Securing Operating Systems

Session Overview

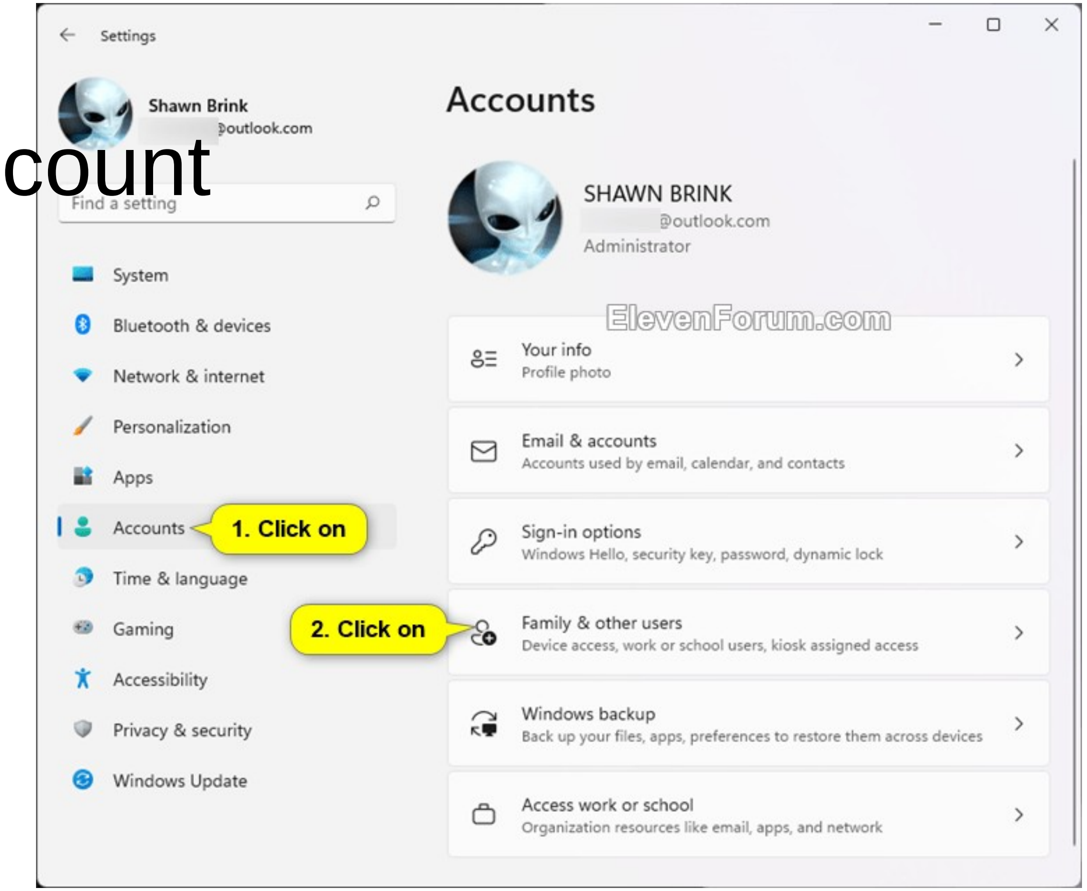
- Secure Operating Systems
- Secure Workstations
- Secure SOHO Networks
- Secure Mobile Devices

Secure Operating Systems

User Account	Description
Administrator	Complete administrative access to a computer,
Power User	A legacy user type that had fewer access privileges than administrators, but more than standard users.
Standard user	Can use most software on a computer. Cannot install/uninstall software. Limited settings. Called a non-privileged user account.
Guest	Limited access only. Default is disabled.

Change Account Types

- Can change between standard and administrator for local accounts
- Must have one valid admin account

