Windows Phone

Windows Phone 8.1 Mobile Device Management Overview

Published April 2014

Executive summary

Most organizations are aware that they need to secure corporate data and minimize risks if mobile devices are lost or stolen. Many of those same organizations are adopting Bring Your Own Device (BYOD) initiatives to enable employees to use personally owned devices (smartphones) to access corporate information and services. Just as desktop and laptop devices require ongoing management and support, smartphones require the same or an even higher level of management, and smartphones are often at greater risk because they are easy to lose and commonly used in public places.

A Mobile Device Management (MDM) system can reduce the support costs and security risks of such situations while improving individual user productivity. In fact, most MDM systems can help you manage devices and apps running on mobile devices regardless of whether they connect directly to your company's intranet, public Wi-Fi hotspots, or over cellular data services.

Originally, MDM systems were designed as self-service, portal-focused solutions. Today, those systems are more IT and admin-centric solutions, with MDM system deployment models possible solely on premises, solely in the cloud, or a hybrid of both.

Windows Intune is a cloud-based MDM system that organizations can use to manage devices on or off premises. Similarly, Microsoft System Center 2012 R2 Configuration Manager is an on-premises MDM system that can also manage devices on or off premises. You can use System Center 2012 R2 Configuration Manager and Windows Intune together to create a comprehensive management solution for mobile and stationary devices and services.

Introduction

MDM management in Windows Phone 8 is based on the Device Management Synchronization Markup Language version 1.2, which is the Open Mobile Alliance standard for device management. Windows Phone 8.1 builds on this standard to create an integrated MDM client that allows MDM system vendors to manage Windows Phone devices.

Note In this guide, *Windows Phone* refers to Windows Phone 8.1 unless explicitly specified otherwise.

The MDM features in Windows Phone make the management of mobile devices simpler than with previous versions of Windows Phone and other mobile device operating systems (such as Apple iOS and Google Android). For example, Windows Phone supports a customizable process that allows you and your MDM system vendor to customize device enrollment.

Windows Phone introduces the ability to initiate the connection from the MDM system (push), helping to ensure that the Windows Phone devices are current with all your MDM policies and configuration standards, which ultimately helps protect the device and the apps that are running on it from unauthorized access. Just as in previous versions of Windows Phone, Windows Phone 8.1 periodically contacts the MDM system at a configured interval (pull) to download configuration information, download apps, download updates, and upload asset inventory and app deployment status.

A comprehensive MDM system performs device management throughout the entire device life cycle, as illustrated in Figure 1. The remainder of this guide discusses the Windows Phone 8.1 MDM management features and how an MDM system uses them in each phase of the life cycle.

