



# Windows Phone 8.1 in the Enterprise

Version 1.4



MobileIron  
415 East Middlefield Road  
Mountain View, CA 94043 USA  
Tel. +1.650.919.8100  
Fax +1.650.919.8006  
info@mobileiron.com

|  |    |
|--|----|
| Introduction   | 3  |
| Why Windows Phone 8.1 is Important to the Enterprise | 4  |
| Improved User Experience for Business Users          | 6  |
| Wi-Fi Configuration                                  | 7  |
| VPN Configuration                                    | 8  |
| RemoteLock Configuration                             | 9  |
| Better Management and Configuration for IT           | 10 |
| Certificate Provisioning                             | 10 |
| Policy Management                                    | 11 |
| Push Notification                                    | 13 |
| Logging Support                                      | 13 |
| Improved Application Security                        | 13 |
| Conclusion   | 14 |



## Introduction

When Windows Phone 8 was first launched, the majority of its platform innovations were focused on delivering a robust end-user experience. Strong support for Microsoft productivity tools, such as Exchange, SharePoint, and Lync, made Windows Phone an attractive option for business users. But not all enterprises were ready to fully embrace the new platform. While it included baseline security and management capabilities like remote wipe and device encryption, Windows Phone 8 did not meet the stringent policies some enterprises required for protecting corporate data and resources.

The release of Windows Phone 8.1 changes the game. Microsoft is delivering a rich new feature-set for business users, and providing IT departments with the compliance and security they require. These new security and management features, called the Enterprise Feature Pack, are included as a core component of Windows Phone 8.1. When combined with an enterprise mobility management (EMM) platform, these capabilities make it much easier for enterprises to adopt the Windows Phone platform.


As a committed Microsoft partner for mobile device management (MDM), MobileIron provides a purpose-built mobile IT platform that helps enterprises take advantage of Windows Phone 8.1 to achieve their Mobile First ambitions. This document is designed to help IT organizations better understand how MobileIron enables a more manageable and secure experience for Windows Phone users.

## Why Windows Phone 8.1 is Important to the Enterprise

Windows Phone adoption has been growing steadily, reaching double-digit market share in many countries, including the top five European markets. Enterprises are finding Windows Phone is an attractive productivity tool given it allows business users to take advantage of the tight integration with Microsoft's infrastructure, such as Active Directory, Exchange, SharePoint, and Lync. IT organizations benefit from their users having a consistent experience. Additionally, as Microsoft continues to push toward a "write once, run anywhere" model, the transition from enterprise application to mobile application development has become much easier.

While Windows Phone 8 brought a lot of functionality to the table for the business user, there were limitations for both IT organizations and developers wanting to enable the platform in their environments. Many of the required building blocks were there – the ability to treat enterprise and personal data separately, corporate policy configuration, selective wipe, password enforcement, and device encryption – but the management and security features didn't satisfy all connectivity and compliance requirements for enterprises.

By comparison, Windows Phone 8.1 adds nearly 10 times the management and security APIs available for IT to ensure that Windows Phone 8.1 devices comply with corporate policies. Along with these improved management and security controls, enterprises now have the ability to enable users to easily connect their Windows Phones to corporate VPN and Wi-Fi – without having to worry about how to get certificates or credentials onto their devices. They'll also be able to offer better Help Desk support when users run into password or application issues.



Windows Phone 8.1 adds nearly 10 times the management and security APIs available for IT to ensure that devices comply with corporate policies.

MobileIron is working closely with Microsoft to ensure all of these security and management features are easy to implement and maintain. Here are the key Windows Phone 8.1 investments in user enablement, management, and security that you can expect to take advantage of using the MobileIron platform:

| User Enablement                       |  |
|---------------------------------------|--|
| VPN Configuration                     | <i>Users will be able to connect to VPN to access corporate resources. Apps can also be configured to automatically connect to a specific VPN when launched.</i>   |
| Wi-Fi Configuration                   | <i>IT will be able to configure, manage, and enable devices to connect to corporate Wi-Fi networks.</i>  |
| RemoteLock                            | <i>Help Desk will be able to reset a user's PIN, eliminating the need for the user to do a complete system reset if they forget their PIN.</i>   |
| Management and Security               |  |
| Certificate Provisioning              | <i>Organizations who rely on certificates for enhanced security will be able to manage certificate provisioning, allowing them to delete, replace, or renew certificates automatically.</i>                  |
| Policy Management                     | <i>IT will have in-depth device hardware, security, and application controls they can enable or disable to ensure devices comply with corporate policies.</i>  |
| Logging Support                       | <i>When users call the Help Desk regarding phone-related issues, service representatives will be able to view phone logs to help them troubleshoot and resolve issues more quickly.</i>                      |
| Client Push Support                   | <i>IT will be able to initiate a management session with any user device to update applications or apply new policies.</i>   |
| Application Whitelisting/Blacklisting | <i>IT will be able to create allow and deny lists for individual applications to prevent non-compliant applications from being downloaded or run on user devices.</i>  |
| RemoteLock                            | <i>To prevent loss of corporate and personal data, IT will be able to remotely lock a device that has been lost or stolen. On devices that may not have had a PIN set, IT will be able to reset the PIN.</i> |