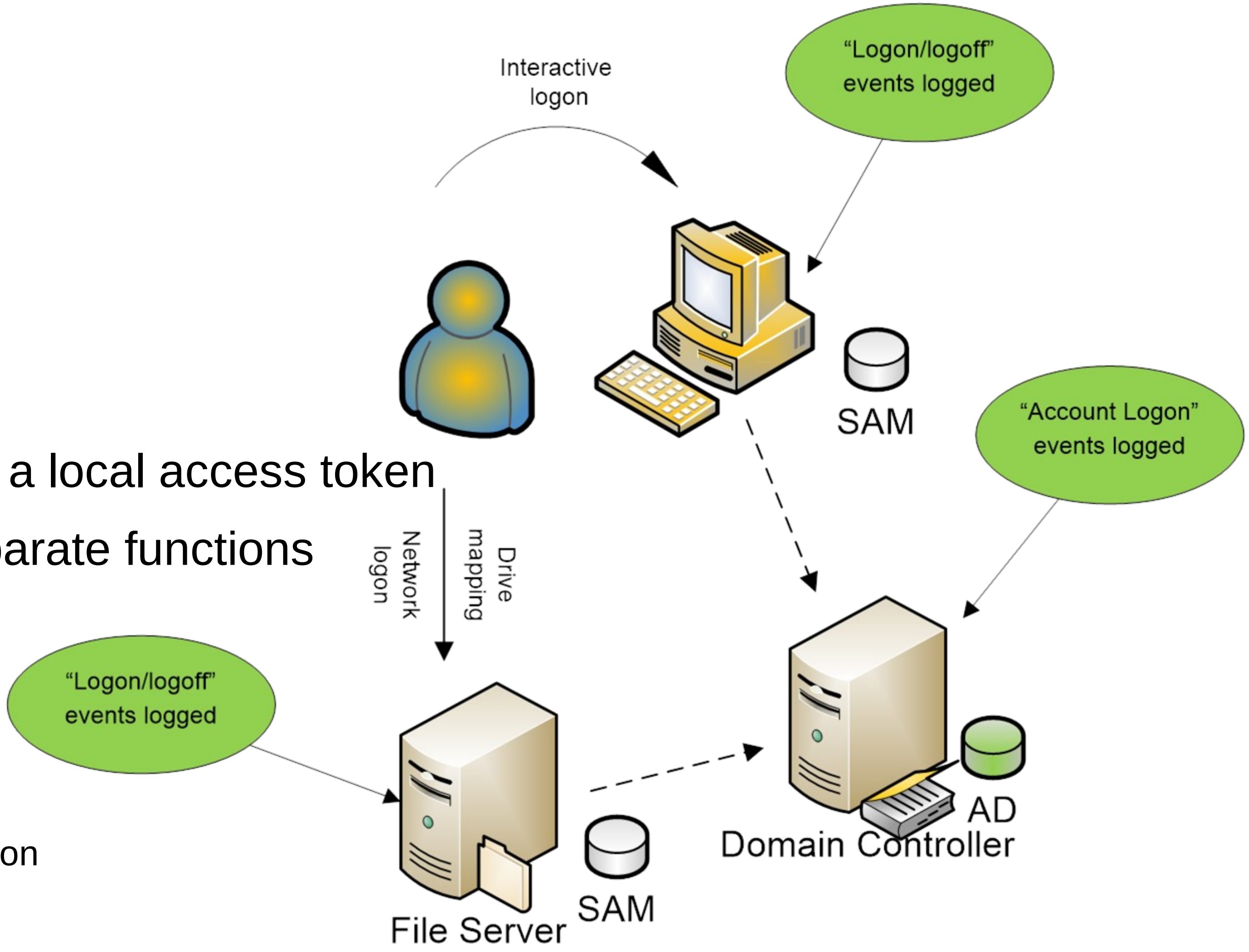


1. Click on

2. Click on

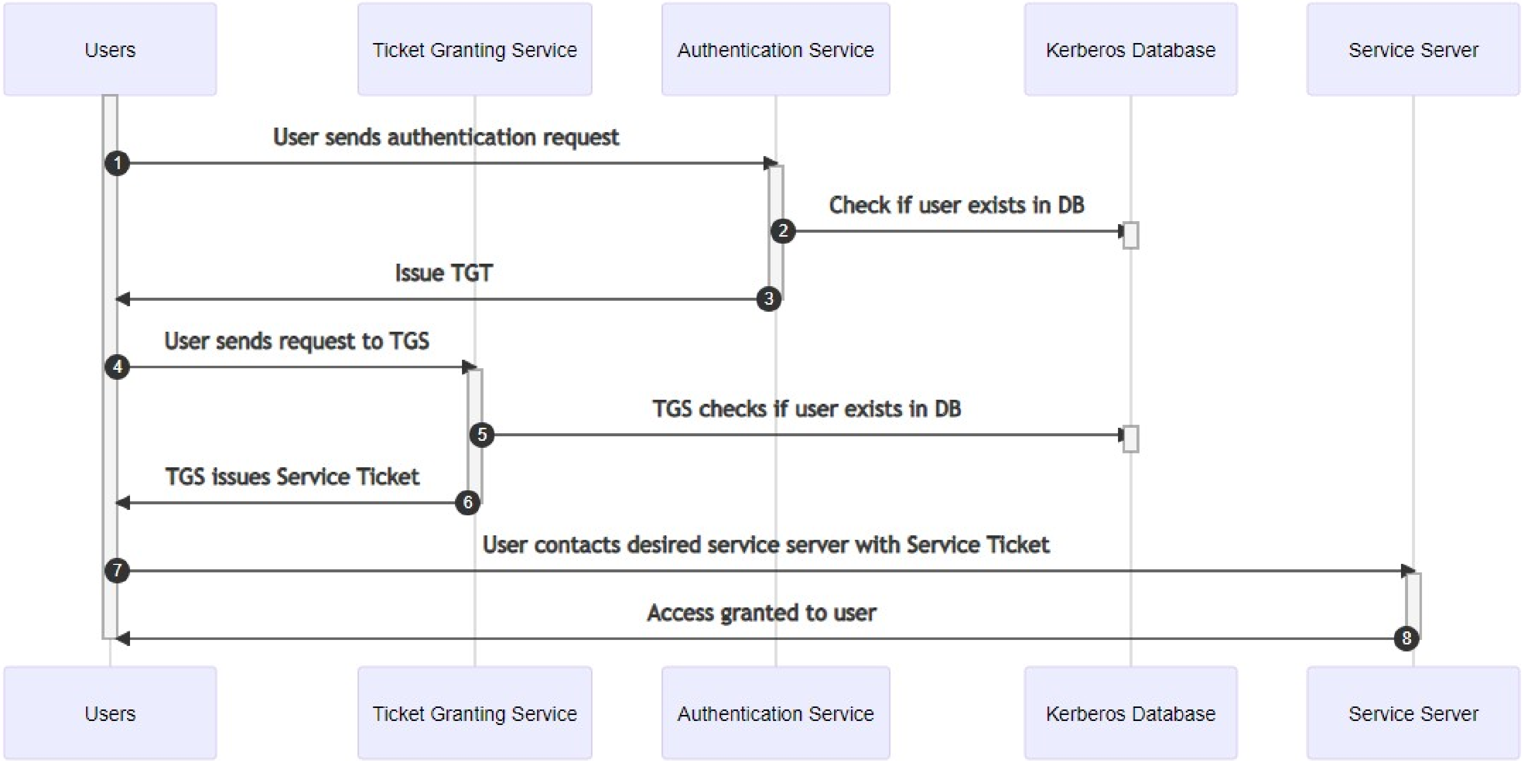
User Authentication

- Two kinds of User Accounts
  - Local Accounts
    - Attackers often target local accounts
  - Domain Accounts
    - stored in Active Directory
    - Authenticated by Domain Controllers
- Local operating system users receive a local access token
- Logon and authentication are two separate functions
  - Local login
    - performs logon and authentication
  - Domain
    - accessed computer performs logon
    - Domain Controller performs the authentication


Interactive logon
"Logon/logoff" events logged
SAM
"Account Logon" events logged
Network logon
Drive mapping
"Logon/logoff" events logged
AD
Domain Controller
SAM
File Server

User Authentication

- Active Directory uses Kerberos v5
  - GUID (globally Unique ID)
- SSO
  - Single Sign On



Users | Ticket Granting Service | Authentication Service | Kerberos Database | Service Server

