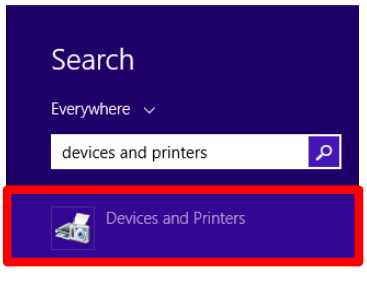
How to Install a printer

	➢ Press on + S ➢ Search for "Software Center" ➢ Press enter or click on the Software Center
	* Please close all running programs before installing any software. * ➢ Under "Applications", select "Printer Installation - Application"
	➢ Select on "Install"
	➢ The following screen will appear, select the level you are on under "Select Location:" and select the printer under "Select Printer:" ➢ After you have completed the selection, select "Install Printer"

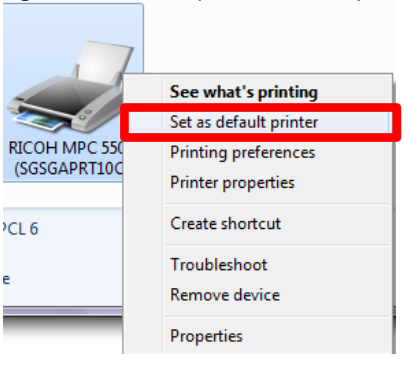
	➢ The following screen should appear, indicating "Please wait, installing printer."
	➢ Once the installation is completed, you will see "Printer is installed" ***If you do not see Printer is installed, please re-run the installation***

How to set default printer

1. Press "⊞ + S" keys on your keyboard to bring up the Windows search panel. Type "devices and printers" in the search field and click on the program.



2. Right click on the printer which you would like to set as default.



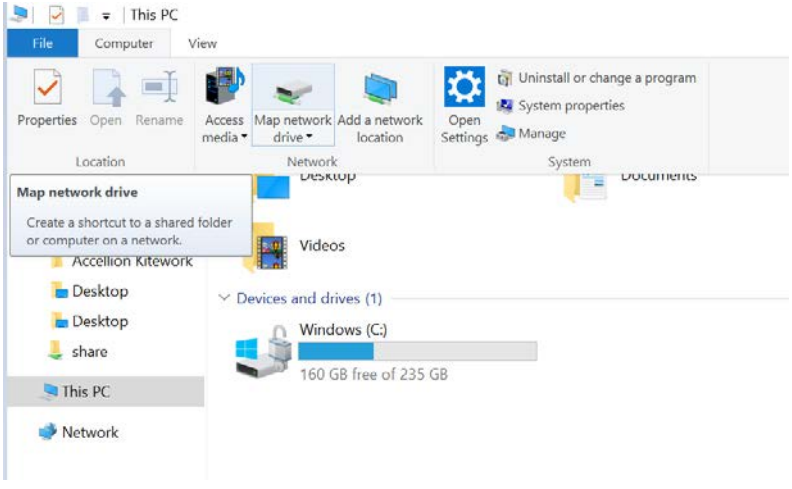
Manually Restoring "S" Drive

KPMG "S" Drive is a network storage which store all the departments files and folder. All users are able access to their own departments shared folder. Users who wish to access to restricted folder are required to fill-in Access Control Request Forms. The "S" drive will be mapped automatically. If you can't locate the network drive you will have to map it manually.