## Improved User Experience for Business Users

For any corporate-owned device or Bring Your Own Device (BYOD) program, it is imperative that employees can use their device to securely access corporate resources and data anywhere, at any time. Many enterprises initially delayed deployment of Windows Phones because they could not provide secure connectivity to corporate networks. Windows Phone 8.1 remedies this challenge with new VPN and Wi-Fi features so enterprises can securely connect employees to corporate resources.

MobileIron has extensive experience with the Windows Phone 8 platform, as well as the Windows 8.1 operating system for laptops and tablets. MobileIron already supports several features in the Enterprise Feature Pack Update for Windows 8.1 devices, including Wi-Fi and VPN configuration features. Supporting these features on Windows Phone 8.1 is a natural extension of the MobileIron platform, helping customers manage and secure any Windows-based device, whether corporate-owned or BYOD.



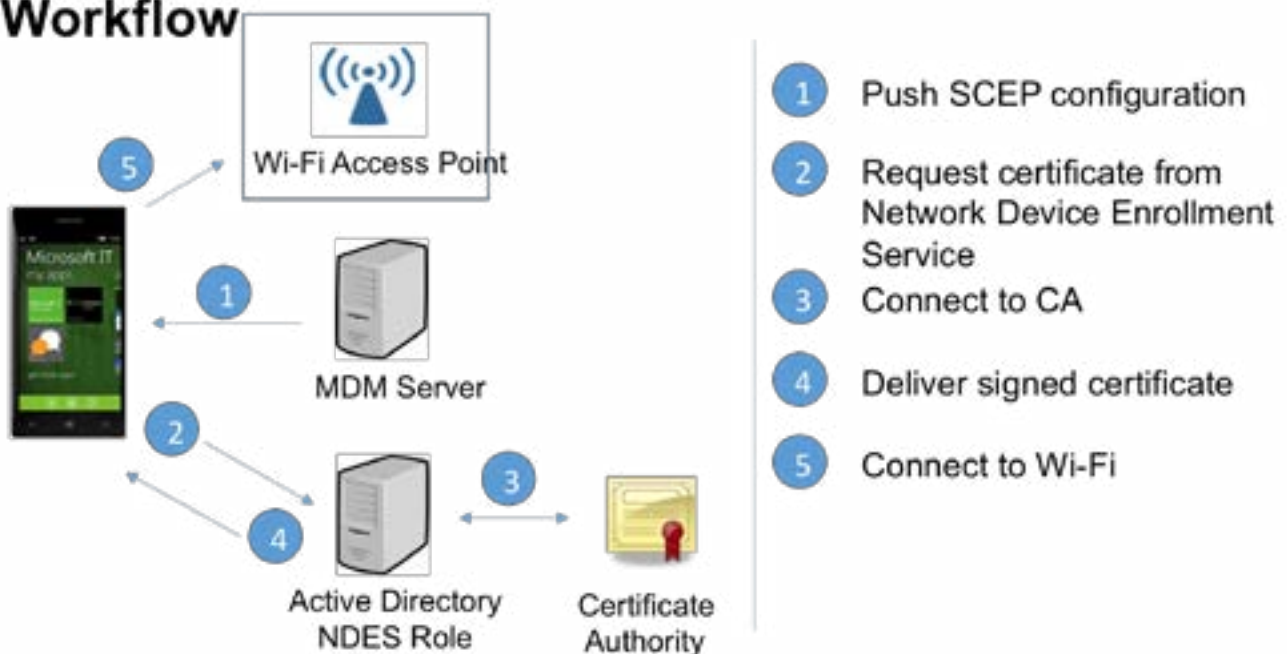
## Wi-Fi Configuration

Prior to the 8.1 release, Windows Phone users could not seamlessly connect their mobile devices to the corporate wireless network. The devices did not support enterprise-standard secure wireless protocols, such as EAP-TLS.

With Windows Phone 8.1, users with the right corporate credentials will automatically be connected to available corporate networks. Their devices will instantly recognize enterprise networks built on Open, WEP, WPA2, PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, EAP-SIM, or EAP-AKA protocols.