1 User sends authentication request

2 Check if user exists in DB

3 Issue TGT

4 User sends request to TGS

5 TGS checks if user exists in DB

6 TGS issues Service Ticket

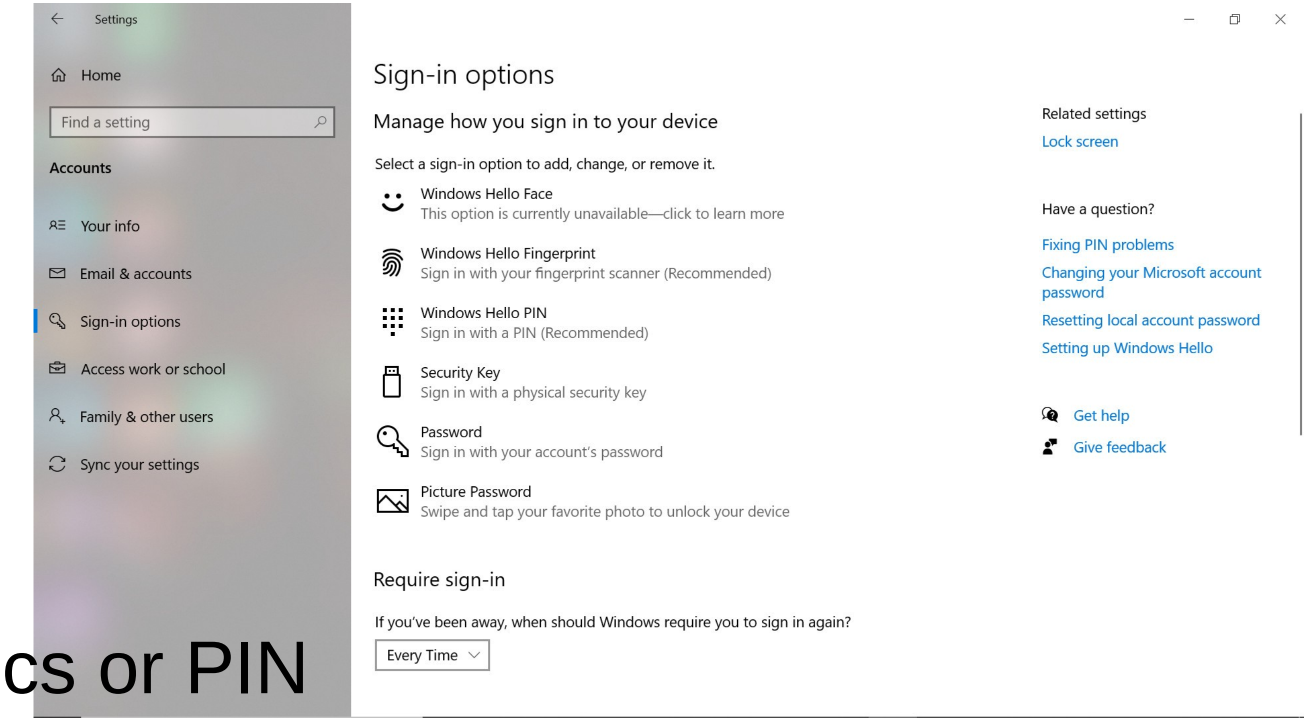
7 User contacts desired service server with Service Ticket

8 Access granted to user

Users | Ticket Granting Service | Authentication Service | Kerberos Database | Service Server

Windows Hello

- Credential Manager
  - Stores users credentials
  - Lock/Unlock with biometrics or PIN
  - Passes credentials on when Unlocked
  - Start → Settings → Accounts → Sign-in Options



Sign-in options

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
This option is currently unavailable—click to learn more

Windows Hello Fingerprint
Sign in with your fingerprint scanner (Recommended)

Windows Hello PIN
Sign in with a PIN (Recommended)

Security Key
Sign in with a physical security key

Password
Sign in with your account's password

Picture Password
Swipe and tap your favorite photo to unlock your device

Require sign-in

If you've been away, when should Windows require you to sign in again?

Every Time

Permissions

- Security setting to determine level of access a user has to a resource.
- Can be applied to printers, files, shares, network resources
- Configuration allows differing level of privileges
- Can be assigned on a per user basis (but inefficient due to maintenance – better to create groups)

NTFS File and Folder Permissions

- Five Standard NTFS file permissions:
  - Read (Read the file and view attributes, ownership and permissions)
  - Write (Overwrite the file and change file attributes)
  - Read & Execute (Run applications and perform Read tasks)
  - Modify (Modify and delete the file)
  - Full Control (Change permissions, take ownership and perform all other tasks)

NTFS File and Folder Permissions

- Six Standard NTFS folder permissions:
  - List Folder Contents (View the names, attributes and permissions of subfolders, but only see the names of files)
  - Read (View names, attributes, permissions and contents of files and subfolders)
  - Write (Create new files and subfolders, and change attributes)
  - Read & Execute (Same as Read and List folder, but execute tasks permitted)
  - Modify (Delete the folder and perform Write, Read and execute)
  - Full Control (Change permissions, take ownership, delete sub folders and files, perform all other tasks)
- Files and sub folders within a folder will inherit the folders permissions

NTFS File and Folder Permissions

- Special permissions are the individual components of standard permissions. Allows a finer level of control.
- File compression and encryption.
  - Implemented as advanced attributes
  - Encryption – protects drive contents
- NTFS compression is not the same as Cabinet (CAB) files

Exercise

- See the sheet Exploring NTFS File Permissions

Shared Files and Folders

- Shares include:
  - Folders
  - Printers
  - Drives
- Allow access from remote computers

Share Permissions

Permission	Description
Read	• View file and subfolder names, contents, attributes • Run program files • Granted to Everyone by default
Change	• Perform all Read permission tasks • Add, change, delete files and subfolders
Full Control	• Perform all Read and Change tasks • Change permissions

NTFS v Share Permissions

- Shared folders have 2 sets of permissions
  - NTFS Permissions (Security tab of folders properties)
  - Share Permissions (Shared Tab of folders properties)
  - No propagation between the two
- NTFS permissions apply to actions users can take on files and folders on locally or on the network.
- Share permissions apply to folders, subfolders, and files that have been shared with other users and are accessed from the network.
- Both NTFS and share permissions can be applied to the same file or folder.
- The most restrictive permission (NTFS or Share) will apply.