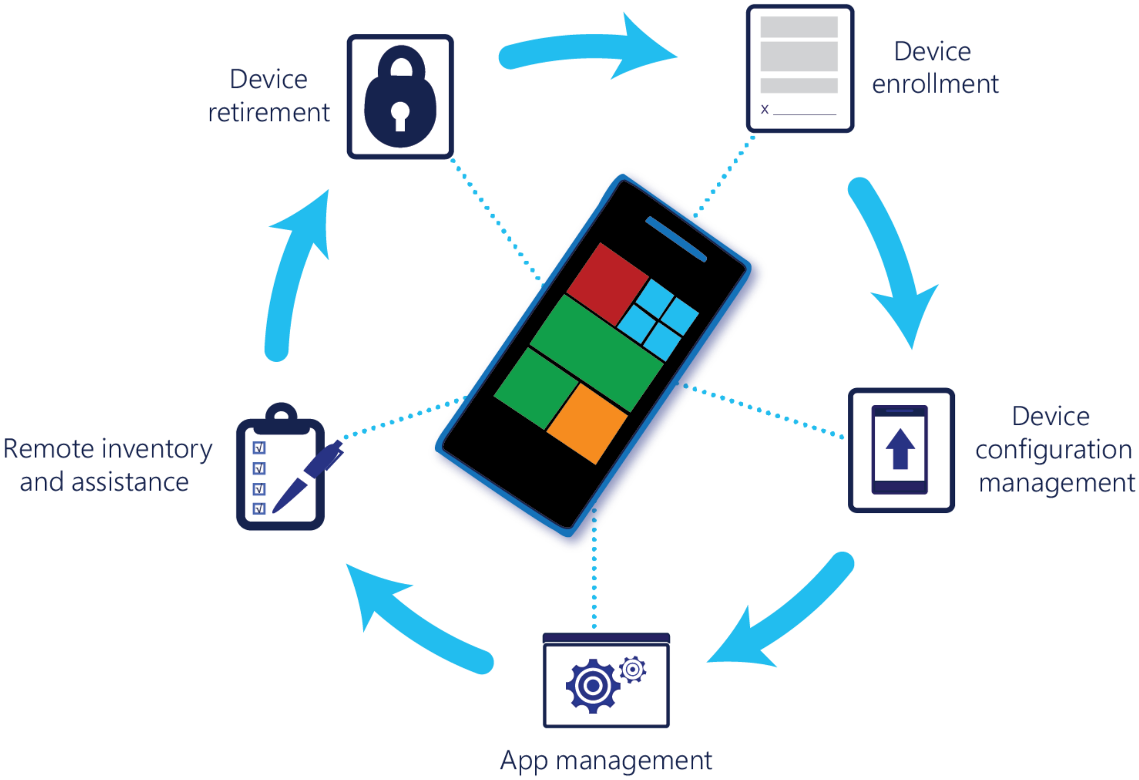

Device retirement
Device enrollment
Remote inventory and assistance
Device configuration management
App management

Figure 1. Device management life cycle

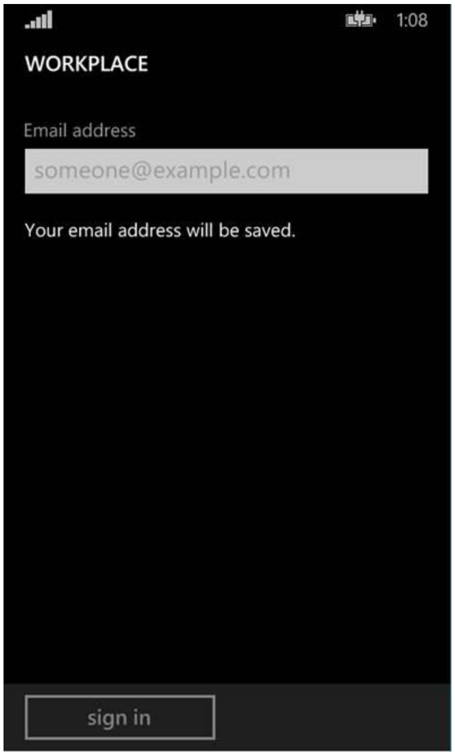
Device enrollment

Device enrollment is the first phase of the device life cycle. Device enrollment registers a device with an MDM system so that the system can manage the device, the apps running on the device, and the confidential data on the device. Enrollment is an integral part of Windows Phone, which means that no additional, custom apps are needed to get the device up and running.

The high-level process for enrolling a device is as follows:

1. The user selects the option to add a workplace account.

2. The user enters their email account for their organization (as shown in Figure 2).



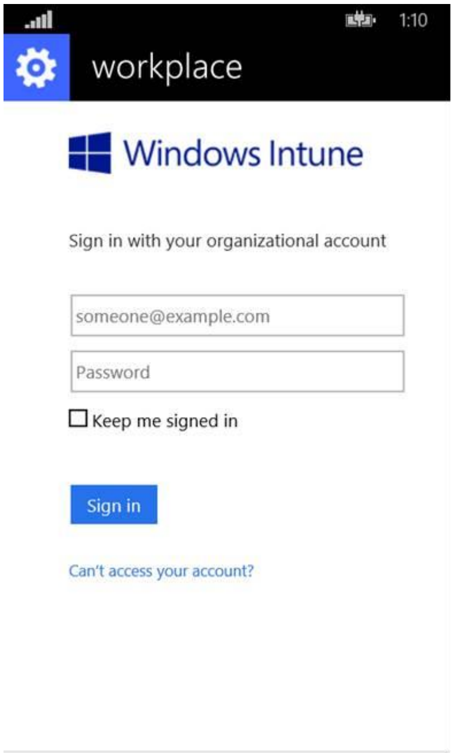
Your email address will be saved.

Figure 2. Entering an email account for workplace enrollment

Windows Phone uses the domain portion of the user’s email address to perform an automatic discovery of the MDM system through a Domain Name system (DNS) record that you enter in your public-facing DNS. For example, if the user’s email address is *mark@contoso.com,* then Windows Phone looks for the *enterpriseregistration.contoso.com* DNS record, which points to the public-facing IP address of the MDM system.