To create these connections, the Windows Phone 8.1 MDM server pushes out the Simple Certificate Enrollment Protocol (SCEP) configurations needed by the device for certificate enrollment. The device uses these SCEP configurations to request a certificate from Active Directory – which then connects it to the certificate authority to obtain the necessary signed certificate and deliver it back to the device. With the certificate in place, the device can then connect to the Wi-Fi access point. All of this is accomplished automatically without end-user input.

### Windows Phone 8.1 Wi-Fi Configuration Workflow



With the MobileIron platform, administrators can easily configure Wi-Fi policies and automatically migrate users to the new settings. For added security, MobileIron makes it possible to prevent users from manually configuring any Wi-Fi connection other than the ones defined in the MobileIron console.

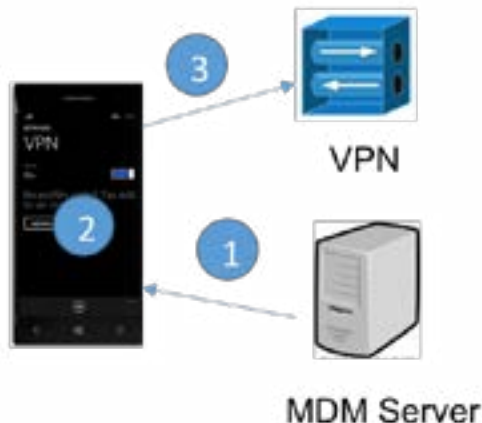
## VPN Configuration

VPNs are also supported for the first time in Windows Phone 8.1, enabling users to access corporate applications from anywhere, anytime. IT administrators will be able to configure policies that allow Windows Phone users to automatically connect to a corporate VPN. Another bonus: MobileIron administrators can manage these configurations with the same familiar interface they use to manage Windows 8.1 laptops and tablets.

Microsoft has also added per-application support for VPN connections in the Windows Phone 8.1 release. With this capability, IT will be able to define how individual applications work with VPN solutions, allowing administrators to match them with a specific destination. For example, a user may have an expense report application that connects to the corporate VPN and a time-tracking spreadsheet managed by a vendor. With Windows Phone 8.1, connecting to the appropriate network becomes fully automated. Simply by clicking on the desired application, it will seamlessly connect to either the corporate VPN or the third-party's VPN.

The application-level VPN configuration can be defined in the MobileIron console, which then pushes the configuration settings to the device. When the user launches the application, it will make sure it is connected to the correct VPN. If another VPN is already active, it will shut down that connection and open the appropriate VPN. All of this gets executed in the background seamlessly and does not require any action from the user. When you consider the alternative – manually selecting a VPN and entering multiple usernames and passwords to gain access – this is not only a better experience for users, it provides a significant productivity benefit as well.

## Windows Phone 8.1 Per-app VPN Configuration



- 1 Define per-app VPN configuration and apply to device.
- 2 Start application
- 3 Application finds VPN configuration and automatically uses it



## RemoteLock Configuration

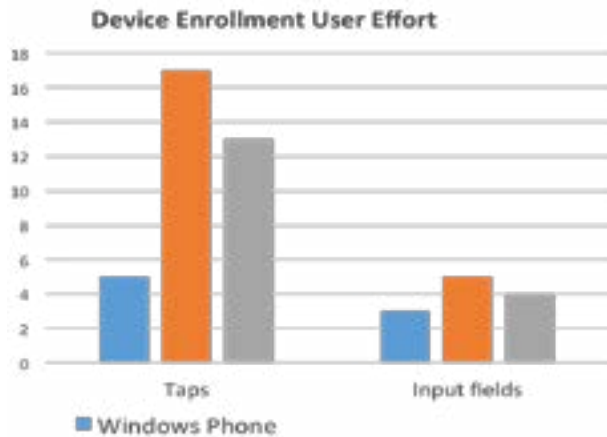
IT organizations have always been able to require that Windows Phone users have a PIN for phones to access corporate resources, such as email. If users forgot that PIN, the only remedy was to do a complete reset of the phone – which could mean hours of reconfiguring settings and reloading applications.

With the release of Windows Phone 8.1 comes RemoteLock, which allows IT to lock a device that has a PIN set, or reset the PIN on any device, even if a PIN was never previously set. If a device is locked, users can contact the Help Desk, which will be able to use the MobileIron console to easily reset the user's PIN. The Help Desk forces the device to generate a new PIN that complies with the PIN complexity policies already established on the device. (If a PIN policy has not been set on the device, the device will generate an eight-digit numeric PIN.) This allows the user to simply log back into their device and find all of their applications and data are still in place, eliminating major work disruptions.