Exercise

- See the sheet Exploring Share Permissions

File System Security

Consideration	Description
Allow or Deny?	When choosing whether to allow or deny an action using permissions, choose carefully between the two. Deny is more restrictive than Allow. If the Deny property is applied on either a file or a folder, it will override any Allow permissions that may have been granted to the user. Use Sparingly.
Move or copy files and folders?	When permissions have been applied, moving a file or folder and copying that file or folder will have different results. It is important to consider those results when choosing whether to move or to copy your files or folders. On the same partition: • Move: retains permissions from old location. • Copy: inherits permissions from new location
File attributes	You can set file attributes on files and folders, and these attributes can affect the actions a user can have on that specific file or folder, regardless of the permissions that have already been set.

Security for Shared Files and Folders

- Permissions Inheritance
  - Permissions assigned to a folder are inherited by files and folders it contains
  - Better to assign permissions to folder rather than files
  - Inherited permissions indicated by gray background check marks
- Permissions Propagation
  - Modifying a parent folder, you can choose to propagate changes downwards to all subfolders

Security for System Files and Folders

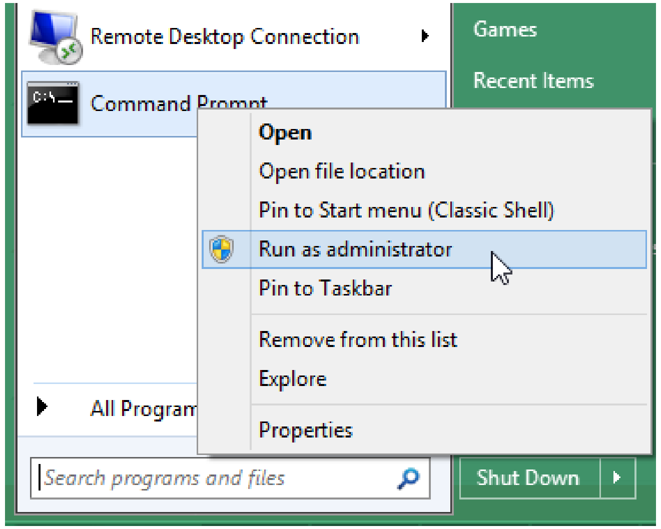
- Configured as Read Only
- Hidden
  - to protect system files and folders from deletion or modification.
- If modification or deletion is necessary, remove the Read Only permission.

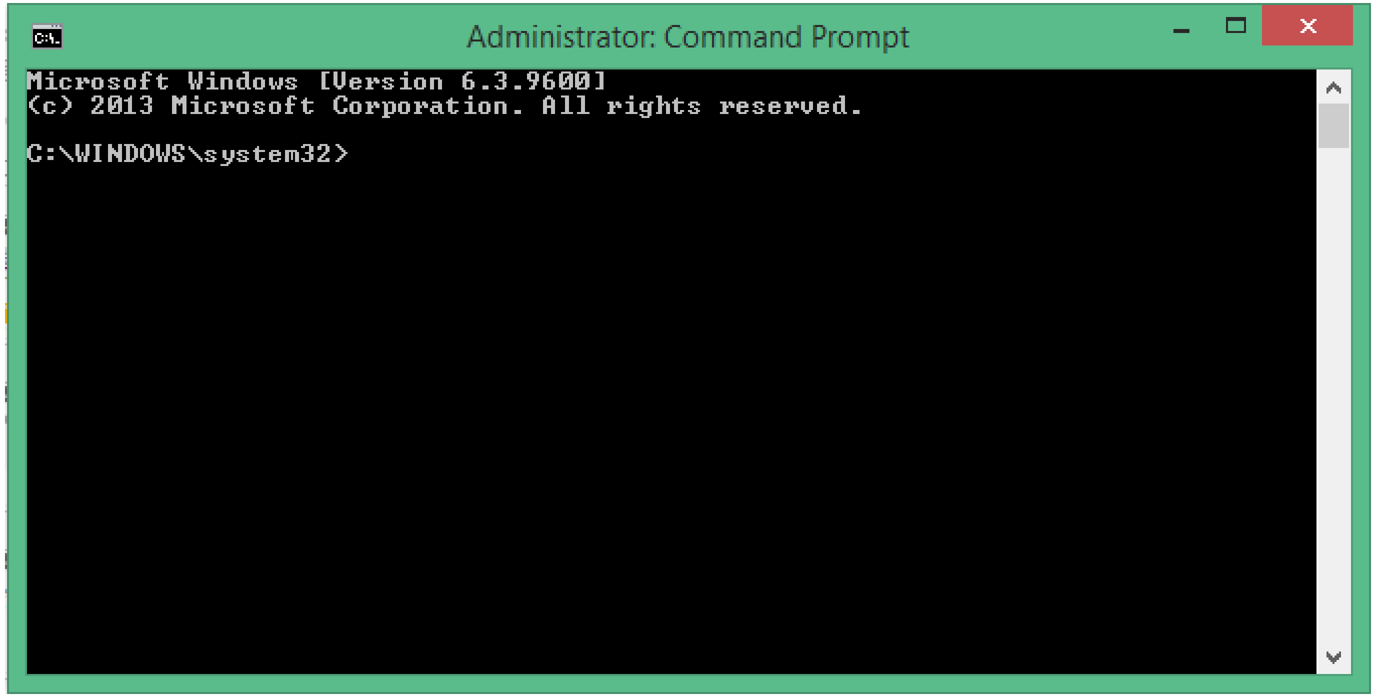
User Authentication

- Proving your identity to gain access to network resources.
  - Username and Password most common
- Methods.
- Factors:
  - What you know (e.g. Password)
  - What you have (e.g. ID card)
  - What you are (e.g. Fingerprint)
- SSO (Single Sign On)
  - One time authentication to multiple resources
  - Requires strong authentication

