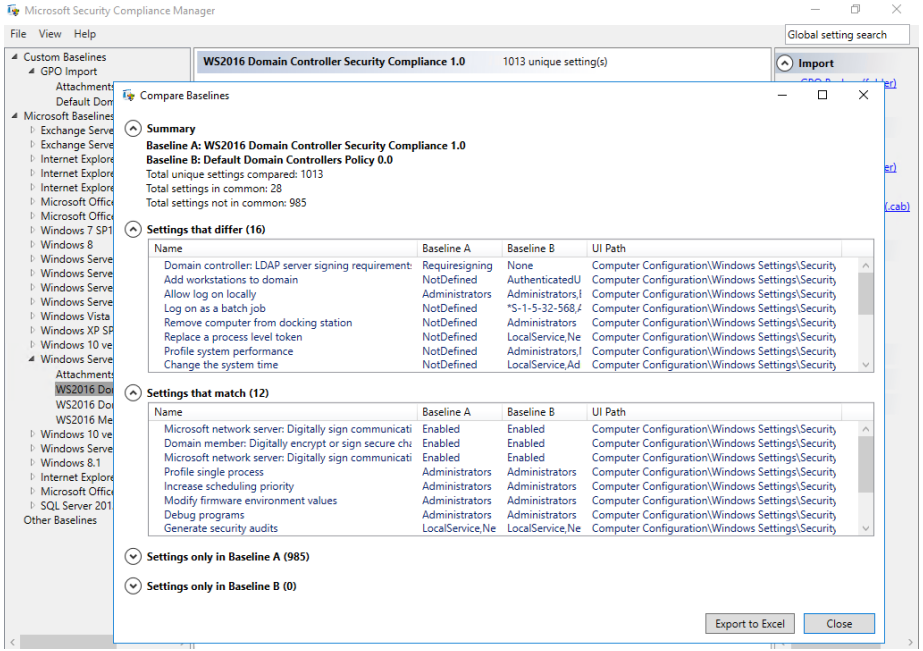
SEC+
Lesson 10:
Assess Endpoint Security Capabilities

Lesson 10

Topic 10A

Implement Endpoint Security

Endpoint Hardening

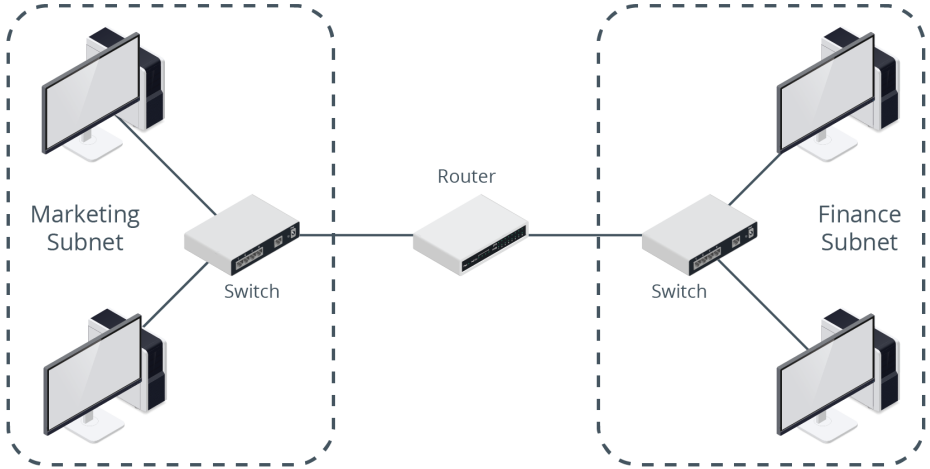


Using Security Compliance Manager to compare settings in a production GPO with Microsoft's template policy settings. (Screenshot used with permission from Microsoft.)

- Operating System Security
  - Workstations
  - Servers
- Baseline Configuration
  - Interfaces
  - Services
  - Ports
  - Storage
  - Many others

Endpoint Protection

- Segmentation
- Isolation
- Antivirus and Antimalware
- Disk Encryption
- Patch Management