Note Some MDM systems, such as Windows Intune, have the necessary DNS record created as a part of the installation or subscription process.

3. The MDM system can optionally send one or more custom enrollment pages to collect additional information (as shown in Figure 3).



Sign in with your organizational account

someone@example.com

Password

□ Keep me signed in

Figure 3. Custom enrollment page

The information collected on these custom enrollment pages is determined by each MDM system. The information could be as simple as collecting the phone number or a onetime passcode, but you could also require to user to accept confidentiality statements or other organizational polices.

In the example that Figure 3 shows, the MDM system collects the user's account information and stores it in the MDM system. Later, support personnel can use the information to help provide assistance to the user.

Depending on the MDM system, you can personalize the enrollment pages to define what your organization needs. The MDM system ultimately stores the information that these pages collect.

4. If all of the information the user entered is correct, the MDM system validates the user account and other account information.

   In addition to validating the user account, the MDM system may perform other validations checks, such as verifying that the account has been enabled or that the subscription is paid. The validation that needs to be performed varies by MDM system.

5. When the MDM system has validated the user account and other criteria, Windows Phone notifies the user that it discovered the MDM system and the device has been enrolled.

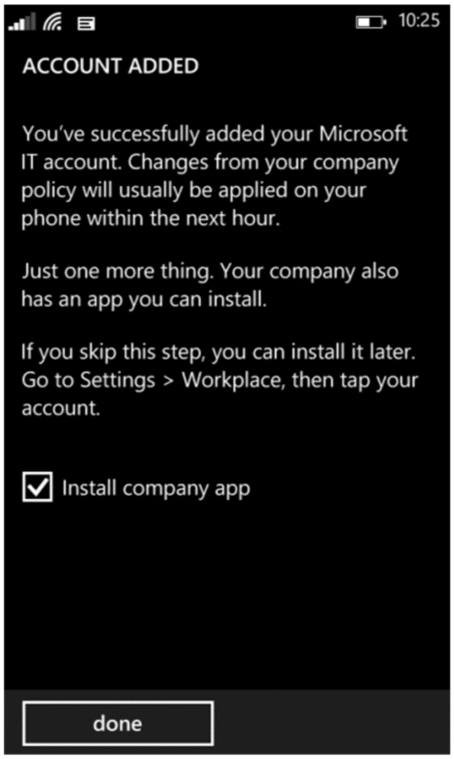
   If the user entered incorrect information, Windows Phone notifies the user and asks them to reenter the information. When the user has corrected the information, Windows Phone attempts the discovery process again.

If the MDM system was unable to verify a valid account, Windows Phone notifies the user to contact their administrator.

6. The MDM system completes the enrollment process, and the workplace information is saved on the device.

   Windows Phone saves the workplace information it collected during the device enrollment, using the information to contact the MDM system to check for updates on a scheduled interval or when the user initiates such a process.

7. When the enrollment process is complete, the MDM system may install additional apps (as shown in Figure 4).



10:25

ACCOUNT ADDED

You've successfully added your Microsoft IT account. Changes from your company policy will usually be applied on your phone within the next hour.

Just one more thing. Your company also has an app you can install.

If you skip this step, you can install it later. Go to Settings > Workplace, then tap your account.

☑ Install company app

Figure 4. Installing additional apps

Note Some MDM systems require additional apps; others might not.

After the user completes the enrollment process, Windows Phone and the MDM system are linked. Management of the device and the apps (including line-of-business [LOB] apps) on it is transparent to the user unless a specific management task requires user interaction. As you can see, the enrollment process requires minimal user interaction and uses information that the user knows.

Device configuration management

After enrolling the device, the MDM system now manages the device's configuration. The MDM system sends a provisioning profile to the device that contains configuration information and policies. The following list is an example of configuration information and policies contained in the provisioning profile:

- Email accounts
- Root certification authority (CA) certificates
- Wi-Fi network profiles
- Virtual private network (VPN) profiles
- Company portal, or other LOB apps
- Policies

This guide discusses each of these items later.

Configuration policies overview

The MDM feature in Windows Phone supports a superset of the policies that Microsoft Exchange ActiveSync (EAS) supports. The MDM system sends policy settings that configure the device. These policies automatically configure the device based on the mobile device standards and security policies the organization has defined. Table 1 lists the policies that both MDM and EAS support as well as the policies that only MDM supports.