Run As Administrator

- Login with least privileges



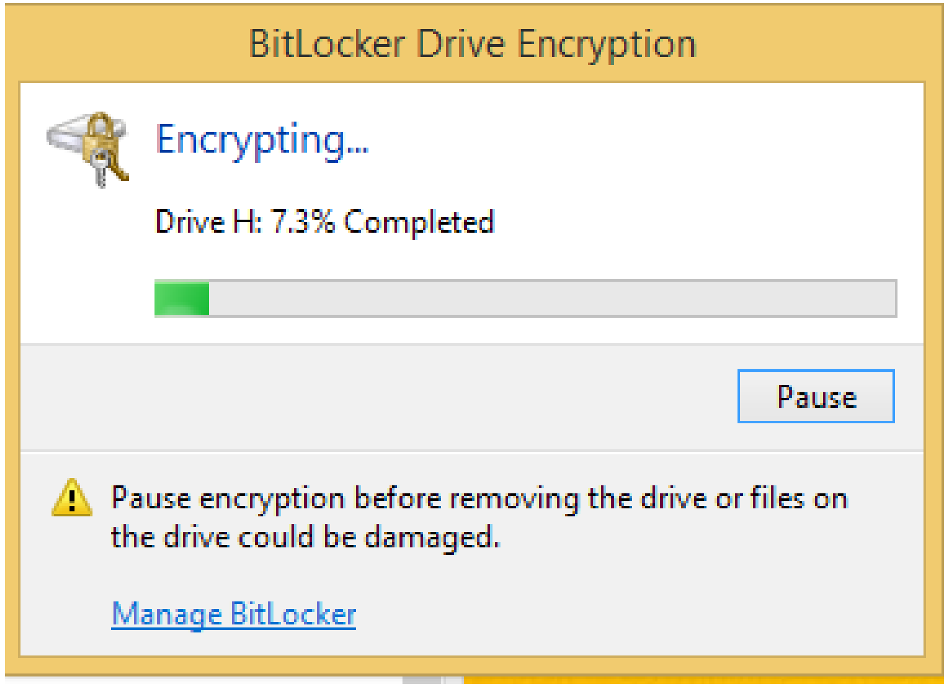


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Bitlocker

- Provides full disk encryption for the OS volume.
- BitLocker To Go encrypts removable storage devices.
- Recovery key backup (if loose or forget password)



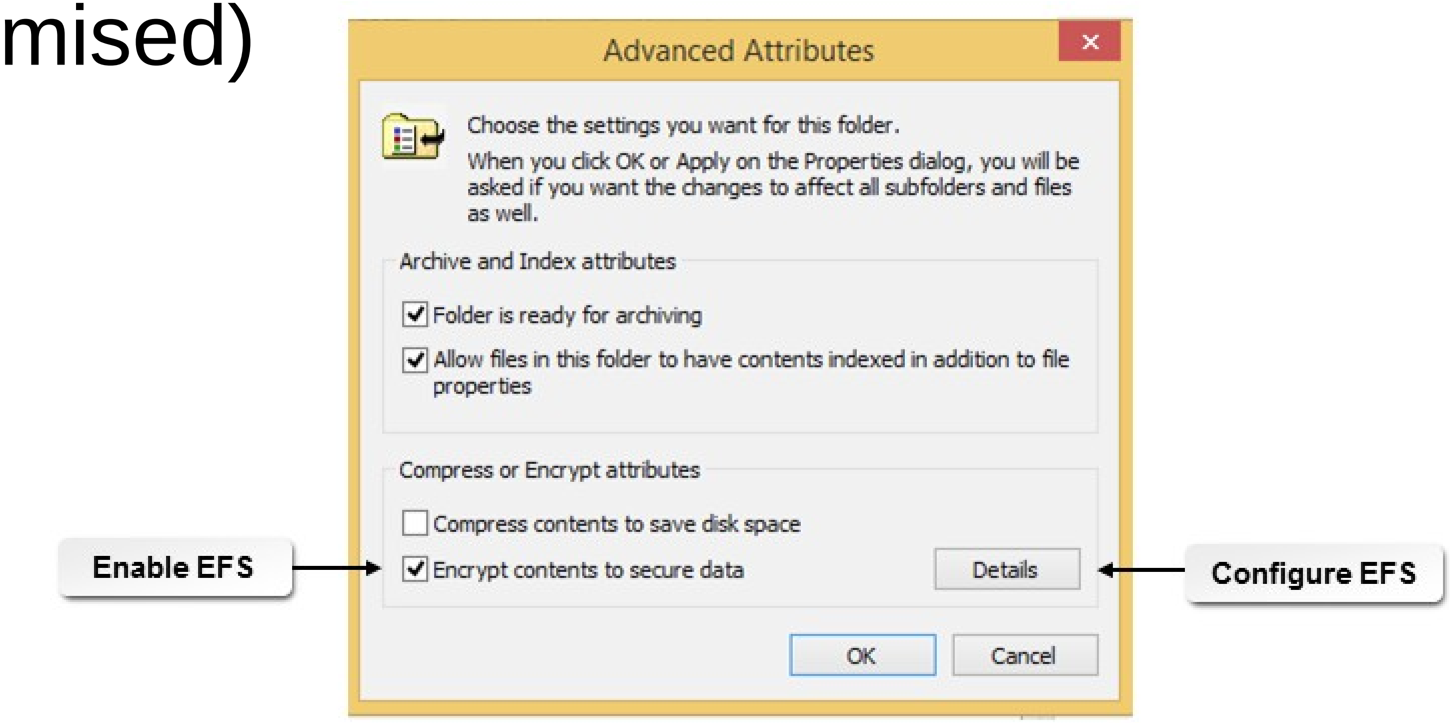
Encrypting...

