Guidance

End User Devices Security Guidance: Windows Phone 8.1

Published 06 January 2015

Contents

This guidance is applicable to devices running Windows Phone 8.1. This guidance was developed following testing performed on Nokia Lumia 520, Lumia 925, and the HTC 8X using System Center Configuration Manager (SCCM) 2012 R2 CU3 with the Windows Intune Connector, Windows Phone 8.1 Extension and ADFS 3.0.

1. Usage scenario

Windows Phone 8.1 devices will be used remotely over 3G, 4G and non-captive Wi-Fi networks to enable a variety of remote working approaches such as:

- accessing OFFICIAL email
- reviewing and commenting on OFFICIAL documents
- accessing the OFFICIAL intranet resources, the Internet and other web-resources

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the Confidentiality and Integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions

- Arbitrary third-party application installation by users is not permitted on the device. An enterprise application catalogue should be used to distribute in-house applications and trusted third-party applications

2. Summary of platform security

This platform has been assessed against each of the twelve security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can satisfy the security recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	[!] The VPN cannot be configured to meet PRIME or PSN interim standards. The VPN can be disabled by the user. The built-in VPN has not been independently assured to Foundation Grade, and no suitable third-party products exist.
2. Assured data-at-rest protection	Windows Phone 8.1 device encryption has not been independently assured to Foundation Grade. It is not possible to set a passphrase to unlock the encryption key.
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	
10. Device update policy	The enterprise cannot force the user to update their device software.
11. Event collection for enterprise analysis	[!] There is no facility for collecting detailed logs remotely from a device, and collecting forensic log information from a device is very difficult.
12. Incident response	

2.1 Significant risks

The following significant risks have been identified:

- The VPN has not been independently assured to Foundation Grade, and currently does not support some of the mandatory requirements expected from assured VPNs. Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- The VPN is unable to negotiate a PRIME or PSN interim compliant set of cryptographic algorithms, as such there is a risk that data transiting from the device could be compromised.
- The VPN can be disabled by the user, leading to potential for data leakage onto untrusted networks.
- Windows Phone 8.1 device encryption has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised. It is not possible to set a passphrase to unlock the disk encryption key.
- Users can choose not to apply device updates that have not been marked as critical, this may lead to security issues not being patched.
- There is currently no mechanism which allows Windows Phone 8.1 devices to send logs to enterprise servers using native functionality or MDM configuration. Therefore the ability for event collection for enterprise analysis is severely limited.

3. How the platform can best satisfy the security recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

3.1 Assured data-in-transit protection

Use the native IPsec VPN client until a Foundation Grade VPN client for this platform becomes available.

3.2 Assured data-at-rest protection

Use the device's native data encryption. The data is protected when powered off, but it is not protected when the device is powered on.

Disable removable storage as data stored on it is not encrypted.

3.3 Authentication

The user has a strong 9-character password to authenticate themselves to the device. This password unlocks a key which encrypts certificates and other credentials, giving access to enterprise services.

3.4 Secure boot

This requirement is met by the platform without additional configuration.

3.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

3.6 Application whitelisting

The platform relies on application code signing to enforce that only applications from the Microsoft Store and appropriately signed line-of-business applications from the enterprise are allowed to run.

An enterprise application catalogue can be established to permit users access to an approved list of in-house applications. If the Windows Phone Store is enabled, a whitelist can be used to control which applications can be installed.

Further restrictions may be placed on functionality within apps (particularly system applications and settings) through Kiosk Mode. The Windows Store can also be disabled if not needed.

3.7 Malicious code detection and prevention

Disable developer-unlocking of devices so that Windows Phone will only run applications from the Store and appropriately signed line-of-business applications from the enterprise.

Applications hosted in the Windows Phone store are scanned for potentially harmful or malicious activity prior to being made available for download.

The enterprise app catalogue should only contain approved in-house applications which have been checked for malicious code. Content-based attacks can be filtered by scanning on the email server.

3.8 Security policy enforcement

Disable un-enrolment from the MDM service. Settings applied to the device via the MDM service cannot then be modified or removed by the user.

The phone can optionally be configured to prevent the user performing a factory reset.

3.9 External interface protection

Wi-Fi, NFC, Bluetooth, removable storage and USB Sync can all be disabled.

3.10 Device update policy

Windows Store apps will automatically download and install updates by default. Installation of device updates rely on user interaction. The enterprise cannot control whether updates not marked as critical are applied.

3.11 Event collection for enterprise analysis

There is no facility for collecting logs remotely from a device, and collecting forensic log information from a device is very difficult.