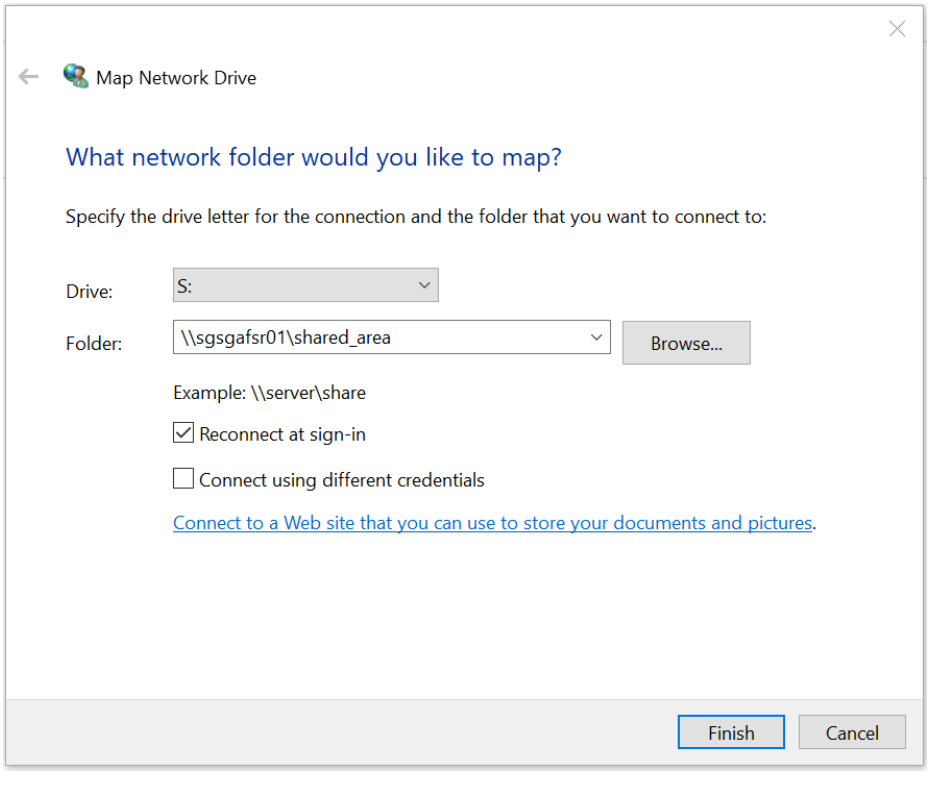
Pre-requisite for Manually Mapping of "S" Drive

- Connected to office network via Network Cable.
- Connected to office network via ITSWireless.
- Connected to VPN Client.

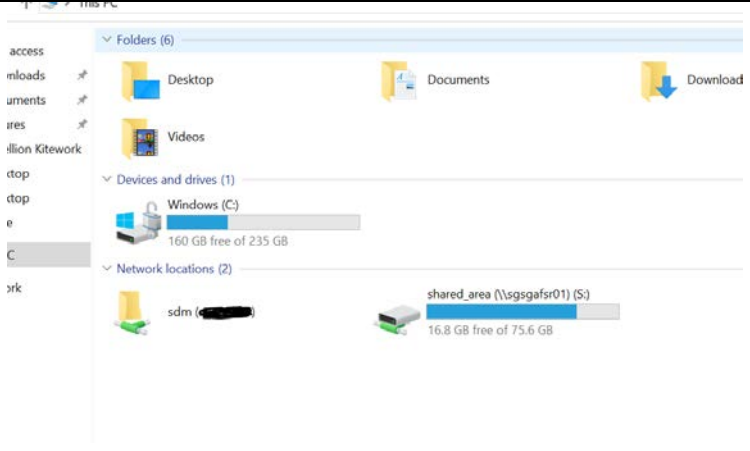
Manually Mapping of "S" Drive



- Click on "File Explorer" located on the Taskbar
- Click on "Computer"
- Click on "Map Network Drive"



- Select the Drive as "**S:**"
- Enter **\\sgsgafsr01\shared_area** in the folder field
- Click on Finish