If a device is lost or stolen, IT will be able to use the MobileIron console to remotely lock the device to prevent unauthorized users from accessing personal or corporate data.

## Better Management and Configuration Options for IT

Enabling Windows Phones in the enterprise means being able to control how these mobile devices interact with corporate resources. Part of that interaction is establishing VPN and Wi-Fi connections or being able to remotely lock a lost device. But there is a much broader set of features required to keep both user and corporate information safe – whether that is from malicious code, confidential data loss, legal liabilities, or simply productivity loss.



As an enterprise-ready operating system, Windows Phone 8.1 includes important new features that help organizations control access and comply with corporate policies. To communicate with a management server that can manage all these interactions, Windows Phone 8.1 has a built-in enrollment client, phone management client, and a host of 50+ APIs.

The streamlined onboarding process for users is quick and easy. It requires only five taps of the phone and the completion of three input fields. This makes it possible to enroll Windows Phone devices in less than one minute.

From enrollment to ongoing administration, MobileIron will take full advantage of all the new components and APIs to make it as simple as possible for organizations to incorporate Windows Phone 8.1 devices into their workplace. At enrollment, the Mobile@Work application automatically loads as soon as the phone is enrolled to provide immediate user access to the Enterprise Storefront. This will allow IT to quickly distribute in-house applications and recommend external third-party applications, all while maintaining the native experience users demand. For administration, IT can expect to use the same familiar MobileIron console and settings to extend management and security to new Windows Phone 8.1 devices.



## Certificate Provisioning

Providing increased security for mobile devices, certificates are particularly important in highly regulated industries, such as finance, government, and healthcare. Certificates ensure that no username or password is stored on the device. If lost or stolen, unauthorized users will not gain access to information that could allow them to breach corporate networks. Perhaps more important to users, certificates allow them to avoid repeatedly re-entering various usernames and passwords to access corporate resources.

MobileIron is one of the only vendors that provided certificate-provisioning functionality for the original Windows Phone 8 release. Now, with these built-in Windows Phone 8.1 capabilities, MobileIron will deliver a more robust solution for managing certificate-based authentication. Windows Phone 8.1 supports root, certificate authority (CA) chain, and client certificates, allowing all of these to be configured by the MobileIron console to secure Wi-Fi, VPN, email, and browser use. IT will be able to enroll, delete, or replace any of these certificates on devices. If an employee loses a device or leaves the company, IT will be able to revoke the certificates resident on that employee's device.

With Windows Phone 8.1, MobileIron will also make it easier to keep certificates up to date. Administrators will be able to proactively trigger new enrollment requests before current certificates expire, automatically giving users uninterrupted access to corporate resources.

## Policy Management

One of the most significant improvements in Windows Phone 8.1 is around device policy management. IT organizations will now have control over more than 20 elements to help limit organizational risk and enforce compliance. Devices that were once wide open can now fall under the strict control that IT expects to provide in an enterprise setting.

The most noteworthy policy control updates are listed in the chart below – all of which will be incorporated into the MobileIron platform to provide a high degree of control over management and security for Windows Phone devices. Most of these policies are enforced device-wide rather than being application-specific. For example, it will not be possible to disable Copy and Paste for a specific application like email, but allow it in Microsoft Word. There is one exception: you can turn off Save As and Sharing capabilities for all Microsoft Office applications. These Office-specific features are separated out to help limit data leakage, while also still keeping users productive on their Office applications.

| Category | Policy Area                    | Functionality  |
|----------|--------------------------------|--|
| System   | Near Field Communication (NFC) | Allow or disable communications with NFC devices, such as parking meters or credit card scanners.                                  |
|          | Bluetooth                      | Allow or disable ability to use Bluetooth devices. Can also disable Bluetooth, but allow the configuration of hands-free profiles. |
|          | Telemetry                      | Allow or prevent the device from sending telemetry information, such as SQM or Watson.   |
|          | Camera                         | Disable or enable device camera.   |
|          | GPS                            | Allow or disable GPS capability to share device location with applications.  |

