



Windows Store apps

A deployment guide
for education

January 2014

Table of contents

3 Planning app deployment

- 3 Overview of user accounts used in Windows Store app deployment
- 4 Plan for Windows Store app deployment
- 8 Plan for app sideloading
- 13 Plan for when to deploy apps
- 13 Select the right app deployment method

18 Deploying apps after operating system deployment

- 18 Use only the Windows Store
- 23 Use only sideloading
- 26 Use both the Windows Store and sideloading

27 Deploying apps during operating system deployment

- 28 Use MDT
- 29 Using the command line

31 Windows Store app deployment FAQ

Window Store apps

A deployment guide for education

The Windows 8.1 operating system builds on the feature and capabilities in Windows 8. One prominent feature is the Windows Store apps. Educational institutions can purchase or create apps for Windows 8.1 that use the new Windows user interface (UI).

But Windows Store apps can raise certain questions:

- What is the best way to deploy Windows Store apps in an educational environment?
- Do all the apps need to come from the Windows Store?
- Can you use existing deployment technologies and processes to deploy them?
- What role does the Windows Store play in the app deployment process?

This guide offers several examples of app deployment strategies and considerations when selecting among them. It is written for school district IT pros, school administrators, teachers, and other faculty who are responsible for deploying Windows Store apps on institution-owned or personally owned devices.

A sample scenario for an educational institution and two user personas provides the backdrop. First is Amy, who is the IT manager for the institution. Second is Mark, who teaches at the institution and has been designated the lead faculty member for Windows 8 device and app deployment. This guide follows Amy and Mark as they deploy Windows Store apps to devices owned by the institution, faculty, and students.

As a starting point, Amy and Mark create a list of Windows Store apps, web apps, and Window desktop applications to be deployed to the faculty and students. They also identify several planning and deployment considerations to address, which include:

- Identifying the resources available to support Windows Store app deployment
- Selecting the best method for deploying Windows Store apps—through the Windows Store or by using *sideloading* (that is, deploying apps without using the Windows Store)

- Determining how apps can be purchased and deployed in bulk to faculty and students
- Providing appropriate degree of flexibility in what apps faculty and students can use on devices
- Identifying how app deployment methods affect app ownership models

These and other considerations are discussed as part of this guide.

The following is a list of assumptions about the institution-owned devices described in this guide:

- The devices are domain joined.
- Users log on to their device by using an institution-issued account instead of their own Windows account (and possibly Microsoft account).
- A Microsoft account may or may not be associated with the user's institution-issued account.
- Some devices may be running Windows 8.1 Enterprise edition.

NOTE

Although much of this guide is applicable to both Windows 8.1 and Windows RT 8.1 devices, this guide focuses on Windows Store app deployment to Windows 8.1.

Planning app deployment

As the first step in deploying Windows Store apps, Amy and Mark review the methods available. Amy and Mark discover that they can deploy Windows Store apps by using the Windows Store, sideloading, or a combination of the two. Amy and Mark considered the information in the following sections when planning their app deployment.

Overview of user accounts used in Windows Store app deployment

Windows 8.1 supports a superset of the user accounts supported in the Windows 7 operating system. The following is a list of the user account types that Windows 8.1 supports:

- **Windows account** This account is stored locally on the Windows 8.1 device (local Windows account) or in an on-premises Active Directory Domain Services (AD DS) domain. This account is identical to the user accounts Windows 7 uses. For domain-joined devices, you can centrally provision and manage Windows accounts by using on- or off-premises AD DS domains.
- **Microsoft account** This Internet-based account is used to access the Windows Store or other services that use Microsoft accounts (previously known as the *Windows Live ID*). This account is used to locate, install, and update Windows Store apps. You can associate a Microsoft account with an existing Windows account.

When users create a Microsoft account, they are asked to verify the account information. This process is done by sending an email to the account with a hyperlink to verify the information.

Users can also designate devices that are trusted by them. This allows users to specify specific devices that are available for performing administrative tasks, such as changing user information or their password.

NOTE

You can use a Windows account to log on to a Windows 8.1 computer but not to access the Windows Store.

Only one Microsoft account can be associated with a Windows account at a time, but you can change the Microsoft account associated with a Windows account at any time. You cannot centrally provision and manage Microsoft accounts. Instead, users will need to obtain their own Microsoft account.

Microsoft accounts cannot be centrally managed—that is, IT cannot create and manage them. Instead, each user is responsible for creating and managing their Microsoft account.

Microsoft accounts in the United States comply with the Children's Online Privacy Protection Act (COPPA) regarding online account creation for children under 13 years of age. To verify that an adult is giving a child permission to create a new Microsoft account, COPPA requires that a small amount (\$0.50) be charged to the adult's credit card.

- **Windows Azure Active Directory account** This Internet-based account is stored in the Windows Azure AD service (which might have been migrated from or integrated with an on-premises AD DS infrastructure). Microsoft Office 365 and Windows Intune use the Windows Azure AD service to store credentials, and you can centrally provision and manage Windows Azure AD accounts.

You can use the email address associated with a Windows Azure AD account (for example, an Office 365 email address) to create a Microsoft account, but associating the two accounts does not allow for synchronization of the credentials, as there are still two separate credential stores and the accounts remain separate and distinct.

NOTE

You can use a Microsoft account to log on to a Windows 8 machine. A Microsoft account is also required to access the Windows Store.

NOTE

You cannot use a Windows Azure AD account to log on to a Windows 8.1 device. You can only use a Windows Azure AD account to access services, such as Office 365 and Windows Intune.

Plan for Windows Store app deployment

The Windows Store is a digital distribution system. It is the primary distribution platform for the new types of applications available in Windows 8.1 and Windows RT called *Windows Store apps*. However, publishers can also use the Windows Store to provide listings for desktop applications certified to run on Windows 8.1 devices and can find links to the developer's website for more information or to purchase the desktop application.

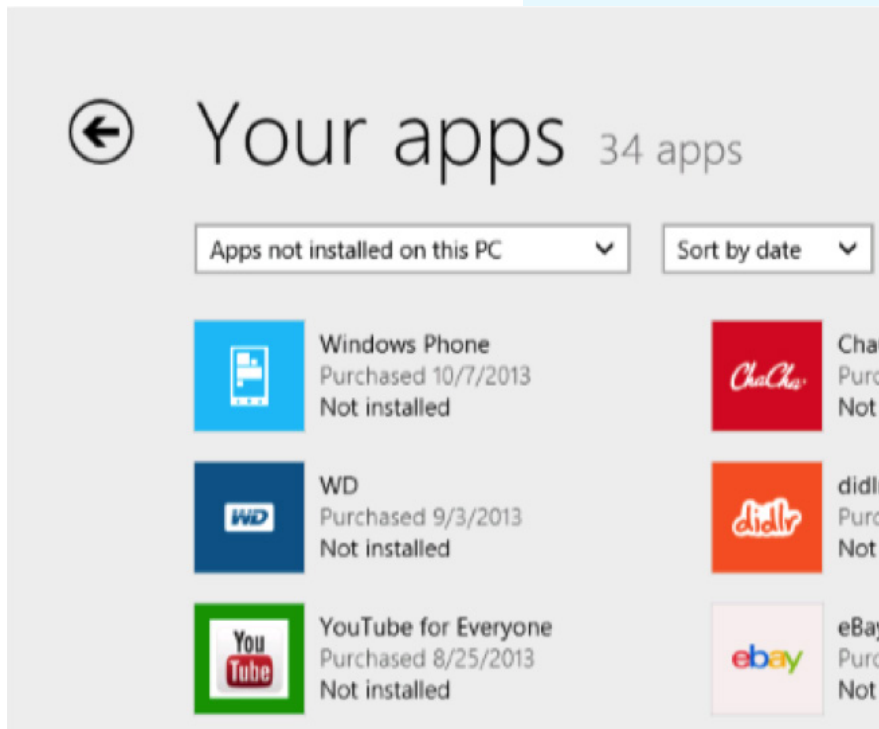


FIGURE 1 Your apps in the Windows Store

After you use your Microsoft account to purchase an app from the Windows Store, you can install it on up to 81 devices (for Windows 8, the limit was five devices). Users can open **Your apps** (acquired by the Microsoft account) in the Windows Store (as Figure 1 shows) to install apps from the Windows Store on other devices, view all of their apps, and see which apps are installed on their devices. Web apps and desktop applications are not displayed in **Your apps**.