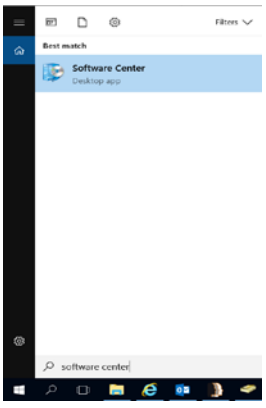


- You should see the S drive mapped under Network Location in This PC

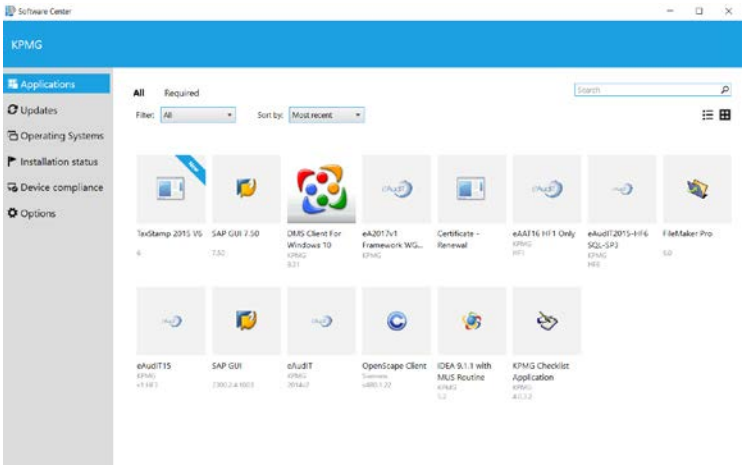
Installing Software Application

Many applications are available to you through the KPMG network. Please close all running programs before installing any software.

To install a program

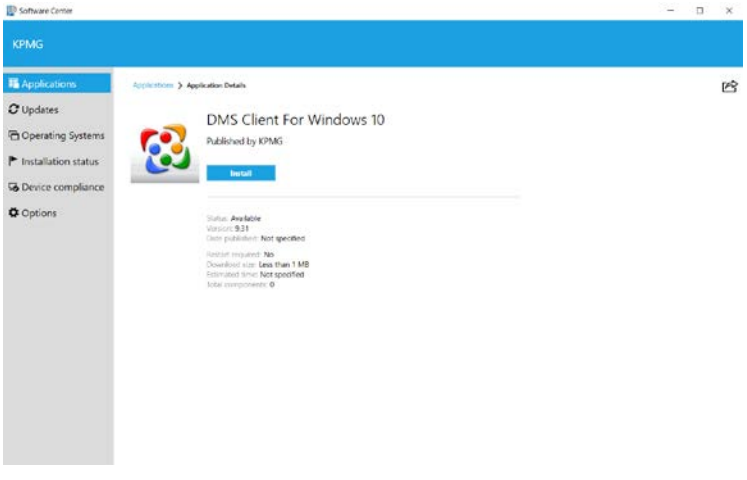


- Press on + S
- Search for "Software Center"
- Press enter or click on the Software Center