Drive H: 7.3% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

EFS – Encrypting File System

- Only available on NTFS partitions
- Uses digital certificates to encrypt files
- Protects a files contents (even if NTFS permissions compromised)



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

Enable EFS

Configure EFS

Guidelines for securing MS Windows

- Log in as a standard user.
- Use Run as Administrator when you need administrative access.
- Provide the minimum permissions to achieve your access goals
- Verify that the combination of NTFS and share permissions provide the expected results:
  - No excessive rights assignment
  - No removal of needed rights
- Use multifactor authentication.
- Consider encrypting file systems

Password Best Practices

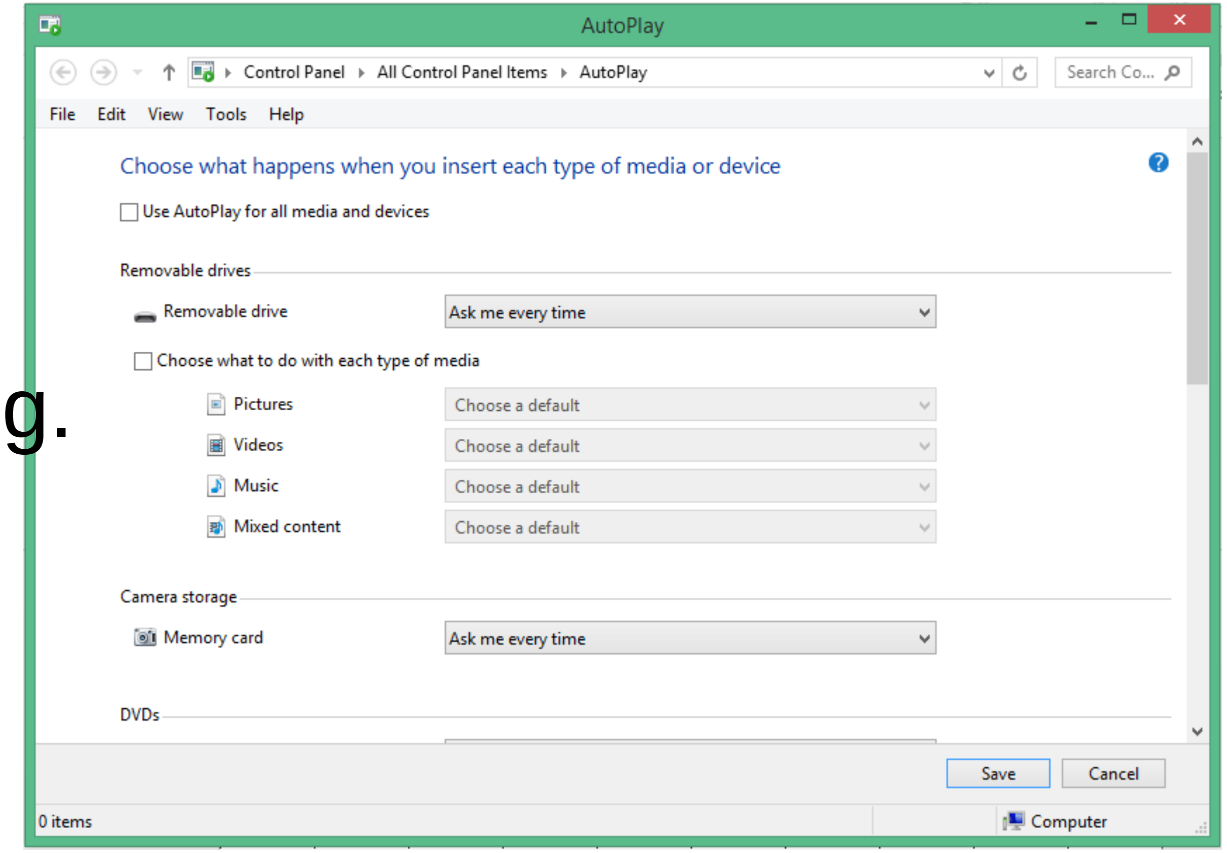
Best Practice	Description
Configuring password expiration	For most organizations, every two to three months is adequate. Some organizations might require more frequent changes.
Changing default user names and passwords	Devices like wireless routers come configured with default user names and passwords, which can be found by a simple Internet search. When you are adding these devices to your environment, change the user name and password to protect against unauthorized access.
Require screensaver passwords	When a user steps away from the computer, they should lock the computer. If they forget to do so, having a screensaver that comes on after one minute and requires a password to unlock the system has the same effect.
Require BIOS or UEFI passwords	Setting a BIOS or UEFI password will help prevent unauthorized users from accessing and changing firmware settings. If users make unauthorized changes to these settings, it might make their system stop working, make it work less efficiently, or make it out of compliance with organizational policies.
Require passwords	On most modern systems, you have to set a password in order to set up the computer. If you are working with older systems, or other devices that don't have passwords by default, you should configure the device to use a password. Smart phones and tablets might not be configured to require a password. Printers and routers might also not require a password to change settings. All of these devices should require passwords whenever possible.

Account Management Best Practices

Task	Description
Restrict user permissions	Follow the principle of least privilege.
Configure login time restrictions	Limit the days and hours that users can log in.
Disable the guest account	Windows guest accounts are disabled by default.
Configure failed login attempts lockout	Select a threshold for entering the wrong password before locking the account, and the amount of time the account should be locked.
Configure a timeout screen lock	Select a timeout interval for idle computers and mobile devices, and require that the password or another method be used to unlock the device.

Autorun

- Disable AutoRun (AutoPlay) on storage media:
  - Optical disc
  - USB drive
- Prevent embedded malware from self-installing.


AutoPlay
Control Panel ▸ All Control Panel Items ▸ AutoPlay
Search Co...
File Edit View Tools Help

