9.6.4 Enforcing Mobile Device Security Facts

One of the key problems associated with managing mobile devices is the fact that they can't be joined to a Windows domain. This means Group Policy can't be used to automatically push security settings to mobile devices.

This lesson covers the following topics:

- Mobile device management (MDM)
- Windows Intune
- Windows Intune configurations
- System configuration for Windows Intune

Mobile Device Management (MDM)

One option you can use instead of Group Policy is mobile device management (MDM). Its security settings include the following:

- Security settings can be manually configured on each individual device. This option doesn't require any additional infrastructure to be implemented. However, it can be a time-consuming task for the administrator (especially in a large organization with many mobile devices) and is not recommended.
- For devices running Apple's iOS operating system, security settings can be distributed in a configuration profile for users to install. The profile can be defined so that only an administrator can delete the profile, or you can lock the profile to the device so that it cannot be removed without completely erasing the device. This option also doesn't require any additional infrastructure for implementation. However, it does rely on the end user to actually implement the profile, which can be problematic. Additionally, it is not a dynamic strategy, so making even the smallest change to your mobile device security policies would require a great deal of effort to implement.
- A mobile device management solution that pushes security policies directly to each device over a network connection can be implemented. This option enables policies to be remotely enforced and updated without any action by the end user. Many companies have MDM products, including Apple, Cisco, and Microsoft.

Windows Intune

One widely used MDM solution is Windows Intune, which provides cloud-based mobile device management that allows you to remotely manage and secure mobile devices (as well as standard desktop systems starting with Windows 7 or later). Intune cannot by used to manage Windows Server. The table below shows which operating systems Windows Intune currently supports:

Device	Supported
Apple	▪ Apple iOS 8.0 and later ▪ Mac OS X 10.9 and later
Windows	▪ Windows 10 (Home, S, Pro, Education, and Enterprise versions) ▪ Windows 10 Mobile ▪ Windows Phone 8.1 ▪ Windows 8.1 RT ▪ PCs running Windows 8.1 ▪ Devices running Windows 10 IoT Enterprise (x86, x64)

	▪ Devices running Windows 10 IoT Mobile Enterprise ▪ Windows Holographic & Windows Holographic Enterprise
Google	▪ Google Android 4.0 ▪ Google Android for Work

Customers with enterprise management + security (EMS) can also use Azure Active Directory (Azure AD) to register Windows 10 devices.

Windows Intune Configurations

Windows Intune can be deployed in two different configurations:

- Intune Standalone is the recommended deployment method. Intune Standalone is a cloud-only solution that is managed using a web console that can be accessed from anywhere with internet access.
- Hybrid MDM with Configuration Manager is a solution that combines Intune's mobile device management capabilities into Configuration Manager. It uses Intune for policies, profiles, and applications for devices, but it uses Configuration Manager to administer content and manage the devices.

> This course covers only cloud-only deployments. Deploying Intune in United Configuration Mode requires experience and skill beyond the scope of this course.

You must first sign up for an account at Microsoft's website before you can use Intune. After you sign up for an Intune account, you can manage the deployment using the following Intune Management Portals:

- Account Portal (https://account.manage.microsoft.com) is used to manage subscriptions, users, groups, and domains. End users can also use the account portal to manage their passwords.
- Admin Portal (https://admin.manage.microsoft.com) is used to manage enrolled devices and policies.
- Company Portal (https://portal.manage.microsoft.com) is used by end users to manage their own account and enroll devices.

System Configuration for Windows Intune

After signing up for a Windows Intune subscription, you need configure the system by completing the tasks listed in the table below:

Configuration Task	Description
Add Intune users	Windows Intune uses administrative and standard users. The first user account created when you sign up for an Intune subscription is made an administrator by default. Additional standard users can be created and managed using the account console by selecting **Management** > **Users** > **New** > **User**. You can also synchronize users and groups into the account console from your Active Directory domain.

Define Intune policies	Intune policies allow you to manage your mobile devices. You can perform tasks such as: ▪ Configuring security settings ▪ Applying updates ▪ Configuring firewall settings Policy settings can be applied to both standalone and domain-joined devices. However, policy conflicts can occur with domain-joined devices. To prevent this from happening, verify that domain-joined devices are not configured to receive the same configuration settings from both Active Directory Group Policies and Windows Intune. Intune provides the following policy templates containing recommended settings that you can deploy: ▪ Mobile Device Security Policy ▪ Windows Firewall settings ▪ Windows Intune Agent settings ▪ Windows Intune Center settings To set up your Intune policies, access the admin console and select Policy > **Add Policy**. Select the policy you wish to deploy and select **Create and Deploy a Policy**. At a minimum, it is recommended that you deploy all of the above policies using the default settings and apply them to either all devices or all users. If necessary, you can later modify the default settings in the policy. You can also configure specific devices or users that a policy applies to.
Manage users and groups	Windows Intune uses two types of groups: ▪ User groups allow you to deploy software and mobile device security polices to specific user accounts. ▪ Device groups allow you to deploy software, Intune agent settings, and firewall settings to specific devices. To add groups using the Account Console, select Admin > Security Groups > New > **Group**.
Enroll computers	You can enroll standard computer systems (desktops and notebooks) in Windows Intune in one of two ways: ▪ Administrator enrollment requires an Intune administrator to set up the enrollment for a specific user. ▪ User enrollment allows a user to enroll a computer through the Company Portal. Before you can enroll a system in Intune, you must first download and install the Intune client software on the computer. To do this using administrator enrollment, complete the following: 1. Open a browser and access the Admin Console. 2. Select Administration > Client Software Download > **Download Client Software**. 3. Once this zip file has downloaded, extract its contents and run the **Windows_Intune_Setup.exe** file as an administrator user.

	4. After the installation is complete, restart the computer. The newly managed computer should appear in the Intune Admin Console after a few minutes. Administrator-enrolled computers must be manually linked to an Intune user ID. In the Admin Console, go to Groups > All Devices; then select the device and select **Link User**. A user can self-enroll a computer by opening a browser, accessing the company portal, and logging in using his or her Intune user ID. Then he or she can select the option to enroll the current device. User-enrolled devices are automatically linked to the user ID that enrolled them.
Enroll mobile devices	To enroll mobile devices in Intune, you must first enable mobile device management in the Admin Console. Select the Administration workspace; then select Mobile Device Management > **Set Mobile Device Management Authority** > **Yes**. Users must configure mobile devices with the address of the Intune enrollment server (enterpriseenrollment-s.manage.microsoft.com) during the enrollment process. Be sure users are provided with this address prior to starting the device enrollment process. At this point, Windows RT mobile devices can be enrolled with Windows Intune. To enroll a Windows RT device, search for and run **Company Apps**; then enter your Intune user ID and password along with the address of the enrollment server. Once enrolled, select the link displayed to install the management app from the Windows store. If you want to enroll other types of mobile devices, you must configure Intune for each platform you plan to support. For example, if you want to manage iOS devices, you must obtain an Apple Push Notification service (APNs) certificate and then upload it to Intune. Alternatively, if you plan to support Windows Phone 8 devices, you must get a Windows Phone Dev Center account and upload a signed enterprise mobile code certificate to Intune.