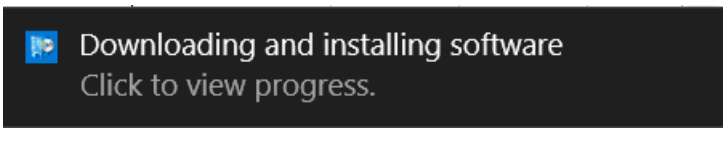


* Please close all running programs before installing any software. *

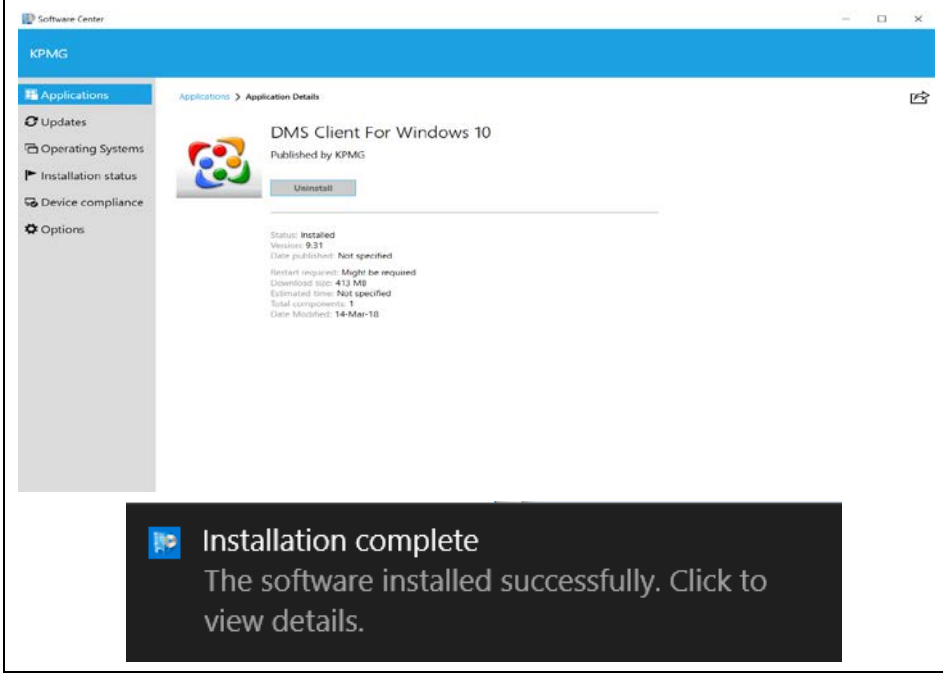
- Under "Applications" select the software you would need to install.



- After selecting the software, it should bring you to "Application Details" page.
- Click on "Install" to get the software installed.



- "Downloading and installing software" will prompt at the bottom right of your screen after clicking on "Install"



- After installation is completed, you should see “Installation complete” at the bottom right of your screen.
- Likewise, in the Software Center, you should see that the installation is completed. Refer to the status, it should be indicated as Installed.
- Done!

Prohibited Software

Here is a list of prohibited software that is prohibited from KPMG computers. The list will be refreshed from time to time should new software be discovered which causes harm to our computers or network. It is recommend that individuals confirm with Information Technology Services (ITS) before loading any software on their KPMG desktop or laptop.

*Click **here** for updated prohibited software list.*

A	B	C - E	F - I
• AdRotator • AdunanzA • AIM • AOL Instant Messenger • Ares • Ares Galaxy Turbo • Ares Lite • Ares MP3 • Ares Torrent Downloader • Ares Ultra •AresGalaxyDownloader • AresLite • Atomic Clock Sync • AudioGalaxy Satellite • Azureus	• BDHelper • BearShare • BearShare Acceleration Patch •BearShareGoldDownloader • BearShare MediaBar • BitComet • BitSpirit • BitTornado • BitTorrent Mainline • Bookmark Express • BT Communicator • BUFFALO BSKP-U201Skype Phone • ByteTaxi	• CnsMin • eDonkey2000 • Emule • eMule • eMule++ • eMule AdunanzA • eMule Plus • eMule VeryCD • eMule.de 44b v16 webcache • eMuleKL • Eyeball Chat 2.2 • Ezula	• FolderShare • FileTopia • Gaim • gaim2-otr • gaim-otr • GameSpy Arcade • Get Yahoo! Messenger • Google Talk • GoToMyPC • Grokster • ICQ • ICQLite • iMesh • iMesh Light-5 • iMesh MediaBar • iMeshSpanish • Internet Optimizer

J - K	L	M	N - R
• JAJC • KaZaA • Kazaa Download Accelerator Pro • Kazaa Lite Resurrection • Kazaa Lite Revolution_ • Kazaa Lite Tools K++ • Kazaa Speedup Pro	• LimeWire • LimeWire Download Manager • LimeWire Ultra Accelerator • LogMeIn • LoudPC	• Manager for Skype • MLDonkey • Morpheus • Morpheus Download Booster • Morpheus Download Client • Morpheus Ultra • MorpheusSoftware • MorpheusToolbar • MSN Messenger (known as Window Live Messenger) • MSN Messenger Khalid Edition 4.2 • MSN Messenger Password Recovery	• NaviSearch • New.Net • NudgeMania 2.0 for MSN Messenger • OverNet • P2P Networking • PocketSkype • PowerStrip • RelatedLinks