Table 1. Comparison of Policies Supported by MDM and EAS and by MDM Only

Policies that MDM and EAS support	Policies that only MDM supports
Simple password	Disable cellular data roaming
Alphanumeric password	Disable Location
Minimum password length	Disable NFC
Minimum password complex characters	Disable Microsoft Account
Password expiration	Disable roaming between Windows devices
Password history	Disable custom email accounts
Device wipe threshold	Disable screen capture
Inactivity timeout	Disable copy & paste functionality
Device encryption	Disable share and save as
Disable removable storage card	App Allow/Deny list
Disable Camera	Disable Microsoft Store
Disable Bluetooth	Disable development unlock (side loading)
Disable Wi-Fi	Disable Internet Explorer
Disable Sync via USB	Disable Internet Sharing over Wi-Fi
	Disable Wi-Fi Off loading
	Disable Manual Configuration of Wi-Fi Profiles
	Disable Wi-Fi Hotspot reporting
	Disable VPN when Roaming over Cellular
	Disable VPN over Cellular
	Disable mdm un-enrollment and soft factory reset
	Disable Wi-Fi credential sharing
	Lock screen notification controls
	Disable telemetry data submission

Windows Phone 8.1 supports all the existing Windows Phone 8 security and device-management policies. In addition, Windows Phone 8.1 has new policies (see Table 1) that extend the management capabilities of MDM systems, such as the ability to disable the Windows Phone store, disable screen capture, disable device retirement (un-enrollment), manage Wi-Fi, and manage VPN. Windows Phone evaluates all the configured policies and applies the most secure policy (if multiple policies are applicable).

The MDM system publishes (pushes) these policies to devices so that they are current with the policies and configuration settings that you specify in the MDM system. As long as the device is connected to the Internet, the policies are sent to the device.

For more information on MDM and EAS policies, see http://go.microsoft.com/fwlink/?LinkId=394987.

Assigned access management

Assigned Access allows you to enable a specific set of apps and settings for users, preventing access to all other functionality. Assigned Access can also disable specific hardware features on devices. You can use this feature to create a single app experience on a device, such as a single app for baggage check agents at an airline or a set of multiple apps for retail customer service agents.

Your MDM system helps you centrally define a list of authorized and blocked apps for your devices. Assigned Access in Windows Phone uses this information to determine which apps are allowed to run and which aren't.

You can also control the built-in apps (for example, phone, text messaging, email, calendar) so that you can provide only those features to the user, helping to ensure that people use the device for its intended experience and purpose. Assigned Access also helps secure the device by preventing users from running apps that they might use to share confidential information with unauthorized users.

Storage management

Windows Phone 8.1 uses BitLocker Drive Encryption to encrypt the internal storage of devices just as it did with Windows Phone 8. This functionality helps ensure that corporate data is always protected from unauthorized users, even when they have physical possession of the phone.

New to Windows Phone 8.1 is the ability to install apps on a secure digital (SD) card. Windows Phone 8.1 stores the apps on a partition on the SD card that is specifically designated for that purpose. Like internal storage, this partition is encrypted by using the 128-bit Advanced Encryption Standard. This feature is always enabled, so there is no need to explicitly set a policy to enjoy this level of protection.

Note The encrypted partition on the SD card is uniquely paired with a device so that the apps and other data stored on the encrypted portion cannot be used on another device. However, data stored on the unencrypted partition of the SD card (such as music or photos) can be used on another device.

You can still use the **Disable removable storage card** policy to prevent users from using SD cards altogether, but the primary advantage of the new SD card app partition encryption feature is that you can give users the flexibility to use an SD card while still protecting the confidential apps and data on the that card.

Certificate management

Certificate management can be a difficult task for users, but certificates are pervasive and used for a wide variety of scenarios, such as account authentication, Wi-Fi authentication, VPN encryption, or Secure Sockets Layer (SSL) encryption of web content. Although some mobile devices require that users manually manage certificates in certain scenarios, Windows Phone does not. Importing certificates manually is supported, but the focus of Windows Phone is to use your MDM system to perform this task.

You can use your MDM system to manage certificates for the entire Windows Phone certificate life cycle, including certificate enrollment, renewal, and deletion. To do so, Windows Phone uses the Simple Certificate Enrollment Protocol (SCEP) to enroll client certificates, which allows you to use the CA of your choice (or whatever CA the MDM system requires).