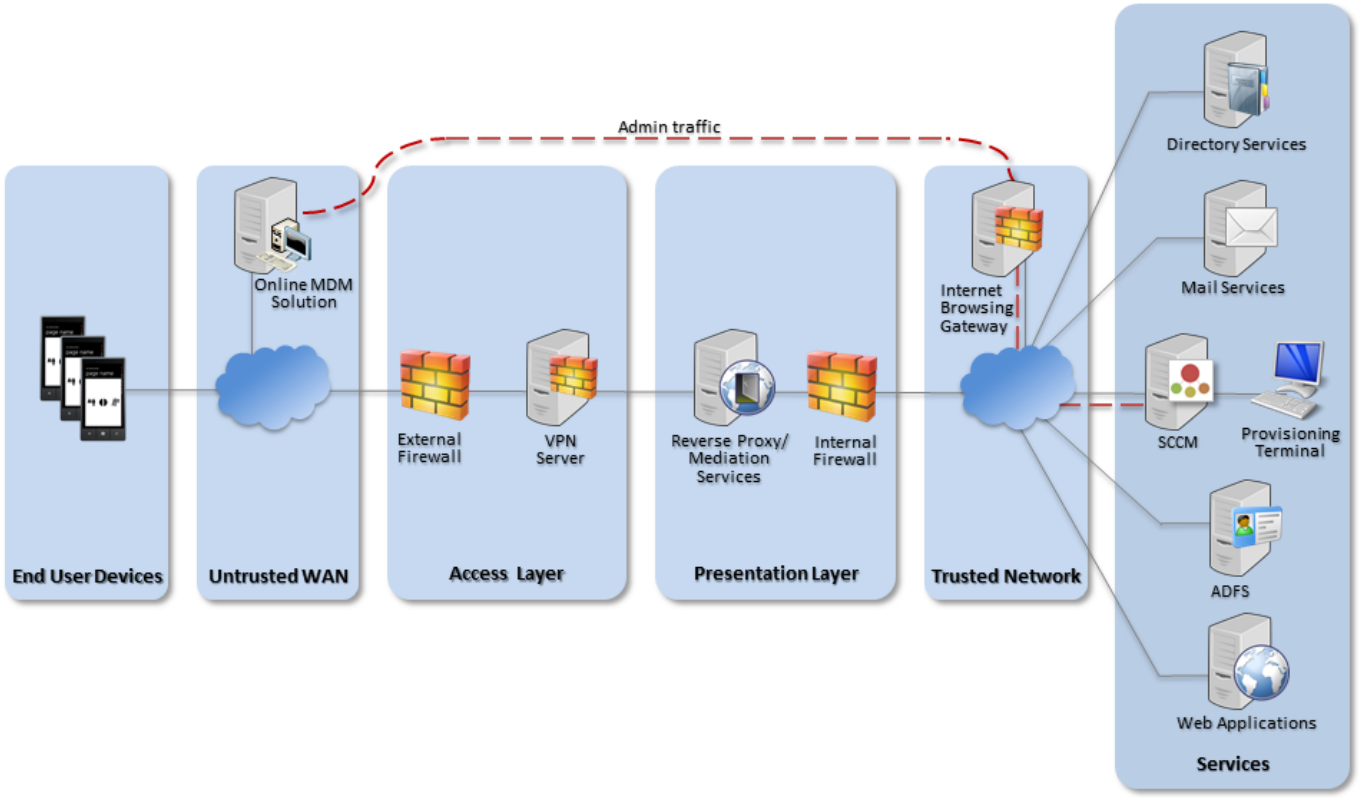
3.12 Incident response

Windows Phone 8.1 devices can be locked, wiped, and configured remotely by MDM. In the event of a compromised device, a full device wipe is recommended, but it is possible to perform a selective wipe of only enterprise data stored on Work Folders and in some enterprise apps.