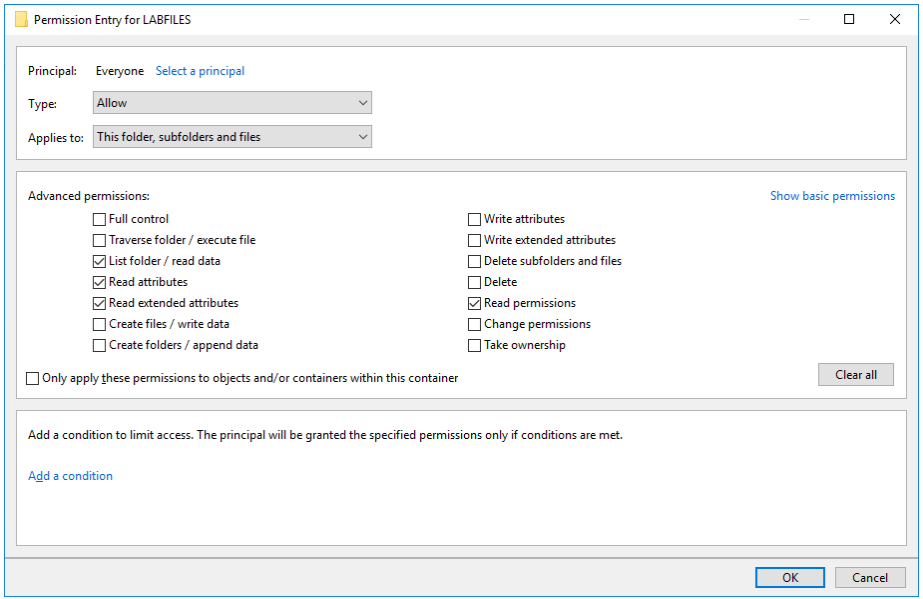


A segmented network showing Marketing and Finance subnets and the placement of network devices. Traffic between the two networks is controlled by the router. (Images © 123RF.com.)

Advanced Endpoint Protection

- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Host-Based Intrusion Detection/Prevention (HIDS/HIPS)
- User Behavior Analytics (UBA)/User and Entity Behavior Analytics (UEBA)

Endpoint Configuration



Configuring an access control entry for a folder. (Screenshot used with permission from Microsoft.)

- Principle of Least Privilege
- Access Control Lists
- File System Permissions
- Application Allow Lists and Block Lists
- Monitoring
- Configuration Enforcement
- Group Policy
- SELinux

Hardening Techniques

- Protecting Physical Ports
- Encryption
  - Full Disk Encryption (FDE)
  - Removable Media Encryption
  - Virtual Private Networks (VPNs)
  - Email Encryption
- Host-Based Firewalls and IPS
- Endpoint Protection
- Changing Defaults
- Removing Unnecessary Software

Hardening Specialized Devices

- ICS/SCADA
  - Strict network segmentation
  - Robust authentication
  - Unidirectional gateways (or data diodes)
    - Limit data flow to one direction
- Embedded and RTOS
  - Select devices based on security capabilities

Endpoint Security

- Endpoint Hardening
- Endpoint Protection
- Advanced Endpoint Protection
- Endpoint Configuration
- Hardening Techniques
- Hardening Specialized Devices

Lesson 10

Topic 10B

Mobile Device Hardening

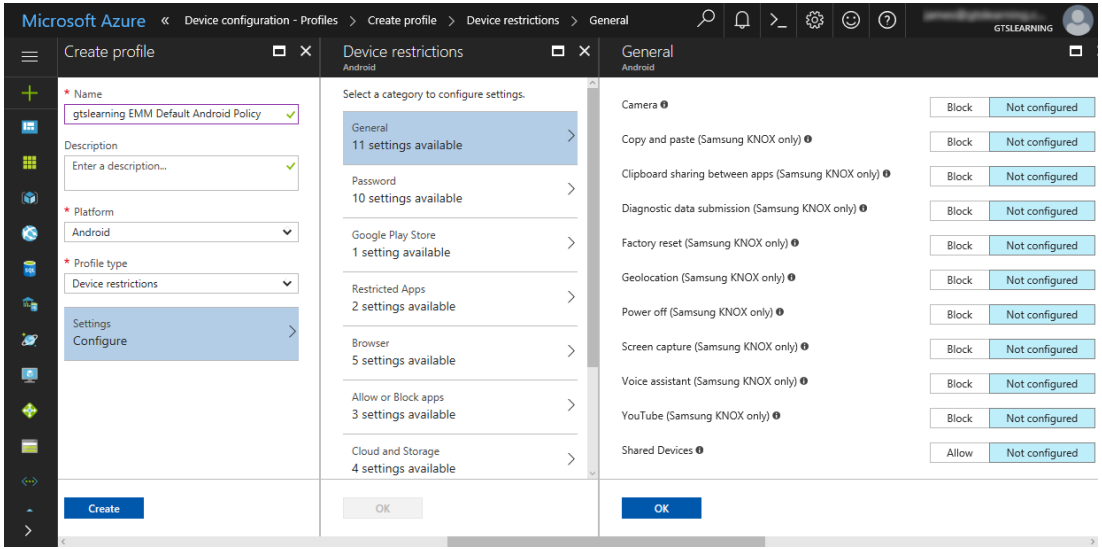
Mobile Hardening Techniques

- Many similarities between hardening mobile devices or traditional computers
- Mobile devices are more prone to physical loss or theft
- Deployment Models
  - Bring your own device (BYOD
  - Corporate owned, business only (COBO)
  - Corporate owned, personally enabled (COPE)
  - Choose your own device (CYOD)
- Mobile Device Management
- Full Device and External Media Encryption