Choose what happens when you insert each type of media or device

□ Use AutoPlay for all media and devices

Removable drives

Removable drive: Ask me every time

□ Choose what to do with each type of media

Pictures: Choose a default

Videos: Choose a default

Music: Choose a default

Mixed content: Choose a default

Camera storage

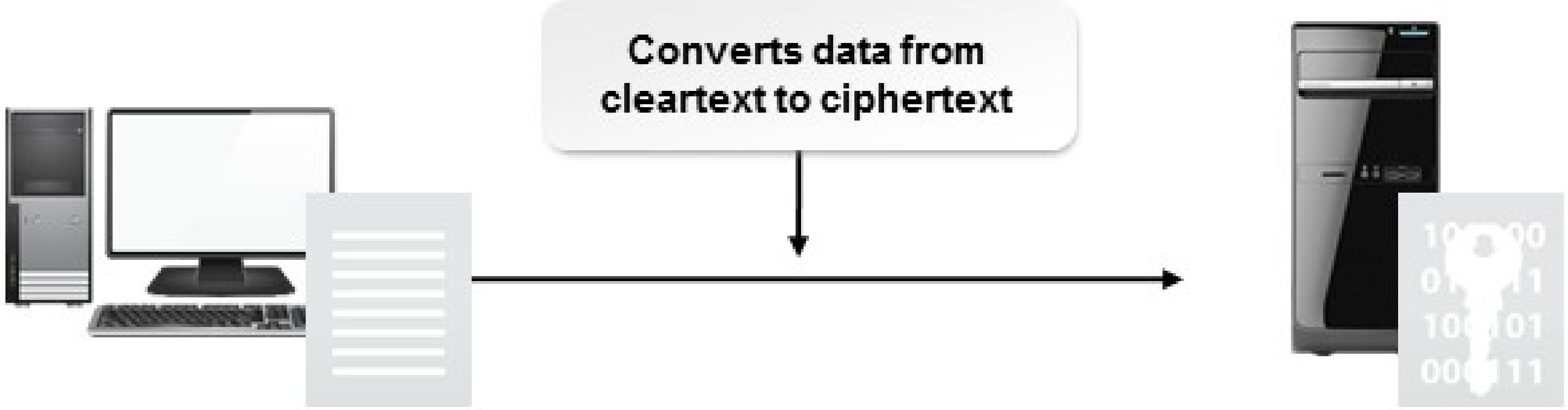
Memory card: Ask me every time

DVDs

Save
Cancel
0 items
Computer

Data Encryption

- Cryptography – convert cleartext (plain text) to ciphertext (coded)
- One way or two way



Data Encryption

- Cipher – actions used to encrypt data
- Enciphering – Applying ciphers to plaintext (to produce ciphertext)
- Reverse process is called deciphering

Patch Management

- Monitoring for, obtaining, evaluating, testing, and deploying integral fixes and updates for operating systems or applications.
- Organized patch management system (example):
  - A person responsible for reviewing vendor patches, security patches, and other updates.
  - A process for reviewing and categorizing updates (urgent, important, and non-critical).
  - An offline environment where urgent and important patches can be tested for functionality and impact.
  - Immediate administrative push delivery of approved urgent patches.
  - Weekly administrative push delivery of approved important patches.
  - Periodic review, testing, and rollout of non-critical patches.

Guidelines for securing Workstations

- Manage user authentication:
  - Default user name and password
  - Strong passwords
  - Multifactor authentication
- Install updates and patches:
  - OS and security updates
  - Application patches for OS utilities, web browsers, and application software

Guidelines for securing Workstations

- Manage user accounts:
  - Disable guest and unnecessary accounts
  - User permissions
- Educate users.
- Apply workstation security measures:
  - Install Antimalware software
  - Activate a Pop-up blocker
  - Install/Enable Firewall
  - Warnings and banners at login to warn users that only authorised use is allowed
  - Disable AutoRun and AutoPlay
  - Screensaver lock
  - Automatic OS updates
  - Limit Shared resources and use permissions

Secure SOHO Networks

- Normally less than 20 nodes
- Infrastructure mode – wireless devices use an access point (AP)
- Ad hoc mode – wireless devices can communicate with each other. No need for an AP. Devices operate peer to peer and are in close proximity to each other.

Secure SOHO Networks

- Change default user name and password.
- Enable MAC filtering. Simple and secure
- Assign static IP addresses. Good for very small networks (turn off DHCP)
- Disable unused ports.
- Configure firewall settings:
  - Enabling / disabling port security
  - Inbound and outbound filtering
  - Reporting and logging activity
  - Malware and Spyware protection
  - Pop up blocking
  - Port assigning, forwarding and triggering

Secure SOHO Networks

- Configure port forwarding and mapping. NAT is used on most SOHO routers to allow one IP address to the outside world.
- Use content filtering and parental controls. Can be configured to send an email report.
- Apply firmware updates to all devices connected.
- Apply physical security controls. Limit users access to the SOHO router.
- Perform security assessments to determine if the current controls are adequate.

Wireless Security

- Any method of securing a LAN to prevent unauthorised access
- Wireless networks more vulnerable to attacks.
- Configure the network settings:
  - Secure your wireless router or access point administration interface.
  - Disable remote administration.
  - Secure/disable the reset switch/function.
  - Change the default channel.
  - Regularly upgrade the Wi-Fi router firmware to ensure the latest security patches and critical fixes.
  - Use the Remote Authentication Dial-In User Service Plus (RADIUS+) network directory authentication where feasible.
  - Use a VPN.

Wireless Security

- Configure the SSID.
- Disable SSID broadcast.
- Enable encryption:
  - Enable WPA2 encryption.
  - Change the default encryption keys.
  - Avoid using pre-shared keys (PSK).
- Properly place the antenna and access point. Signals can extend beyond boundaries.

Wireless Security

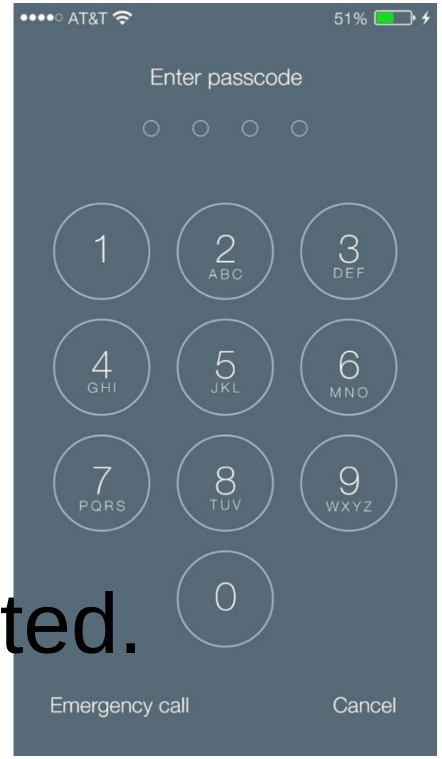
- Secure the WAP
  - Implementing some form of user authentication.
  - Implementing a security protocol that requires over-the-air data encryption.
  - Updating firmware on the device to implement any manufacturer security patches and enhancements.
  - Restricting unauthorized devices from connecting to the WAP by filtering out unauthorized MAC addresses.
  - Implementing a firewall. For a small office or home office, enable a firewall on the WAP, and then also on the host computer to further secure your network.
  - Configuring vendor-recommended security settings on your wireless router or access point
- Adjust radio power levels.
- Disable WPS as its vulnerable to brute force attacks
- Configure the workstation.