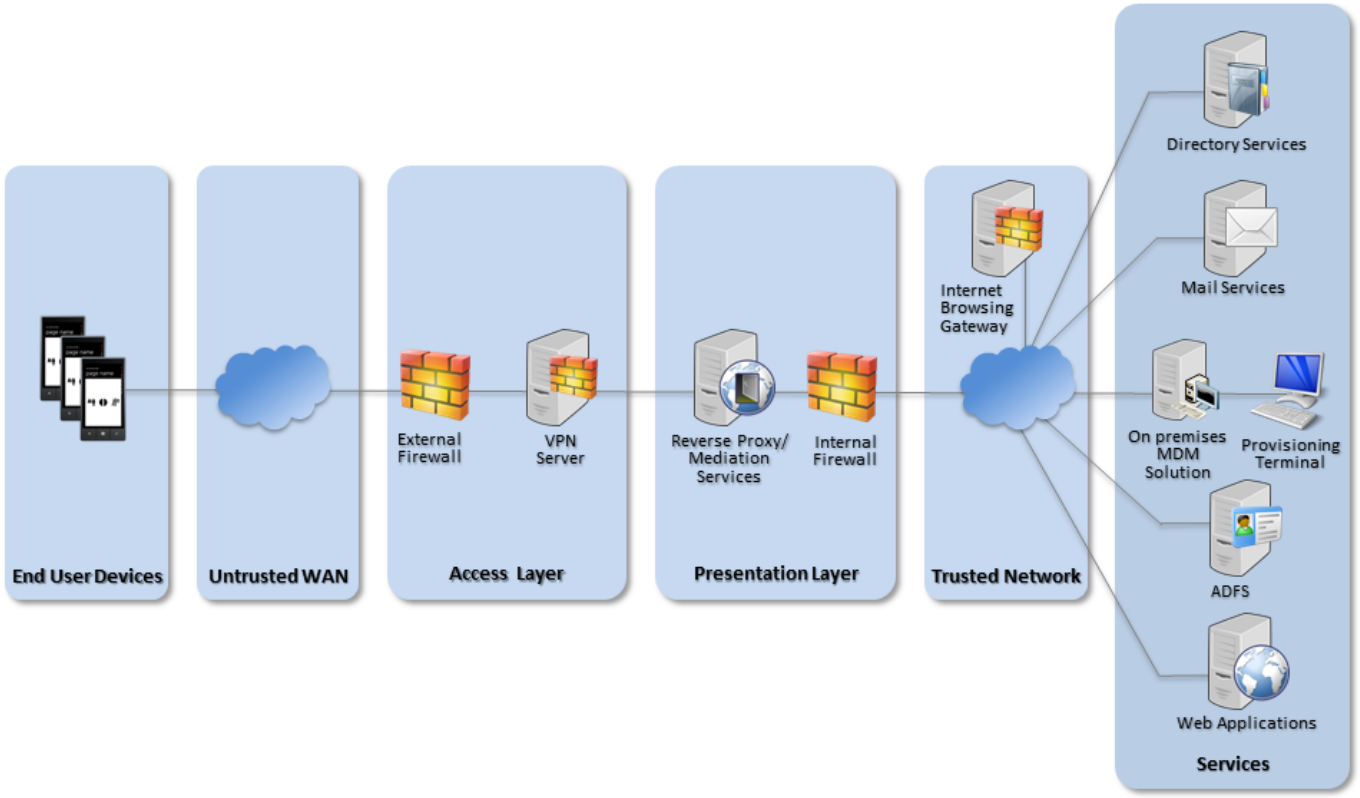
4. Network architecture

All remote or mobile working scenarios should use a typical remote access architecture based on the Walled Garden Architectural Pattern. The following network diagrams describe the recommended architecture for this platform.

Windows Phone 8.1 devices can be either be managed by an on-premises MDM or an online MDM solution, in either case the device configuration to be applied must be set by an administrator from the organisation.



Recommended network architecture for Windows Phone 8.1 deployments using an online MDM solution



Recommended network architecture for Windows Phone 8.1 deployments using an on-premises MDM solution

5. Deployment process

The following steps should be followed to prepare the enterprise infrastructure for hosting a deployment of these devices:

1. Deploy an appropriate MDM solution to manage devices. Recommended options are SCCM with Windows Intune Connector, Windows Intune in a cloud configuration, or a suitable third party MDM solution which supports the required settings.
2. Procure, deploy and configure other network components, including an approved IPsec VPN gateway.
3. Deploy ADFS and a web application proxy if using Workplace Join.
4. Deploy a Company Portal app signed with an enterprise code-signing certificate.
5. Set up the configuration profiles for the end-user devices in accordance with the settings later in this guidance including VPN profiles and corresponding client certificate profiles using Simple Certificate Enrolment Protocol (SCEP).

6. Provisioning steps

The following steps should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users:

Load the following certificates into the machine store on the device, using the provisioning terminal:

- Enterprise CA certificate (used to validate the server certificates presented by the Exchange server, proxies and VPN server certificate)
- SSL client certificate (for authentication to the reverse proxy for intranet services - into the TPM if available)

If using Microsoft Intune:

- Add the mobile user into Intune and assign the required access groups, this can be done via Azure Active Directory sync (AAD sync).
- Install the company portal app either by downloading it from the company store or via the `workplace` option within the device settings and adding your company credentials.

If using a third party MDM solution:

- Enrol the device into the deployed MDM solution by installing the MDM client software onto the device and deploying the predefined configuration profile.