Full Device Encryption and External Media

- In iOS, there are various levels of encryption
  - All user data on the device is always encrypted
  - Email data and any apps using the “Data Protection” option are subject to a second round of encryption
- In iOS, Data Protection encryption is enabled automatically when you configure a password lock on the device
- A mobile device contains a solid state (flash memory) drive for persistent storage of apps and data

Location Services

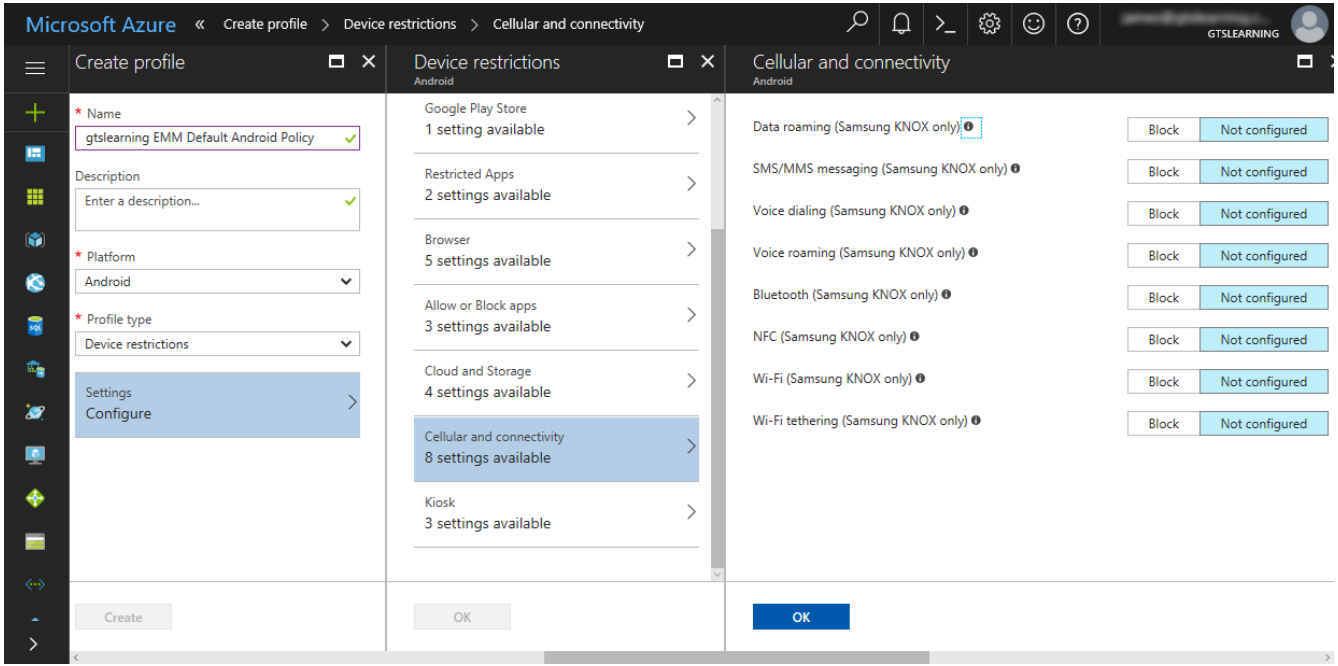


Restricting device permissions such as camera and screen capture using Intune. (Screenshot used with permission from Microsoft.)

- Global Positioning System (GPS)
- Indoor Positioning System (IPS)
- Geofencing
- GPS Tagging (ex. EXIF Data)
- Primary concern of location services is privacy

Cellular and GPS Connection Methods

- Cellular/Mobile Data Connections
- Global Positioning System (GPS)



Locking down Android connectivity methods with Intune—note that most settings can be applied only to Samsung KNOX-capable devices. (Screenshot used with permission from Microsoft.)

Wi-Fi and Tethering Connection Methods

- Mobile devices usually default to using a Wi-Fi connection
  - Home/Public vs Enterprise Network
  - Rogue/Evil Twin networks
- Personal Area Networks (PANs)
  - Peripherals
  - Other devices/computers
- Ad Hoc Wi-Fi and Wi-Fi Direct
- Tethering and Hotspots

- Mobile Hardening Techniques
- Full Device Encryption and External Media
- Location Services
- Cellular and GPS Connection Methods
- Wi-Fi and Tethering Connection Methods
- Bluetooth Connection Methods
- Near-Field Communications and Mobile Payment Services

Lesson 10

Summary