Wireless Security

- Do not auto-connect to open Wi-Fi networks.
- Enable firewalls on each computer and the router.
- Assign static IP addresses to devices to prevent inadvertent broadcasting of IP addresses to unauthorized parties.

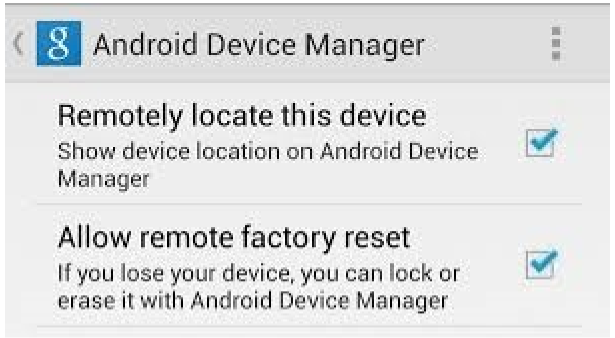
Secure Mobile Devices – Screen Lock

- Enable Screen Lock
- Enable with a passcode, a fingerprint, facial recognition, or a swipe pattern.
- Configure idle time before screen lock is activated.
- Organizational security policies.



Secure Mobile Devices – Remote Wipe

- Removes sensitive data from mobile devices.
- Useful if device is lost or stolen.
- Organisational security policies.
- Administrative rights for remote wipe.



Android Device Manager

Remotely locate this device ☑
Show device location on Android Device Manager

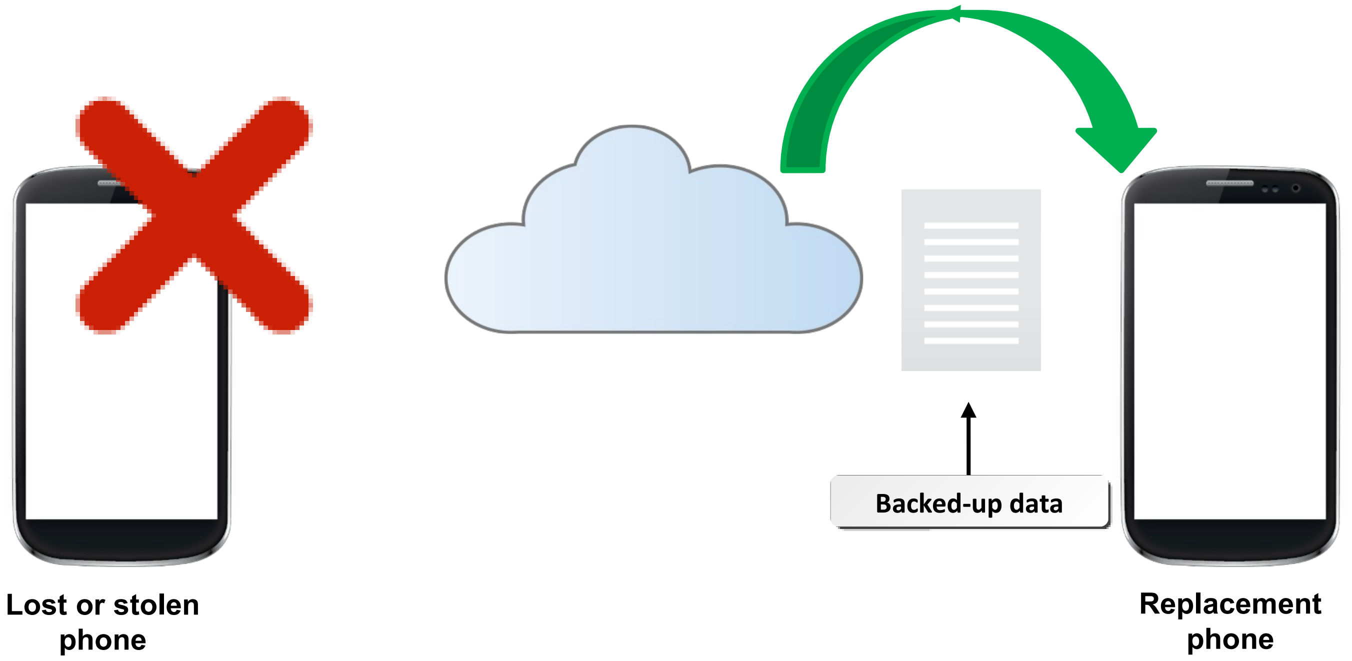
Allow remote factory reset ☑
If you lose your device, you can lock or erase it with Android Device Manager

Secure Mobile Devices – Locator Applications

- GPS tracking.
- Useful if device is lost or stolen.
- Third-party apps.
- Enable camera to help catch thief.

Secure Mobile Devices – Remote Backup

- Help with recovering data when a device is lost or stolen.
- OS-based:
  - iCloud
  - Google Drive



Secure Mobile Devices – Failed Login

- iOS device: disable after X failures to log on:
  - Up to 5: usually no action.
  - 5 to 10: disabled for 1 to 60 minutes.
  - More than 10: data deleted.
- Android device: disable after X failures to log on:
  - Unlocking the device will require the Google account details used to set up the device.

Secure Mobile Devices

- Install Antivirus and Antimalware applications
- Mobile OS Patches and Updates
  - Similar to updates for other computing devices.
  - Configure devices to update automatically.
- Enable Biometric Authentication
- Full Device Encryption

Secure Mobile Devices

- Multifactor Authentication
  - Combination of PIN and swipe pattern
  - Combination of biometrics and password
  - Authenticator app
    - Two-step authentication
- Only used trusted sources
  - Applications
  - Networks access

Secure Mobile Devices

- Policies and Procedures
  - Large organisations
    - Bring Your Own Device (BYOD)
    - Corporate Owned, Personally Enabled (COPE)
  - Security profiles
    - Policies
    - Procedures
    - Standards
    - Baselines
    - Guidelines