Amy and Mark review the features and benefits, listed in Table 1, of using Windows Store for app deployment.

TABLE 1 Windows Store App Deployment Features and Benefits

FEATURE	DESCRIPTION
App installation	<ul style="list-style-type: none"> • Users can install apps on Windows 8.1 devices by using the Store app (found on the Start screen), which supports a self-service app deployment model. • Users can use their Microsoft account to install an app on as many as five devices. • Apps are installed on a per-Windows account basis from the Windows Store by using the Microsoft account associated with the Windows account. • An app must be installed for each Windows account that uses a device, even if another Windows account installed the app.
App update	<p>After an app is installed, updates to the app are automatically detected and installed. This is a change in behavior from Windows 8, where the user was notified of the updates in the Store app, then installed the updated version of the app from the Windows Store. In Windows 8, the user initiated the installation, and there was no method to push app updates. As mentioned, Windows 8.1 updates apps automatically, ensuring that users run the latest versions. App updates can be installed regardless of whether the user has a Microsoft account.</p>
Microsoft account integration	<ul style="list-style-type: none"> • Users must have a Microsoft account to access the Windows Store and purchase and install apps. Some apps require authentication within the app by using a Microsoft account or the account the app developer uses to run (even if the app is already installed on the device). • The apps are associated with the Microsoft account but are installed on the Windows account that is configured to use the Microsoft account for Windows Store access. This means that if a user uses a Microsoft account to install an app to a Windows account, then changes the Microsoft account associated with the Windows account, installed apps are unchanged. • User and app settings will roam if the user uses a Microsoft account or a local or domain account that has a Microsoft account associated with it to log on, but if the user uses a local Windows account to log on, user and app settings do not roam by default. To allow user and app settings to roam, consider employing products such as Microsoft User Experience Virtualization (UE-V).

FEATURE	DESCRIPTION
App purchase	<p>With Windows 8.1, the Windows Store makes the purchase of paid apps and in-app purchases more accessible. In the Windows Store, users are able to:</p> <ul style="list-style-type: none"> • Purchase stored value as a redeemable code from non-Microsoft e-commerce sites • Purchase stored value as a card with a redeemable code from partner stores • Send or give a specified amount of Windows Store credit as a gift to someone else • Store redeemed credit with a Microsoft account for later use <p>When users enter a redeemable code into their account, the specified amount is added to the stored value associated with the their Microsoft account. The users can then apply the credit to purchases on other Microsoft platforms, such as Windows Phone, that are accessed with the same account.</p> <p>When a user decides to purchase an app, the stored account value is treated as the default payment method, provided that the balance is not zero. If there are insufficient funds to complete the transaction, the Windows Store prompts the user to cover the remainder by using an alternative payment method.</p> <p>Note A stored value is redeemed into a billing account specific to its country and currency. The redeemed value can be used only on apps (and in-app purchases) available in that market.</p>
Privacy and protection	<ul style="list-style-type: none"> • The Windows Store shows content (such as screenshots or app descriptions) for apps that is appropriate for people 12 years of age and older. This means that users can browse apps for audiences 16 years of age and older in the Windows Store, but the content shown for the apps is approved for those 12 years of age and older. <p>In some countries, the standards for considering content inappropriate vary. Check the regulations for a specific country to determine the level of appropriateness of content.</p> <ul style="list-style-type: none"> • The Windows Store app certification process includes a step that scans the app for malware to help prevent uploading infected apps to the Windows Store (as described in the section “Security tests” in the article Submitting your app at http://msdn.microsoft.com/en-us/library/windows/apps/br230835.aspx).
Discovery and information	<p>The Windows Store categorizes and catalogs apps by type. You can also find apps by searching the store. The Windows Store provides app previews and reviews, but there is no method for viewing the Windows Store through a web browser at this time. You also cannot filter apps by categories or types. Category and type metadata is for informational purposes only.</p>

Amy and Mark also review the high-level process for using the Windows Store to deploy an app:

1. Sign up for a Microsoft account.
2. Configure security appliances to support the Windows Store (such as firewalls or web proxies).
3. Associate the Microsoft account from step 1 with the appropriate Windows account.
4. Find apps in the Windows Store.
5. Purchase apps from the Windows Store.
6. Install apps from the Windows Store.

For details on how to use the Windows Store to deploy an app, see the section “Use only the Windows Store” on page 18 in this guide.

NOTE There is a limit to the number of Microsoft accounts users can create from a specific IP address each day. Currently, that number is three Microsoft accounts. Contact Microsoft Support if you receive an error indicating that you cannot create more accounts at the IP Whitelist exception site at <https://support.live.com/eform.aspx?productKey=wlidipexc&ct=eformts&st=1&wfxredirect=1>.

Plan for app sideloading

Sideloading is a process for installing Windows Store apps without using the Windows Store. To sideload an app, you must have access to the app installation files (.appx and related files), which you can obtain from the app developer (either internally or from an independent software vendor). You cannot obtain app installation files to be used for sideloading through the Windows Store.

For apps you install by sideloading, you are responsible for validating and signing them, as sideloading bypasses the validation

requirements of the Windows Store. Also, you are responsible for deploying any app updates to their users.

IT pros often perform sideloading by using an *enterprise app store*. An enterprise app store provides similar features to the Windows Store but is exclusive to an organization. You can create such a store by using an electronic distribution system, such as Microsoft System Center 2012 R2 Configuration Manager or Windows Intune. An enterprise app store allows you to manage the app through the entire software life cycle, including deployment, updates, supersedence, and uninstallation.

Types of sideloading available include:

- **Deploy an app to all Windows accounts on a device**
This method allows you to deploy the app to all Windows accounts on targeted devices when you want to include one or more apps as a standard part of the user experience on the device. Conceptually, these apps are similar to the Windows 8 built-in apps and are also known as *provisioned apps*. Only 24 provisioned apps can be installed in an image. This is a common scenario when multiple students or faculty members use a shared device. Use this method as a part of the image-creation process, not for the ongoing management of apps on an existing operating system.
- **Deploy an app to a specific Windows account on a device**
This method allows you to selectively deploy apps to specific Windows accounts. Conceptually, these apps are similar to those obtained through the Windows Store and are also known as *installed apps*. The apps must be deployed to each Windows account on a device.

NOTE

A Windows account can be a domain-based account or a local account. You can associate a Microsoft account with either type of Windows accounts.

Amy and Mark review the types of sideloading in the previous list to identify which is best for their needs. Ultimately, they decide that a combination of both types is required. Amy and Mark also read that before they can sideload an app, they must make certain that the apps and Windows 8 devices are ready for sideloading. Amy and Mark reviewed the following app prerequisites:

- **Prerequisites for running a sideloaded app** Table 2 on page 10 lists the prerequisites for running a sideloaded app.