In addition, Windows Phone includes advanced certificate management options based on a full set of certificate management application programming interfaces (APIs) that an MDM system or custom apps can use. For example, the system could use these APIs to archive Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption and signing certificates for later use in decrypting that same data, regardless of the device used.

Windows Phone devices also protect signing and encryption certificate keys by using the Trusted Platform Module (TPM) built into each device. Doing so requires that the user enter the TPM PIN to authorize access to the certificate keys, which further secures the device by enabling dual-factor authentication for certificates that are protected in this manner. For example, you could use this functionality to implement a virtual smartcard solution on devices.

Note The TPM PIN required to access certificate keys is different than the password (PIN) used to unlock the device.

Certificate management through your MDM system is fully transparent to users, requiring no user intervention. Although users can manually install certificates (they cannot view or delete manually), doing so through your MDM system helps improve user productivity and reduce support calls.

For more information about SCEP, see http://go.microsoft.com/fwlink/?LinkId=394989.

Wi-Fi networking management

Users use Wi-Fi connections almost as much as they use their cellular data connections. In some instances, they may use Wi-Fi connections even more, which means that management of Wi-Fi network connections is essential to any MDM management solution.

Your MDM system can fully configure the wireless connections without any user intervention. MDM management support for Wi-Fi networks in Windows Phone includes:

- Provisioning Wi-Fi profiles, which includes the service set identifier—even if it’s hidden—and any preshared keys
- Provisioning certificates used for Extensible Authentication Protocol (EAP)–Transport Layer Security and EAP–Tunneled Transport Layer Security wireless, certificate-based authentication

Policies available for managing Wi-Fi networks include:

- Disable Internet Sharing over Wi-Fi
- Disable Wi-Fi offloading
- Disable Manual Configuration of Wi-Fi Profiles
- Disable Wi-Fi Hotspot reporting
- Do not use Wi-Fi to offload data traffic

For more information about the policies used to manage Wi-Fi networks in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394991.

VPN management

Users often need to access resources securely on your organization's intranet by using a VPN connection. Windows Phone includes support for several VPN vendors in addition to Microsoft VPN connections. Windows Phone 8.1 introduces support for Internet Key Exchange Protocol version 2, IP security, and SSL VPN connection (although SSL VPN connections require a downloadable plug-in from the VPN server vendor).

Windows Phone 8.1 also supports auto-triggered VPN support (similar to the auto-triggered VPN support in Windows 8.1). You can define a VPN connection for each app that requires connectivity to intranet resources. When the user switches between apps, Windows Phone 8.1 automatically establishes the VPN connection for that app.

Note You can only have one active VPN connection at a time. If a user switches from one app to another and uses different VPN connections, Windows Phone 8.1 disconnects the VPN for the first app, and then establishes a VPN connection for the second app.

In the event that a VPN connection is lost, Windows Phone automatically reconnects the VPN connection without user intervention.

MDM management support for VPN connections in Windows Phone includes:

- Provisioning and updating VPN connection profiles, including the type of VPN connection and credentials
- Associating VPN connections with apps

Policies available for managing VPN connections include:

- Disable VPN when Roaming over Cellular
- Disable VPN over Cellular

These VPN connection policies help manage VPN connections over cellular data connections, which can in turn help reduce the costs associate with roaming charges or data plan charges.

For more information about the policies used to manage VPN connections in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394992.

Email account management

Probably one of the most important services for users is email. Today, most users are unable to perform their normal job functions without email, and mobile users are no exception. In fact, they are even more dependent on email to maintain communication while on the move.

Windows Phone allows your MDM system to manage user email accounts. You can push specific email accounts to devices as well as prevent users from adding personal email accounts, which helps ensure that organization-owned devices are used for their intended purpose and also prevents users from getting malware from unprotected email accounts.

Email message management

You can use your MDM system to manage the email accounts and connectivity to your mail system, but what about the management of the email messages themselves? You can use EAS services that Microsoft Exchange Server provides in conjunction with your MDM system to manage email messages. Table 2 lists the policies that MDM and EAS support as well as and the policies that only EAS supports.