S	T - Z	Others
• SBC Yahoo! Messenger • Seekmo • Shareaza • Shareaza Turbo Accelerator_is1 • Shareaza_is1 • ShareP2P • Shopperreports • Soulseek •StanaPhone_is1	•ToolBand.SkypeIEToolbarToolbar • TotalIRC •Useful Skype PTT for Smartphone • Yahoo Messenger • Yahoo! Messenger Explorer Bar • Yahoo! Messenger for Windows CE • Yahoo! Messenger with BT Communicator • Zango • Zango Toolbar	

Note: Users who installed the above software without authorized permission will be dealt with disciplinary action.

Avoiding Viruses

Most viruses come through attachments to emails. These will often look like zip files or Word documents. There will usually be some text in the email telling you why you should open the file. Do not take anything at face value!
Some viruses, such as the Sasser Worm, can infect your computer just by being on the internet. These exploit security holes in the Windows operating system.

Avoiding Viruses

Most viruses come through attachments to emails. These will often look like zip files or Word documents. There will usually be some text in the email telling you why you should open the file. Do not take anything at face value!
Some viruses, such as the Sasser Worm, can infect your computer just by being on the internet. These exploit security holes in the Windows operating system.

NEVER open an attachment unless you are sure of what it is - even if you know the person! If you are uncertain about an attachment, email or phone the person it claims to have been sent by and ask them if it is a genuine attachment. 99% of virus infections come from people opening attachments they shouldn't have.
ALWAYS update Antivirus definition. You should update it often (at least every week) or have it autoupdate itself from the internet. Run a full system scan every couple of weeks.
ALWAYS keep your operating system updated. Run Windows Update often and install all Critical Update Patches. Many of the recommended patches may be useful for other things, but the critical patches actually plug the security holes which Viruses and Worms exploit.

A few of the things Viruses can do to your computer are:

• Send out emails to other people without your knowledge, containing copies of the virus. Modern viruses can also 'spoof' the email address so that the recipients think that the emails have been sent by someone else entirely. If you start getting emails from people you have never heard of, saying you have sent them a virus, then it is likely that someone else's infected PC is 'spoofing' your email address so people think you have the virus, when in fact it is nothingto do with you. The Netsky and LovGate viruses both did this.

• Cause your computer to shut down. An annoying feature which makes working very hard and also makes it difficult to clean the system if you cannot stay on long enough to download the fix. These normally require an update patch to Windows to be downloaded from Microsoft. If you download the patches quickly then you should never get the virus in the first place! The recent Sasser Worm was an example ofthis.

•Corrupt or delete your files & slow down your PC. Viruses can corrupt your own files, losing you work, or they can corrupt or delete files from the operating system, causing your system to slow to or crash.

•Attack other computers. A virus can use your computer to attack another computer over the internet. Not only will this annoy the other person, it also slows down your own computer. Many infected computers attacking a single computer or organisation (often Microsoft!) can cause that companies network to stop working. This is called a Denial of Service attack.

Note: If your computer is exhibiting any of these behaviors, it is worth checking it for viruses.

Virus Hoaxes, Trojans, Spyware and Malware

A virus hoax is often circulated by E-Mail, containing news of a 'devastating' virus. Often there is no virus and central mailers across the globe will become 'clogged up' with messages containing news about a non-existent virus.

Sometimes you will get emails telling you someone wants to give you $15million to launder for them, and you need to send them your bank details. Do not believe it. Even if it were true it would be illegal. Never send strangers your bank details.Sometimes you will get emails telling you Microsoft/AOL/someone else has discovered a catastrophic new virus and you need to send this warning to all your friends. Delete it. Treat any email telling you to forward it on to all your people as highly suspicious. This include ones telling you that AOL (or whoever) is tracking the email and will donate money to cancer research (or whatever) for every time it is forwarded. Sometimes an email will claim to be from your bank, asking you to reregister your account or something. Never give your account details, PIN number or password to anyone by email! Your bank will never ask you to do this.