- **Running a sideloaded app** After you install a sideloaded app on a device, the app tile on the Start screen shows an **X** in the bottom right corner of the tile until the device meets all sideloading requirements. The **X** indicates that a problem is preventing the app from running.
- **Certificate used for app signing** The devices running the app must trust the root certification authority (CA) for the certificate used for app signing. This trust is typically accomplished by signing the application with a certificate from a trusted CA or by adding the root CA to the trusted root in the certificate store on the targeted devices. The app developer is responsible for ensuring that the app is properly signed.

TABLE 2 Prerequisites for Running a Sideloaded App

PREREQUISITE	DESCRIPTION
All devices	Enable the Allow all trusted applications to install Group Policy setting. For more information how to enable this setting, see the section, "To set Group Policy for sideloading," in the topic "How to Add and Remove Apps" at http://technet.microsoft.com/en-us/library/hh852635.aspx#SideloadRequirements .
Device that is not domain joined running Windows 8.1 Enterprise or devices running Windows 8.1 Pro or Windows RT 8.1	<p>Activate a sideloading product key for each device. For more information about:</p> <ul style="list-style-type: none"> • Obtaining a sideloading product key, see the <i>Windows 8 Licensing Guide</i> at http://go.microsoft.com/fwlink/?LinkId=267899. • Activating a sideloading product key, see the section "To activate a sideloading product key" in the topic "How to Add and Remove Apps" at http://technet.microsoft.com/en-us/library/hh852635.aspx. <p>You can upgrade an existing Windows 8 edition to Windows 8 Pro by purchasing the appropriate upgrade, as describe at http://windows.microsoft.com/en-us/windows-8/feature-packs. Upgrades to Windows 8.1 Enterprise are available based on Microsoft Volume Licensing agreements, as described at http://technet.microsoft.com/en-us/library/jj203353.aspx.</p>

The following is a list of the technologies you can use to perform app sideloading:

- **Command line** Sideload apps by using Deployment Image Servicing and Management (DISM), the **Add-AppxProvisionedPackage** Windows PowerShell cmdlet, or the **Add-AppxPackage** Windows PowerShell cmdlet. To provision an app to:
 - All users on a device, use DISM or the **Add-AppxProvisionedPackage** cmdlet
 - A specific user on a device, use the **Add-AppxPackage** cmdlet

- **Microsoft Deployment Toolkit (MDT) 2013** MDT automates provisioning apps to all users on a device during the operating system deployment process. MDT allows you to create a list of applications that can be selected at the time of deployment and provides a unified console for managing apps during operating system deployment. It can integrate with System Center 2012 Configuration Manager to enhance operating system deployment.
- **System Center 2012 R2 Configuration Manager** System Center 2012 R2 Configuration Manager automates deploying apps to a user after the operating system deployment process. With it, you can create a list of applications for deployment through the Application Catalog. System Center 2012 R2 Configuration Manager provides a unified console for managing apps and can integrate with MDT to enhance operating system and app deployment.
- **Windows Intune** Windows Intune automates deploying apps to a user after the operating system deployment process. Windows Intune can integrate with System Center 2012 R2 Configuration Manager to provide a hybrid method of managing app deployment. Windows Intune supports a self-service model by using the Company Portal app.

Table 3 lists criteria for selecting technologies to performing app sideloading. You can use any combination of these technologies to sideload an app. For example, you may decide to use System Center 2012 R2 Configuration Manager with for institution-owned devices and Windows Intune for personally owned devices.

TABLE 3 App Sideload Technology Selection

	COMMAND LINE	MDT	SYSTEM CENTER 2012 R2 CONFIGURATION MANAGER	WINDOWS INTUNE
Can be used by any electronic software distribution (ESD) or other methods (such as logon scripts)	Yes	No	No	No
Device domain membership	Domain joined or stand-alone	Domain joined or stand-alone	Domain joined or stand-alone (recommended to integrate with Windows Intune for stand-alone devices)	Domain joined or stand-alone

	COMMAND LINE	MDT	SYSTEM CENTER 2012 R2 CONFIGURATION MANAGER	WINDOWS INTUNE
Provides a unified solution for the entire app life cycle, including installation, updates, supersedence, and removal	No	No	Yes	Yes
Supports creation of an enterprise app store	No	No	Yes	Yes
Provides highly automated deployment process	No	Yes	Yes	Yes
Supports a push deployment model	Yes	Yes	Yes	No
Supports a self-service deployment model	No	No	Yes	Yes
Can be used for institution-owned devices	Yes	Yes	Yes	Yes
Can be used for personally owned devices	Yes	Yes	Yes	Yes
Infrastructure requirements	None	Managed network	Managed network System Center 2012 R2 Configuration Manager infrastructure	None
Supports the use of stand-alone media (USB flash drive)	Yes	Yes	Yes	No
Requires additional purchase	No	No	Yes	Yes (subscription model)
Deploy an app during operating system deployment	Yes	Yes	No	No

Users installing apps from the Windows Store require little or no IT help, but sideloading requires IT resources to prepare for the process. Amy recognizes that she and other IT pros at the institution

will assume most of the effort required to meet the sideloading prerequisites. Amy and Mark also decide which apps will be provisioned to all users on a device and which apps will be deployed to specific users on a device.

Amy and Mark decide to use System Center 2012 R2 Configuration Manager and Windows Intune to perform sideloading, because this method allows them to create an enterprise app store. They also decide to use System Center 2012 R2 Configuration Manager to manage apps on institution-owned devices and Windows Intune to manage apps on personally owned devices.

For details on how use sideloading to deploy an app, see the section, “Use only sideloading” on page 23 in this guide.

Plan for when to deploy apps

Apps can be deployed:

- **During operating system deployment** Sideloading only; typically performed on institution-owned devices (not deploying operating systems to personally owned devices)
- **After operating system deployment** Windows Store, sideloading, or a combination of both; can be performed on any device (institution-owned or personally owned)

For each app in the portfolio, Amy and Mark determine whether it will be deployed during or after operating system deployment.

Select the right app deployment method

You can deploy apps by using the Windows Store, sideloading, or both, but how do you determine which method is best for a specific app? Table 4 on page 14 lists the criteria for selecting the right app deployment method.

TABLE 4 Criteria for Selecting the Right App Deployment Method

SELECTION CRITERION	WINDOWS STORE	SIDELOADING
Technical skill required	<p>Low—Installation can be performed by a faculty member or student.</p> <p>Management of apps (by using AppLocker or other partner management products) requires IT pro skills.</p>	<p>High for the IT pro skills to configure and perform sideloading (not easily performed by a typical information worker).</p> <p>Low for the users who will install the apps (in a self-service model).</p>
User age	<p>To comply with COPPA, Microsoft requires users younger than 13 years of age to have an adult help create the Microsoft account. To create a Microsoft account for someone younger than 13 years of age, the adult must provide a credit card, and a charge of \$0.50 is applied to the card. You can control which Windows Store apps can be installed and run on devices by using AppLocker, which requires Windows 8 Enterprise. The Windows Store shows content (such as screenshots or app descriptions) for apps that is appropriate for people 12 years of age and older.</p>	<p>Can provide flexibility to deploy apps to users under 13 years of age, but additional effort or software might be required (such as creating a targeted user collections based on age in System Center 2012 Configuration Manager or Windows Intune).</p>
Technical infrastructure required	<p>Low—Requires Internet connectivity and the IT infrastructure to support access to the Windows Store, such as Internet ingress and egress, firewalls, and web proxies.</p>	<p>High—Might require additional infrastructure depending on the method selected for sideloading (e.g., a System Center 2012 R2 Configuration Manager infrastructure or Windows Intune accounts).</p>
Deployment life cycle	<p>Apps can only be deployed after the operating system has been deployed. You can install Windows Store apps by using deep links in Windows Intune or System Center 2012 R2 Configuration Manager.</p>	<p>Apps can be deployed both during and after the operating system has been deployed. However, only 24 apps can be provisioned in an operating system (such as during operating system deployment).</p>
App ownership model	<p>Personally owned—Each user owns and manages apps through their Microsoft account (as allowed by other institution management tools, such as AppLocker, for institution-owned devices).</p>	<p>Institution-owned—The institution owns and manages the apps.</p>
App availability	<p>Apps that are in the Windows Store can be downloaded at any time.</p>	<p>Must obtain the .appx installation package directly from the app developer.</p>