Table 2. Comparison of Policies Supported by MDM and EAS and EAS only

Policies that MDM and EAS support	Email Policies that only EAS supports
Simple password	Include past email items (duration)
Alphanumeric password	Include past calendar items (duration)
Minimum password length	Email body truncation size
Minimum password complex characters	HTML email body truncation size
Password expiration	Require signed S/MIME messages
Password history	Require encrypted S/MIME messages
Device wipe threshold	Require signed S/MIME algorithm
Inactivity timeout	Require encrypted S/MIME algorithm
Device encryption	Allow S/MIME encrypted algorithm negotiation
Disable removable storage card	Allow S/MIME SoftCerts
Disable Camera	
Disable Bluetooth	
Disable Wi-Fi	
Disable Sync via USB	

The EAS-only polices allow you to control the email messages themselves. You can manage all aspects of email on Windows Phone by using Exchange Server and your MDM system together. For example, you can use Exchange Server to manage S/MIME policies and your MDM system to manage the S/MIME certificates.

For more information on the:

- Management of certificates through MDM on Windows Phone, see “Certificate management” earlier in this guide
- Policies used to manage email messages in Exchange Server, see http://go.microsoft.com/fwlink/?LinkId=394993.

App management

App management is a huge part of any MDM solution. Windows Phone devices help you manage your apps efficiently and effectively, but you can also deploy non-Microsoft apps published through the Windows Phone Store. In addition, you can deploy apps developed by your organization or partners that are not published in the Windows Phone Store (also known as *sideloading*). The Windows Phone MDM features support both deployment methods.

You designate apps as *mandatory* (required to be installed) or *available* (installed at the user's discretion) through your MDM system. This functionality allows you to push any app to a device and optionally make it required for the user. The MDM system can update Windows Phone Store and sideloaded apps. The MDM system can remove sideloaded (LOB) apps without user intervention, as well, which allows you to manage apps without requiring user interaction and helps ensure that only the apps that you desire are installed on devices. Configurable MDM policies prevent the use of Internet Explorer on Windows Phone devices, allowing you to control user access to web content.

Windows Phone Store apps

Most apps are obtained through the Windows Phone Store, from which your MDM system can provide a deep link to Windows Phone Store apps to Windows Phone devices. Your MDM system can also display a catalog of apps that are available from the Windows Phone Store for users to install. In this way, you can limit the apps available for use on Windows Phone devices.

Note If you disable user access to the Windows Phone Store, users will be unable to install Windows Phone Store apps by clicking the deep links.

Similarly, the MDM system allows you to create a list of apps (either by app or by publisher) that users can (approved) or cannot (deny) install. This list offers you fine granularity in controlling which apps can be installed from the Windows Phone Store. You can even limit apps to those deployed through the MDM system.

Sideloaded apps

For sideloaded apps, ensure that the app is signed with your enterprise certificate. Then, you can add the app to your MDM system. When added, your MDM system can deploy the app to approved users and devices. Sideloading keys are not required to sideload apps to Windows Phone 8.1 devices, but the apps must be signed by using a certificate obtained from the Company Dev Center. This certificate must also be installed on the devices that will sideload the app.

For development of custom internal apps, you can register as a Windows Phone app developer at http://dev.windowsphone.com and unlock devices and sideload apps for testing through Microsoft Visual Studio. You can prevent users from unlocking their devices by setting the **Disable development unlock (side loading)** policy, which you can configure with your MDM system.

App Allow and Deny Lists

With the number of available apps in the Windows Phone Store, organizations must be able to control the apps that can run on devices. With Windows Phone, you can create lists of approved and blocked apps by using the App Allow and Deny Lists feature, thereby controlling the availability of Windows

Phone Store or LOB apps on users' devices. Configure the lists through your MDM system by setting the **App Allow/Deny list** policy.

Use the App Allow and Deny Lists feature in conjunction with Assigned Access to provide even tighter control of apps. For example, you could use App Allow and Deny Lists to select which apps from the company portal are available in your MDM system, then use Assigned Access to hide the built-in Windows Phone Store app. In this way, you force users to go to your company portal instead of the built-in Windows Phone Store app.

For more information about managing the Assigned Access feature, see the "Assigned access management" section earlier in this guide.

For more information about the **App Allow/Deny list** policy, see the "Configuration policies overview" section earlier in this guide.

Remote inventory and assistance

Mobile devices rarely remain stationary, and they may rarely connect to your organization's intranet. This means you need to manage and provide support for devices remotely. Windows Phone includes the Remote Inventory and Remote Assistance features to help keep on-the-go users productive in their job roles.

Remote Inventory

Remote Inventory helps you better manage devices by providing in-depth information about each device. Table 3 lists the inventory and additional information that Windows Phone 8.1 provides.