There are lots of annoying programs and cookies which you can get from the internet which do things such as causing lots of popup to appear when you use the internet, or changing your homepage. They can also do things you don't notice, such as tracking your internet use. These are rarely picked up by antivirus software.

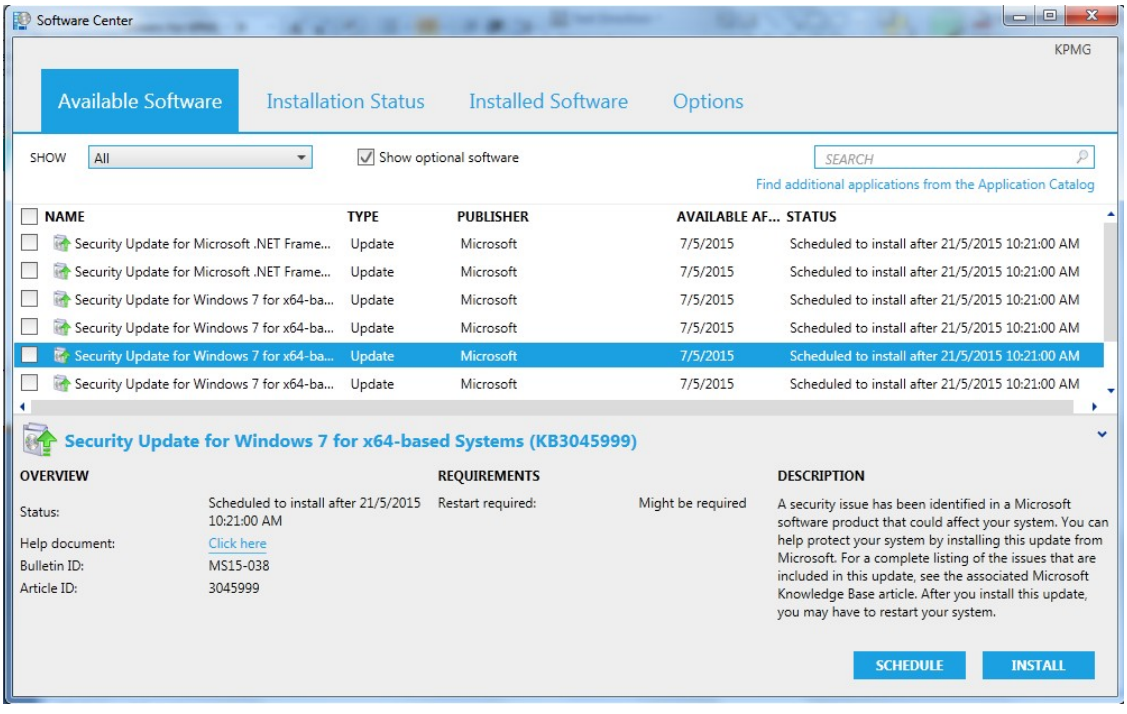
Tip: If machine is infected with Viruses or Trojans, avoid sharing of portable storage devices such as thumb drive to prevent the spread of viruses to other machines.

Automatic installation of Windows Update

Windows Update is a service provided by Microsoft that provides updates for the Microsoft Windows operating system and its installed components (e.g. security patches). An optional feature provides updates for other Microsoft Windows software.

Automatic installation of windows updates

Windows Updates icon will appear at the bottom right of the screen prompting for "Update installation is required". Click on it and Software Center window will appear. Click "Install".



Note: Windows will automatically restart after the updates. Any unsaved work will be lost!

ITS Operating Info

Monday to Friday	: 0845 – 2030
IT Support	: 6213 2266 (Option 1)
eAudit Helpdesk	: 6213 2233 (Technical questions)
Email Address	: sg-helpdesk@kpmg.com.sg

Other Contacts

Admin	: 6213 2266 (Option 2)
Human Resource	: 6213 3111
eAudit Kiosk	: 6213 3666 (Business questions)