SELECTION CRITERION	WINDOWS STORE	SIDeloading
Shared device support	<p>App installation—Apps must be installed for each user on the device on a user-by-user basis. There is no limit to the number of users who can install apps on a device, but a specific app for a specific user can only be installed on up to five devices.</p> <p>When a user logs out of a device and another user with a different Microsoft account logs on to the same device, only the apps associated with the currently logged-on Microsoft account will be available.</p>	<p>App provisioning—Apps can be provisioned to a device, and then all users can use the app on that device. You can install no more than 24 apps in an image before you receive an error message.</p>
Curated user experience	<p>You cannot control which apps in the Windows Store users can browse, but you can control which apps can be installed and run by using AppLocker and partner products.</p>	<p>The institution fully controls user experience and selection of apps, but the institution must take responsibility for ensuring that the apps have been certified and are free from malware. Although not required for sideloaded apps, it is recommended that any apps that will be sideloaded have been tested by using the Windows App Certification Kit.</p>
Paid app distribution	<p>The user must purchase and install the app through their Microsoft account.</p>	<p>The institution can purchase and install the app through an agreement between the app developer and the institution.</p>
Controlling app updates	<p>Users are notified of app updates through the Store app on the Start screen. Users must manually initiate app updates by using the Store app: The institution cannot <i>push</i> updates to the users and devices and also cannot choose which update are installed. There is no centralized app update management.</p>	<p>The institution can provide app updates either as mandatory (<i>pushed update</i>) or at the user's discretion (self-service model). The apps can be delivered to users and devices through existing software distribution products (such as System Center 2012 R2 Configuration Manager or Windows Intune).</p>
Obtaining apps	<p>Users obtain apps from the Windows Store by using their Microsoft account. Different types of apps can be obtained, including paid apps, free apps, and free apps with an in-app purchase option.</p>	<p>Apps must be obtained directly from the app developer based on an agreement between the institution and the app developer.</p>

SELECTION CRITERION	WINDOWS STORE	SIDELOADING
Identity infrastructure	<ul style="list-style-type: none"> Windows Store apps require a Microsoft account. Users may require additional accounts to access other resources (such as institution resources or Office 365). User credentials (such as passwords) cannot be synchronized among different identity systems, such as between a domain-based account and a Microsoft account. 	<ul style="list-style-type: none"> Sideloaded apps require a Windows account. Optionally requires a Microsoft account, because some apps require a Microsoft account to run.
Device ownership	Can be used for all device scenarios (institution-owned or personally owned devices).	<ul style="list-style-type: none"> During operating system deployment, apps can only be sideloaded to institution-owned devices. After operating system deployment, apps can be sideloaded for all device scenarios (assuming that sideloading has been enabled on the devices).
Deployment speed and flexibility?	Flexible, as students and faculty can download a discovered app immediately.	Less flexible, as IT would need to acquire an .appx package, license the offering, and sideload the app.

Ultimately, you make the decision by prioritizing app deployment requirements, and then selecting the method that best meets the higher-priority requirements. Examples include:

- If an app can only be obtained through the Windows Store (that is, the app cannot be obtained directly from the app developer), then you must use the Windows Store deployment method. In contrast, if the educational institution obtains the app installation files directly from the developer, then you must use the sideloading method.
- If the institution owns a device, then apps can be deployed during operating system deployment by using sideloading. If a faculty member or student owns the device, then the app must be deployed after operating system deployment by using the Windows Store or sideloading.

Amy and Mark prioritized the criteria in Table 4 on page 14 for each app, and then selected the best method based on their prioritization.

Additional resources:

- The Windows Store at <http://windows.microsoft.com/en-us/windows-8/windows-store#1TC=t1>
- The section, "To configure your enterprise PCs for sideloading using Group Policy," in the topic "How to Add and Remove Apps" at <http://technet.microsoft.com/library/hh852635.aspx#SideloadRequirements>
- The topic "Configure PCs for Sideload Requirements" at <http://technet.microsoft.com/en-us/library/hh852635.aspx#SideloadRequirements>
- The *Volume Licensing Guide for Windows 8.1 and Windows RT 8.1* at http://download.microsoft.com/download/9/4/3/9439A928-A0D1-44C2-A099-26A59AE0543B/Windows_8-1_Licensing_Guide.pdf
- "DISM App Package (.appx or .appxbundle) Servicing Command-Line Options" at <http://technet.microsoft.com/library/hh824882.aspx>
- Add-AppxProvisionedPackage Windows PowerShell cmdlet at <http://technet.microsoft.com/library/dn376490.aspx>
- Add-AppxPackage Windows PowerShell cmdlet at <http://technet.microsoft.com/en-us/library/dn448376.aspx>
- The Windows 8.1 Springboard Series at <http://aka.ms/windows8itpro>
- The *Windows 8.1 FAQ for IT Professionals* at <http://technet.microsoft.com/windows/jj721676>

Deploying apps after operating system deployment

As part of the planning process, Amy and Mark selected the app deployment method for each app. The next step is for Amy to prepare the IT infrastructure for app deployment, and then deploy the apps to the appropriate users and devices. The changes you must make to your IT infrastructure depend on the app deployment method selected.

You can deploy apps after Windows 8 operating system deployment by using the Windows Store, sideloading, or a combination. Each deployment scenario is discussed in further detail in a subsequent section. For information about deploying apps during operating system deployment, see the section “Deploying apps during operating system deployment” on page 27.

Use only the Windows Store

In most cases, users (the consumers of the apps) install apps by using the Windows Store. From the IT perspective, the greatest responsibility is ensuring that the IT infrastructure allows proper access to the Windows Store. Table 5 on page 19 lists the high-level steps for installing apps by using only the Windows Store and the user persona responsible for performing the step.

TABLE 5 High-Level Steps for Deploying Apps by Using Only the Windows Store

STEP	DESCRIPTION	PERFORMED BY
1	<p>Configure the IT infrastructure to support the Windows Store. Ensure that the IT infrastructure allows access to the Windows Store. This step includes the following tasks:</p> <ul style="list-style-type: none"> Put the Windows Store domains on any firewall- or web proxy–approved “white” lists, which are documented at the following articles: http://support.microsoft.com/kb/2778122 http://support.microsoft.com/kb/2777643 Enable TCP ports 80 and 443 on firewalls. Enable access to the Internet for institution-owned or personally owned devices, as required. Configure proxy authentication for Windows Store access. 	IT pros
2	<p>Ensure that each faculty member and student has a Microsoft account that can be associated with their Windows account. Each user must create a new Microsoft account or use their existing Microsoft account to access the Windows Store. For students under 13 years of age, an approved guardian must assist in creating a Microsoft account because of COPPA regulations. To verify that an adult is giving a child permission to create a new Microsoft account, COPPA requires that a small amount be charged to the adult’s credit card.</p>	Faculty, students, and student guardians
3	<p>Publish the list of apps to be used. The faculty and IT pros will need to publish the list of recommended or required apps. This list can be published on a website, as part of a course syllabus, or as part of list of school supplies sent home to parents. If a specific version of an app is required, ensure that the list indicates the desired version. For example, a faculty member could be designated as the coordinator for the list of recommended and required apps. The faculty member could then publish the list on the institution’s main website.</p>	IT pros and faculty
4	<p>Install apps on devices. Faculty and students must install the apps on their devices by using the Microsoft accounts obtained earlier in the process. Depending on the age or skill level of the student, faculty may need to assist the student in logging on to and installing the app on their device. Apps are installed by using the Store app on the Start screen on the device. Apps can be found by searching the Windows Store (as shown in Figure 2 on page 21), by browsing content in the Windows Store, or by a direct hyperlink to the app in the Windows Store (also known as <i>deep links</i>). You can deploy deep linked apps by using System Center 2012 R2 Configuration Manager and Windows Intune.</p>	Faculty, students, and student guardians