Table 3. Comparison of Inventory Information in Windows Phone 8 and Windows Phone 8.1

Windows Phone 8 and Windows Phone 8.1	New information in Windows Phone 8.1 only
Installed enterprise apps	Phone number
Device name	Roaming status
Device ID	IMEI & IMSI
OS platform type	Wi-Fi IP address
Firmware version	Wi-Fi DNS suffix and subnet mask
OS version	
Device local time	
Processor type	
Device model	
Device manufacturer	
Device processor architecture	
Device language	
Wi-Fi MAC address	

Your MDM system collects the inventory information remotely from the device, then you can use the reporting capabilities of your MDM system to analyze device resources and information. Using this information, you can determine the current hardware and software resources of the device, which helps you keep track of which devices are current with updates.

For more information about the policies used to manage remote inventory in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394994.

Remote Assistance

Users will carry Windows Phone devices with them everywhere. The Remote Assistance feature is designed to help resolve issues that users might encounter even when support personnel don't have physical access to the device. These features include:

- **Remote lock.** Support personnel can remotely lock a device. This ability can help when a user loses the phone and can retrieve it but not immediately (such as leaving the phone at a customer site).
- **Remote password (PIN) reset.** Support personnel can remotely reset the password (PIN) to unlock the device, which helps when users forget their PIN and are unable to access their device. None of the corporate or user data is lost, and the user is able to gain access to their device quickly.
- **Remote ring.** Support personnel can remotely make the device ring. This ability can help a user locate a misplaced device and, in conjunction with the Remote lock feature, help ensure that unauthorized users are unable to access the device if they find the device.

These remote management features help you reduce the IT effort required to manage devices. They also help users quickly regain use of their device should they misplace it or forget the device password.

For more information about the policies used to manage remote assistance in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394995.

Device retirement

Device retirement (un-enrollment) is the last phase of the device life cycle. Typically, mobile device retirement is a complex and difficult process for organizations. When the device is no longer needed, any corporate data must be removed (wiped) from the phone. BYOD scenarios make retirement even more complex, because the user might have personal data on the device that they want to keep. So, organizations must remove their data without affecting the user's data.

If the device is lost or stolen, the organization must remove any corporate data from the device, as well. For these scenarios, device retirement must be done remotely, because authorized users won't have physical access to the device.

You can remotely remove all corporate data from a Windows Phone device without affecting the existing user data. IT pros or the device's user can initiate device retirement. When the retirement is completed, the device is returned to a consumer state. The following list offers some of the corporate data removed from a device when it is retired:

- Email accounts
- Enterprise-issued certificates
- Network profiles
- Enterprise-deployed apps

- Any data associated with the enterprise-deployed apps
- Enterprise-issued device policies

Note All of these features are in addition to the software and hardware factory reset features of the device, which people can use to restore the device to the factory configuration.

The policies that are available for managing device retirement include:

- Disable user manual MDM un-enrollment
- Disable user manual MDM software and hardware factory reset

Your MDM system can set these policies on devices as required (see the “Configuration policies management” section earlier in this guide). For BYOD device, user may want to retire the device as well. When the user retire a device, you MDM system receives a report from the device that user is retiring the device. Use this information to perform additional analysis, if necessary.

For more information about the policies used to manage device retirement (un-enrollment) in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394996.

Conclusion

Mobile devices (and specifically smartphones) are an integral part of doing business today, and this continuing proliferation of mobile devices requires a comprehensive MDM system that can provide the management tools you need. Windows Phone 8.1 includes many new MDM features that help MDM systems provide superior management capabilities compared with other mobile operating systems. The ease of device enrollment; the breadth and depth of configuration management; the granularity of app management; and the collection of remote inventory, remote assistance, and device retirement (un-enrollment) make Windows Phone the right choice for providing enterprise-class MDM support.

You can manage Windows Phone 8.1 by using an on-premises, off-premises, or hybrid MDM solution, such as those that System Center 2012 R2 Configuration Manager and Windows Intune provide as well as third party MDM solutions. When used in conjunction with Exchange Server, you can not only manage the device and configuration settings but protect even the email messages users send and receive on the device.

Try a free evaluation of System Center 2012 R2 Configuration Manager and Windows Intune to explore the MDM features in Windows Phone 8.1. Alternatively, contact your MDM system vendor about evaluating their its for Windows Phone 8.1 MDM features. Find out today how Windows Phone 8.1 can help protect your confidential data and improve user productivity and satisfaction, all while reducing your support cost.