7. Policy recommendations

7.1 MDM policy

The following table outlines the recommended policy settings when using Windows Intune.

Configuration Rule	Configuration Setting
Password	
Require a password to unlock a mobile device	Required
Minimum password length	9
Remember password history	Yes
Prevent reuse of previous passwords	8
Number of repeated sign-in failures to allow before the device is wiped	5
Minutes of inactivity before screen turns off	10
Password complexity	Strong

Require password type	Alphanumeric
Minimum number of character sets	3
Allow simple passwords	No
Accounts and Synchronization	
Allow Microsoft account	Disabled
Email	
Allow non-Microsoft account	Disabled
Encryption	
Require encryption on mobile device	Yes
Hardware	
Allow geolocation	No
Allow removable storage	No
Allow NFC	No
Allow Bluetooth	No
Allow Wi-Fi hotspot reporting	Disabled

Additional Settings (by OMA-URI suffix)	
Security/AllowManualRootCertificateInstallation	0
ApplicationManagement/ApplicationRestrictions	[Permitted app whitelist]
ApplicationManagement/AllowDeveloperUnlock	0
Search/AllowStoringImagesFromVisionSearch	0
Experience/AllowManualMDMUnenrollment	0
Experience/AllowSyncMySettings	0
DeviceLock /DeviceePasswordExpiration	90
System/AllowTelemetry	0
Enterprise Owned devices	
System/AllowUser ToResetPhone	0

7.2 VPN profile

A VPN profile should be configured using Microsoft System Center Configuration Manager to negotiate the following parameters. It should be delivered by MDM to prevent the settings being changed by the user. Some of the configuration must be performed on the VPN server.

This configuration differs slightly from that of other End User Devices (which follow the PRIME and PSN interim cryptographic profiles) as Windows Phone 8.1 does not completely support these. A secondary VPN server or configuration may therefore need to be configured to run in parallel if other devices are being deployed.

SCCM VPN profile

Setting	Value(s)
Tunnel Type	IKEv2
Authentication Mode	Use machine certificates (provisioned using SCEP)
Send all traffic through the VPN	Yes

Negotiation parameters

Setting	Value(s)
IKE DH Group	2 (1024-bit)
IKE Encryption Algorithm	AES-256
IKE Hash Algorithm	SHA-256
IKE Authentication Method	RSA X.509
IPsec Encryption	AES-256
IPsec Auth	SHA-1
SA Lifetime	24 Hours

8. Enterprise considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for Windows Phone 8.1 deployments.

8.1 Windows Phone Store applications

The configuration given above prevents users from installing applications from the Windows Phone Store. An organisation can still distribute its own applications using the Company App and Windows Intune or other compliant MDM solution.

If the Microsoft account is enabled to provide access to the Store, there are no enterprise controls to disable Cloud backup or the 'find my phone' feature.

8.2 Mobile device management

Some of the recommended policies above are only available when using an MDM that supports the Open Mobile Alliance (OMA) device management protocol such as SCCM with the Windows Intune Connector. Standalone Intune deployments will not support the items listed under `Additional Settings`.

It is essential that system architects evaluate which policies their MDM solution will allow them to set. MDM solutions that cannot set all the policies specified in the policy recommendations section should not be considered for use.

Provisioning of Windows Phone 8.1 devices via MDM solutions that require cloud based interaction are intrinsically dependent on the vendor's online services and considerations around the risk of placing the security and control of their devices and data under a third party should be made.

8.3 Workplace Join and Selective Wipe

Windows Phone 8.1 devices can be registered with the enterprise using Workplace Join. The feature enables single sign-on to corporate web apps, allows access control decisions to consider the device type and to synchronise data to the device using Work Folders and helps automate device enrolment with the workplace.

Work Folders is a feature that synchronises enterprise data to mobile devices. As that data is encrypted on the phone, it can be easily removed with a Selective Wipe. This is a separate feature to the Selective Wipe implemented by Intune, which is designed to remove Company Apps, Company App data and MDM policy. It is not necessary to implement Work Folders to use the Selective Wipe implemented by Windows Intune, and vice versa.

8.4 Cloud services

Organisations choosing to use cloud based services such as OneDrive can use the CESG Cloud Security Guidance to help them understand both the benefits and risks of using online services.

OneDrive is incorporated into many applications available for use by the Windows Phone 8.1 device such as Microsoft Office Mobile. Procedural controls are necessary to prevent users from authenticating to OneDrive

and storing sensitive files within the Microsoft cloud.

The Store and default Mail applications will not function if the Microsoft account is disabled as recommended above. Access to corporate email, and enterprise apps are not affected by this.

Legal information