STEP	DESCRIPTION	PERFORMED BY
5	Manage access to the Windows Store. One aspect of apps in education that must be managed is students browsing in the Windows Store for apps that do not directly relate to the curriculum (such as games or apps that are not age appropriate). Microsoft partners provide solutions that can help IT pros and faculty manage the student accessibility to the Windows Store. Also, educational institutions typically want to control which apps can be installed and run on devices. They can do this by using AppLocker and Group Policy settings in Windows 8.1 Enterprise.	IT pros and faculty
6	Manage apps on devices. Most educational institutions want to control the apps that can run on institution-owned devices. Use Group Policy settings and AppLocker to prevent the installation of unauthorized apps or running unauthorized apps on institution-owned devices.	IT pros
7	<p>Update apps on devices. Updates to apps are published through the Windows Store. Users are notified of app updates on the Store app tile on the Start screen. The Store app tile shows the number of app updates available based on the apps installed for the currently logged-on user. Users can elect to install updates on an app-by-app basis or update all apps at once. As with the installation of apps, faculty might need to assist students in logging on to and installing the app on their device (depending on age or skill level). Each user on a device must install the app updates, regardless if other users have installed the app update or not. Establish a time for app updates to be installed that is acceptable to the faculty. For example, ensure that app updates are always installed prior to the start of a class or event so that time is not wasted on app updates. Also, ensure that students are not distracted during class or events by dynamically restricting access to the Windows Store during class or event periods by using AppLocker (available only in Windows 8.1 Enterprise) and products from Microsoft partners.</p> <p>Note You cannot dynamically restrict access to the Windows Store on devices running Windows RT 8.1.</p>	Faculty and students

Amy and Mark have divided the tasks in Table 5 on page 19 based on their job roles. Amy ensures that the IT infrastructure allows access to the Windows Store and performs a series of tests to ensure that all Windows Store features work as expected. Amy also configures Group Policy settings and AppLocker to help prevent the installation of unauthorized apps or starting unauthorized apps on institution-owned devices. For the most part, Amy's responsibilities are complete.

In contrast, Mark has been busy working with the faculty on deployment. First, he has been helping the faculty identify the apps they want to use in their curriculum. Mark and other faculty members search the Windows Store (illustrated in Figure 2 and Figure 3 on page 22) to help them find the right apps. They also find out that they can search by app name or other keywords.

Mark and other faculty members also browse content in the Windows Store by category, such as education (shown in Figure 4 on page 22). They can use different categories of apps to find the right app quickly.

During the deployment process, Mark receives an email from a teacher who is having trouble installing an app on the 30 devices in her classroom. After meeting with the teacher, Mark tells her to have each student log on to a device using their assigned Microsoft account, and then have each student install the app. Mark also points out that each student should log on to the same device each day in class to avoid spending the time required to log on to a device for the first time while in class.