| Category        | Policy Area            | Functionality  |
|-----------------|------------------------|--|
| Connectivity    | Wi-Fi                  | Allow or disable Wi-Fi connection. Can also limit ability to manually set up Wi-Fi connections outside of MDM-server installed networks.       |
|                 | Internet Sharing       | Allow or disable Internet sharing  |
|                 | HotSpots               | Allow or disable the device from automatically connecting to Wi-Fi hotspots and social networks or report on hotspot information to Microsoft. |
| Data Protection | USB                    | Allow or disable the ability for a desktop to access phone storage via USB.  |
|                 | OneDrive/Live Accounts | Allow or disable Microsoft OneDrive or Windows Live Accounts.  |
|                 | Encryption             | Allow enterprise to turn on internal storage encryption. (Once turned on, cannot be turned off).   |
|                 | Copy and Paste         | Allow or disable the ability to copy and paste data from a device.   |
|                 | Storage Card           | Allow or disable use of SD storage card.   |
|                 | Screen Capture         | Allow or disable the ability to take screen captures.  |
| Cost Control    | Roaming                | Prevent the device from using data, profile, or VPN when roaming to avoid unwanted carrier charges.  |
| Applications    | Browser                | Allow or disable Internet Explorer on a device   |
|                 | Manual email setup     | Allow or prevent users from manually configuring email accounts on a device.   |
|                 | Microsoft Office       | Allow or disable Save As functionality and/or Sharing in Microsoft Office.   |
|                 | Microsoft Store        | Specify whether app store is allowed on the device.  |

## Push Notification

With push notification, IT administrators can make sure the latest policies are applied to devices. While Windows Phone 8.1 will check every four hours for updates and policy changes, if IT is troubleshooting a device, they may want to see policy changes take effect immediately. Just as it does currently for Windows 8.1 laptops and tablets, the MobileIron console will be able to “force” check-in for the device in real-time. This can be especially useful if IT needs to push critical application downloads to end-user devices.


## Logging Support

When it comes to supporting users with troubleshooting device issues, Windows Phone 8.1 offers great improvements for the Help Desk. Prior to this release, the Help Desk team had no ability to see what the user was experiencing. With logging support, staff can now use the MobileIron console to examine device logs to more quickly resolve user issues. Logs include transaction errors during MDM enrollment, DM session, and SCEP certificate enrollment. Logs are exposed via Windows Phone Developer Power Tools in WP8.1 SDK and can be viewed in Windows Performance Analyzer.

## Improved Application Security

On corporate networks, preventing rogue applications from running on devices is extremely important. Inappropriate applications can introduce malware, compromise confidential information, or open up companies to legal liabilities. The new application security features in Windows Phone 8.1 make it even easier to prevent these risks.

Using the MobileIron console, IT administrators can configure a list of applications that can be allowed or denied on any device or group of devices. Different types of applications, such as a Windows Phone Store app or an enterprise line-of-business app, can easily be blocked if required. The only applications that cannot be blocked are native applications published by Microsoft. The two exceptions to this are Internet Explorer and Windows Phone Store, which were mentioned in the previous section as they can be disabled via policy.



IT administrators can configure a list of applications that can be allowed or denied on any device or group of devices.

The Allow list – or application whitelist – ensures that only those applications explicitly listed by IT will be available for use or install by the user. If a user does attempt to download or run an unapproved application, they will get an administrator message explaining why the download or use was denied.

The Deny list – or application blacklist – defines a set of applications that cannot be installed or run (if the

application already exists on the device). Enterprises often use this capability to prevent the use of non-compliant applications on mobile devices. For example, DropBox is very popular, but enterprises concerned with protecting confidential data do not want employees saving corporate documents to this application. To prevent this, DropBox can be added to the deny list and users will not be able to install or launch the app (if the app was installed prior to the policy being initiated).

## Conclusion

With the Windows Phone 8.1 release, enterprises can confidently embrace these devices in conjunction with the MobileIron Platform. It's a win-win: users get to use great productivity devices and companies can ensure compliance polices are enforced to minimize risk to corporate information and resources.

Windows Phone 8.1 also opens up opportunities for organizations to re-evaluate existing mobility infrastructure. Enterprises with BlackBerry Enterprise Server (BES), for example, can use a combination of MobileIron and Windows Phone 8.1 to provide BES-caliber security and management without the expense and user frustration that comes with being locked in with a single mobile hardware provider. Using this solution, IT organizations can accelerate migration from legacy BlackBerry deployments in their journey to becoming a Mobile First organization.

MobileIron is actively helping enterprises fast track their Mobile First plans with our highly scalable Mobile IT platform. Enterprises globally can now further leverage the MobileIron platform to take advantage of Windows Phone 8.1 devices. Our close alignment with Microsoft engineering and years of in-depth experience managing Windows Phones in the enterprise give us a unique ability to help customers maximize their success with these new devices. For more information on managing Windows Phone 8.1, contact your MobileIron sales representative.



MobileIron  
415 East Middlefield Road  
Mountain View, CA 94043 USA  
Tel. +1.650.919.8100  
Fax +1.650.919.8006  
info@mobileiron.com