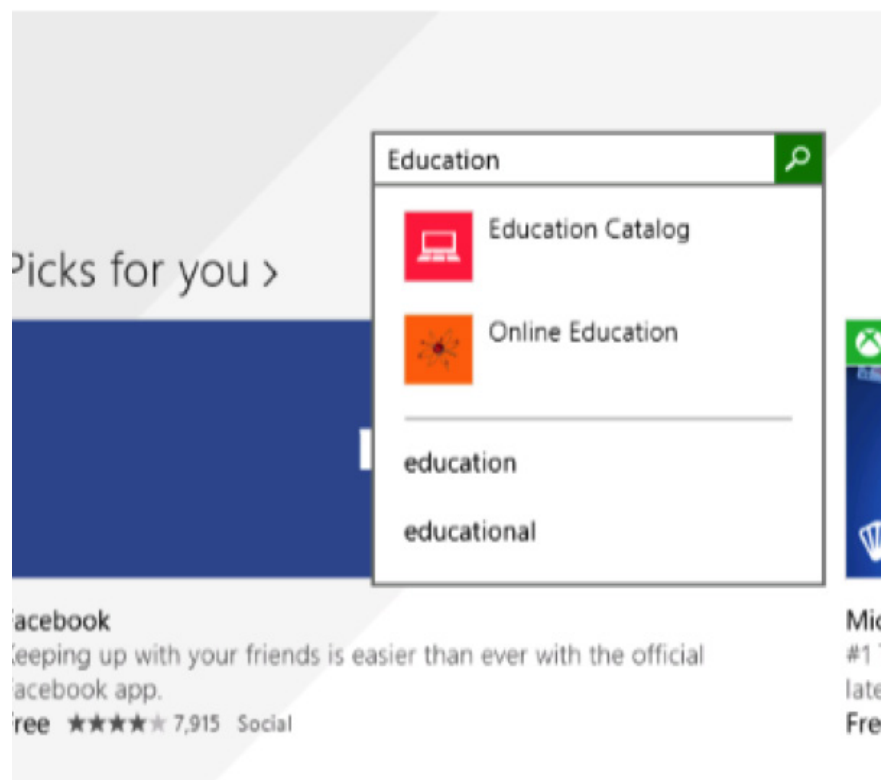


FIGURE 2 Searching the Windows Store

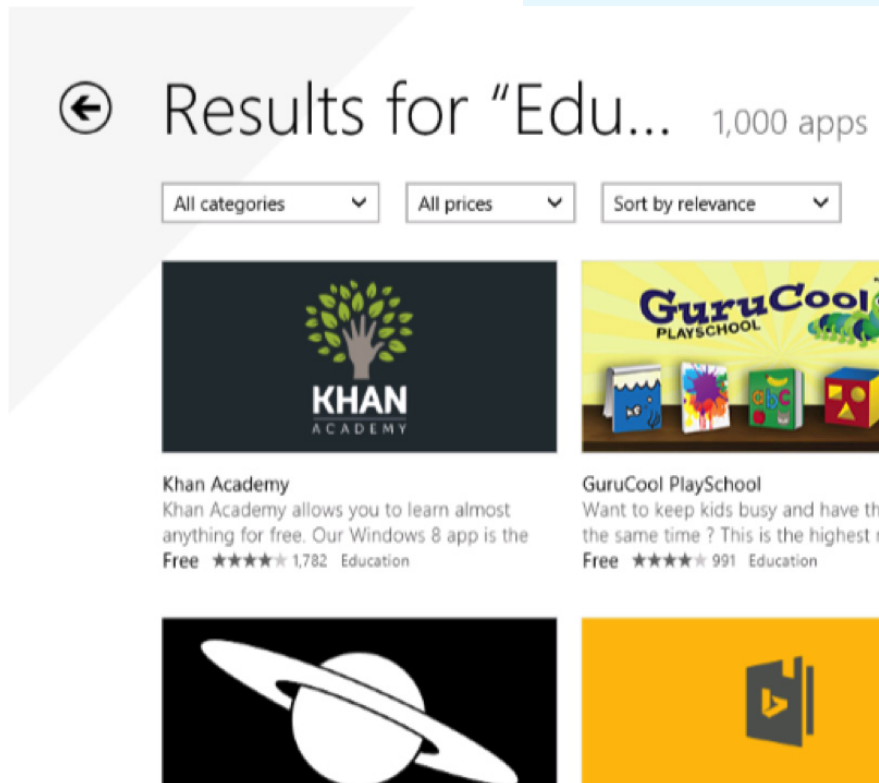


FIGURE 3 Search results in the Windows Store

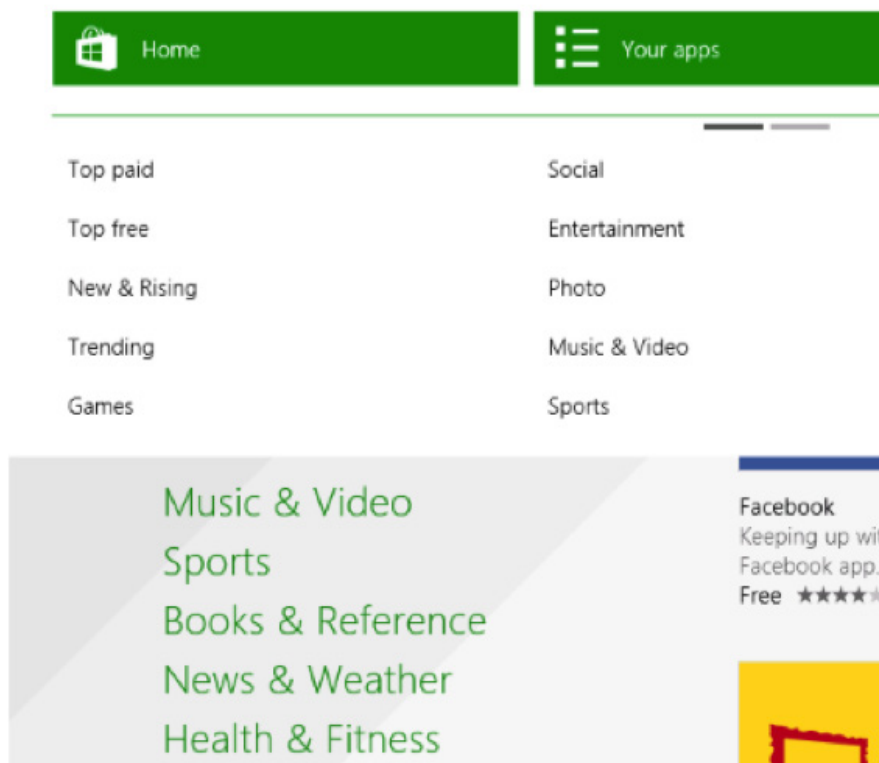


FIGURE 4 Browsing content by category in the Windows Store

Use only sideloading

IT pros must perform the majority of the steps to deploy apps by using sideloading: Users are responsible for installing only optional apps. Table 6 lists the high-level steps for using sideloading to deploy apps and the user persona responsible for performing each step.

TABLE 6 High-Level Steps for Deploying Apps by Using Only Sideloading

STEP	DESCRIPTION	PERFORMED BY
1	Obtain the app package files. IT pros and faculty can work together to obtain the app package files from the app developer.	IT pros and faculty
2	Configure the appropriate method for performing sideloading. For each sideloading deployment method selected in the section “Plan for app sideloading” on page 8, configure the method for performing app sideloading. This choice includes activities such as creating System Center 2012 R2 Configuration Manager applications and deployment types, uploading apps into Windows Intune, or configuring logon scripts.	IT pros
3	Ensure that devices are properly configured for sideloading. Configure devices for sideloading based on the sideloading prerequisites discussed in the section “Plan for app sideloading” on page 8. Preparation for sideloading depends on device ownership.	IT pros
4	Manage access to the Windows Store. If all apps are to be sideloaded, disable access to the Windows Store by using the Turn off the Store application Group Policy setting. The Turn off the Store application Group Policy setting also disables the ability to automatically install updates from the Windows Store. If deploying apps by using both the Windows Store and sideloading, see the section “Use both the Windows Store and sideloading” on page 26. This step only applies to institution-owned devices, not personally owned devices.	IT pros
5	Manage apps on devices. Most educational institutions want to control the apps that can be run on institution-owned devices. Prevent users from installing and running unauthorized apps on institution-owned devices by using Group Policy settings and AppLocker with Windows 8 Enterprise. This step only applies to institution-owned devices, not personally owned devices.	IT pros

STEP	DESCRIPTION	PERFORMED BY
6	Update apps on devices. The IT pro or faculty member designated as the primary point of contact for the app developer obtains an updated version of the .appx installation package directly from the developer. Use System Center 2012 R2 Configuration Manager or Windows Intune to deploy updates automatically. Other methods must follow the same process as installing the app. App updates can also be pushed or made available in a self-service model. For the push model, no user interaction is required. For the self-service model, users must install the app updates on their device. When you update an app, you do not need to uninstall the older version first. The new version of the app will automatically remove the older version before installing the newer version. Also, when you update an app any existing app data is typically retained. However, this could vary between apps and you should contact the app developer prior to updating the app.	IT pros, faculty, and students

During the planning phase, Amy and Mark decided to use System Center 2012 R2 Configuration Manager and Windows Intune to perform sideloading. Amy and Mark work with the faculty to obtain the app packages for all the apps to be sideloaded. Amy and Mark also work with the faculty to determine which apps need to deploy by using the push model and which can be deployed by using the self-service model.

Then, Amy configures System Center 2012 R2 Configuration Manager and Windows Intune to sideload the apps. For System Center 2012 R2 Configuration Manager, Amy creates a Configuration Manager application and deployment type by using the Create Application Wizard (as illustrated in Figure 5 on page 25).

Amy also uploads the apps into the Software workspace in Windows Intune (as illustrated in Figure 6 on page 25). Then, she deploys the apps to the user groups previously defined in Windows Intune.

Amy also uses Group Policy, System Center 2012 R2 Configuration Manager, and Windows Intune to prepare the devices for sideloading:

- Enable the **Allow all trusted applications to install** Group Policy setting for domain-joined devices running Windows 8 Enterprise.
- Activate sideloading keys for all other devices.

When Amy is finished, Mark works with other faculty members and students to install apps that are deployed by using a self-service model. Mark also works with faculty members and students to help them deploy app updates to their devices.

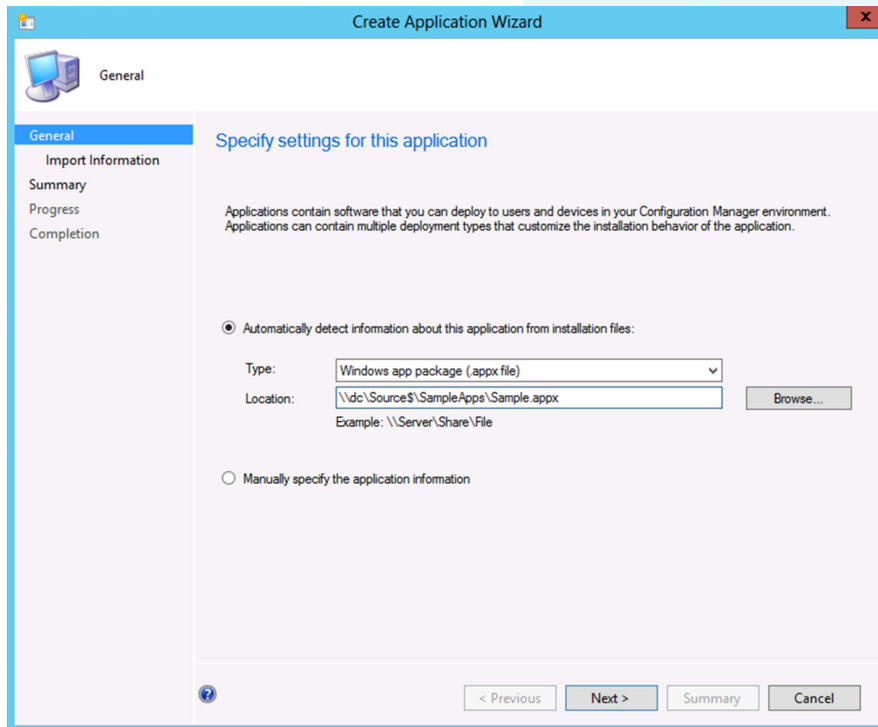


FIGURE 5 General page in the Create Application Wizard

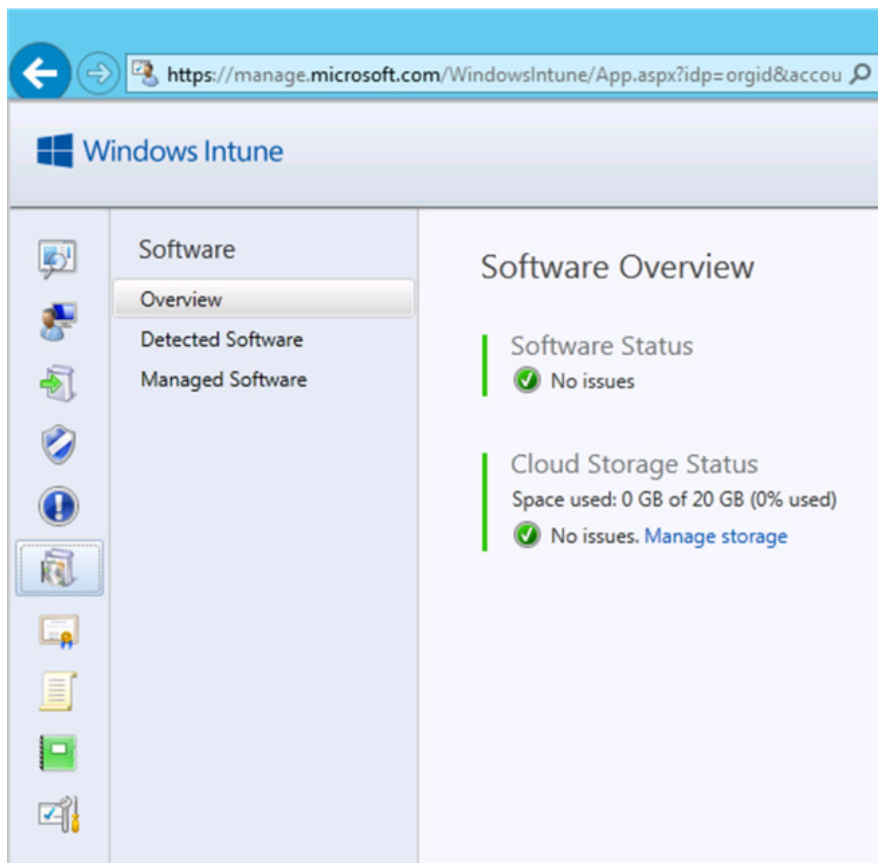


FIGURE 6 The Software workspace in Windows Intune

Use both the Windows Store and sideloading

Most educational institutions deploy apps by using a combination of the Windows Store and sideloading to provide additional flexibility in app deployment. For example, using a combination of both methods allows an institution to deploy some apps as a part of operating system deployment by using sideloading while allowing faculty and students the flexibility to purchase apps as they desire from the Windows Store. In addition, you can use Microsoft partner products to make AppLocker and other app management tools more dynamic and automated.

If you decide to deploy apps by using both the Windows Store and sideloading, follow the steps provided in the sections “Use only the Windows Store” on page 18 and “Use only sideloading” on page 23, with the exception that you should not use the **Turn off the Store application** Group Policy setting to disable access to the Windows Store. Otherwise, perform all steps when using both the Windows Store and sideloading.

Additional resources:

- Windows 8.1 apps website at <http://windows.microsoft.com/en-us/windows-8/apps>.
- System Center 2012 R2 Configuration Manager with SP1 at <http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx>.
- Windows Intune at <http://www.microsoft.com/en-us/windows/windowsintune/pc-management.aspx>
- AppLocker Overview at <http://technet.microsoft.com/library/hh831409.aspx>

Deploying apps during operating system deployment

You can deploy apps during Windows 8.1 operating system deployment by using MDT, command-line utilities, or a combination of these methods. Each deployment scenario is discussed in further detail in a subsequent section. For information about deploying apps after operating system deployment, see the section “Deploying apps after operating system deployment” on page 18.

Table 7 lists the high-level steps for deploying apps during operating system deployment and the user persona for each. These steps are similar to those for deploying apps after operating system deployment.

TABLE 7 High-Level Steps for Deploying Apps During Operating System Deployment

STEP	DESCRIPTION	PERFORMED BY
1	Obtain the app package files. Obtain the app package files from the app developer.	IT pros and faculty
2	Configure the appropriate method for performing sideloading. For each sideloading deployment method selected in the section “Plan for app sideloading” on page 8, configure the method to perform app sideloading. This task includes activities such as creating System Center 2012 R2 Configuration Manager applications and deployment types, creating MDT applications, creating task sequences, or writing Windows PowerShell scripts.	IT pros
3	Ensure that devices are properly configured for sideloading. Configure devices for sideloading based on the sideloading prerequisites discussed in the section “Plan for app sideloading” on page 8. The preparation for sideloading depends on device ownership.	IT pros
4	Manage access to the Windows Store. If all apps are to be sideloaded, use the Turn off the Store application Group Policy setting to disable access to the Windows Store. If deploying apps by using both the Windows Store and sideloading, see the section “Use both the Windows Store and sideloading” on page 26.	IT pros
5	Deploy Windows 8 and the apps to the devices. The deployment of Windows 8 apps during operating system deployment is integral for MDT and System Center 2012 R2 Configuration Manager. You can deploy Windows 8 apps manually from the command line, but deployment typically requires some level of automation, as well, to provide consistency in the deployment process.	IT pros

Mark and Amy decide to deploy apps during operating system deployment by using System Center 2012 R2 Configuration Manager integrated with MDT. Mark will create standard

deployment images and add the apps to be sideloaded to System Center 2012 R2 Configuration Manager.

Use MDT

Use MDT to manage the deployment of apps during operating system deployment. MDT supports the deployment technologies listed in Table 8, which you can use for different deployment infrastructures and scenarios.

TECHNOLOGY	DESCRIPTION
Lite Touch Installation (LTI)	<ul style="list-style-type: none">• Requires minimal infrastructure and uses a wizard-driven UI to manage and perform deployments• Allows you to specify configuration settings in advance or at the time of deployment
Zero Touch Installation	<ul style="list-style-type: none">• Requires a System Center 2012 R2 Configuration Manager infrastructure to deploy and manage Windows 8.1• Requires that you specify all configuration settings in advance of deployment
User-Driven Installation (UDI)	<ul style="list-style-type: none">• Requires a System Center 2012 R2 Configuration Manager infrastructure to deploy and manage Windows 8.1• Allows you to specify configuration settings in advance or at the time of deployment

TABLE 8 MDT
Deployment Technologies

MDT also includes a centralized configuration database (called the *MDT database* [MDT DB]), which you can use to provide configuration settings during the deployment process. You can use the MDT DB instead of providing configuration settings interactively during the deployment process (for LTI and UDI) or in the CustomSettings.ini file (for all MDT deployment technologies).

MDT allows you to create custom queries to return configuration settings as desired. For example, you could query the MDT DB for configuration settings that are associated with the media access

control address of a specific device. In a classroom setting, this would allow you to fully automate all the deployment configuration settings for a specific device.

Resources for using MDT to deploy apps during operating system deployment are listed in the "Additional resources:" on page 30 section.

Using the command line

You can use DISM and the **Add-AppxProvisionedPackage** Windows PowerShell cmdlet to install Windows Apps during operating system deployment. You can also install Windows 8.1 apps during operating system deployment by using these command-line tools with an ESD system. Although it is possible to perform these tasks manually, Microsoft recommends that you use highly automated deployments of the operating system and Windows 8.1 apps.

Resources for using DISM and the **Add-AppxProvisionedPackage** Windows PowerShell cmdlet to deploy apps during operating system deployment are listed in the "Additional resources:" section on this page.

Additional resources:

- The topic “Why does Microsoft charge me when I create an account for my child?” at <http://windows.microsoft.com/en-US/windows-live/family-safety-why-does>
- MDT 2013 at <http://www.microsoft.com/en-us/download/details.aspx?id=40796>
- Windows 8.1 apps website at <http://windows.microsoft.com/en-us/windows-8/apps>.
- System Center 2012 R2 Configuration Manager at <http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx>
- Windows Intune at <http://www.microsoft.com/en-us/windows/windowsintune/pc-management.aspx>
- The topic “Step-by-Step: Deploying Windows 8 Apps with System Center 2012 Service Pack 1—Migration and Deployment Series (Part 16 of 19)” at <http://blogs.technet.com/b/keithmayer/archive/2013/02/25/step-by-step-deploying-windows-8-apps-with-system-center-2012-service-pack-1.aspx#.UYHeoejn-t8>
- “DISM App Package (.appx or .appxbundle) Servicing Command-Line Options” at <http://technet.microsoft.com/library/hh824882.aspx>
- The Add-AppxProvisionedPackage Windows PowerShell cmdlet at <http://technet.microsoft.com/library/dn376490.aspx>
- Add-AppxPackage Windows PowerShell cmdlet at <http://technet.microsoft.com/en-us/library/dn448376.aspx>

Windows Store app deployment FAQ

The following sections include answers to frequently asked questions about Windows Store app deployment.

Additional resources:

- The Windows Web App Gallery at <http://www.microsoft.com/web/gallery>
- The topic “Single sign-on for apps and websites” at <http://msdn.microsoft.com/en-us/library/live/hh826544.aspx>
- The topic “How to Add and Remove Apps” at <http://technet.microsoft.com/en-us/library/hh852635.aspx>
- The topic “Managing Client Access to the Windows Store” at http://technet.microsoft.com/en-us/library/hh832040.aspx#BKMK_UseGP
- The topic “Supported Exchange ActiveSync policy parameters in Windows 8 and RT” at <http://support.microsoft.com/kb/2823900>
- NetSupport School solutions at <http://netsupportschool.com>
- The topic “How to restore, refresh, or reset your PC” at <http://windows.microsoft.com/en-US/windows-8/restore-refresh-reset-pc>

How can I deploy desktop applications on devices running Windows 8.1?

The deployment process for desktop applications on devices running Windows 8.1 is the same as it was for the Windows 8 and Windows 7 operating system. As a result, you can use the same methods for deploying desktop applications available for Windows 8 and Windows 7, such as System Center Configuration Manager, MDT, Group Policy, or local installation media (including USB flash drives).

There are no limitations to the number of desktop applications you can provision to a device (unlike Windows Store apps, which can only have up to 24 provisioned apps installed in an image). Also, desktop applications do not typically require a Microsoft account for installation.

How can I deploy web apps on devices running Windows 8.1?

Windows 8.1 includes a Windows Store app and desktop version of Internet Explorer 11. When you manually pin a web app to the start screen, it creates a tile that reflects the web app. For example, if you pin a Bing web app to the start screen, the tile displays the Bing logo. Some deployment methods, such as MDT, will only create a generic Internet Explorer icon when a web app is pinned to the start screen.

How can Windows Store apps be removed from a device?

You can remove Windows Store apps interactively on the Start screen, or you can use:

- DISM to remove provisioned apps from a device
- The **Remove-AppxProvisionedPackage** Windows PowerShell cmdlet to remove provisioned apps from a device
- The **Remove-AppxPackage** Windows PowerShell cmdlet to remove installed apps from a device

For example, you could use the **Remove-AppxProvisionedPackage** cmdlet to remove the standard SkyDrive app so that users will use the SkyDrive Pro desktop app (installed with Microsoft Office Professional Plus 2013), instead.

How can I remove a device from the list of devices that are allowed to install purchased apps from the Windows Store?

Windows Store keeps track of the devices where you have installed purchased apps. You are allowed to install a purchased app on as many as 81 devices. You can remove a device from the list of devices by starting the **Windows Store** app, click **Settings**, click **Your account**, and then remove the device from the list.

How can I use Group Policy settings to manage Windows Store apps?

IT administrators can use Group Policy to manage Windows Store apps and access to the Windows Store, including:

- Allowing or prohibiting their users from accessing the Windows Store
- Allows apps to be sideloaded
- Window Store privacy settings
- Controlling access to which Windows Store apps can be installed and run by using App Locker
- Configuring the Windows Store to auto-download (but not install) available updates
- Using Group Policy settings to control and manage the installation of apps

NOTE

AppLocker is available only for managing domain-joined devices running Windows 8.1 Enterprise.

How can Windows Store apps be managed in the classroom?

You can manage Windows Store apps in the classroom by using any of the following methods:

- Any of the methods listed in the question, "How can I use Group Policy settings to manage Windows Store apps?"
- Preventing apps from being installed or run by using AppLocker (for domain-joined devices only)

Which mobile device management solutions work with Windows Store apps?

You can manage Windows 8.1 by using:

- **Solutions that support the Microsoft Exchange ActiveSync platform** You use Exchange ActiveSync policies to configure mobile devices that use Exchange ActiveSync to connect. Administrators can create mobile device mailbox policies to

apply a common set of policies or security settings to a collection of users (not to be confused with Group Policy).

- **Windows Intune** You can manage Windows Store apps on manage domain-joined and non-domain-joined devices by using Windows Intune. Windows Intune allows you to deploy Windows Store apps by using deep links or by sideloading app packages.

What happens to Windows Store apps if a user performs a device reset or a device recovery?

When a user performs a:

- Windows 8.1 device refresh, Windows 8.1 is reinstalled, but the personal files, settings, and any Windows Store apps are retained
- Windows 8.1 device reset, Windows 8.1 is reinstalled, but the personal files, settings, and any Windows Store apps are deleted

The behavior described above is the same for apps that are installed from the Windows Store or that are sideloaded. After a Windows 8.1 device reset, you must install Windows Store apps as though you were installing the apps on a different device by using **My Apps** in Windows Store.

For institution-owned devices, users will not be administrators, so they will be unable to reset devices. IT pros or faculty will need to reset devices as required. For personally owned devices, the user will be an administrator and will be able to reset their own device.



© 2014 Microsoft Corporation. All rights reserved.

This document is for informational purposes only and is provided "as is." Views expressed in this document, including URL and any other Internet Web site references, may change without notice. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.