Guidance

End User Devices Security Guidance: Windows Phone 8.1 Update 2

Published 14 September 2015

Contents

1. About this guidance

The End User Devices Security and Configuration Guidance is for Risk Owners and Administrators to understand the risks, security advantages and recommended configuration of Windows Phone 8.1 Update 2 within a remote working environment at the OFFICIAL and OFFICIAL SENSITIVE classification. Risk owners are encouraged to read the Risk owners' summary and Enterprise considerations sections. Administrators and system integrators are encouraged to read the whole document.

This guidance is applicable to devices running Windows Phone 8.1 Update 2, and is an update to the previous guidance for Windows Phone 8.1. Windows Phone 8.1 Update 2 introduced some updates that have security implications, including changes to the VPN that allow it to be locked into an always-on mode and an update to e-mail protection ensuring that they are encrypted when the phone is locked.

This guidance was developed following testing performed on a Nokia Lumia 830 managed with System Center Configuration Manager (SCCM) 2012 R2 SP1 with the Windows Intune Connector, Windows Phone 8.1 Extension, ADFS 3.0 and Azure Active Directory Sync Services.

It is important to remember that any guidance points given here are just recommendations;

none of which are mandatory. They have been suggested as a way of satisfying the 12 security recommendations that mitigate the threat at OFFICIAL. Risk owners and administrators should agree a configuration which balances the business requirements, usability and security of the platform and use this guidance for advice where needed.

2. Risk owners' summary

When using Windows Phone 8.1 as part of a remote working scenario, the following architectural choices are recommended to minimise risk:

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

When configured in this way, risk owners should be aware of the following technical risks associated with this platform. These technical risks are associated to one of the 12 security principles for end user devices.

Associated security principle	Explanation of risks
Data in transit	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 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.
Data at rest	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.
Device update policy	Users can choose not to apply device updates that have not been marked as critical, this may lead to security issues not being patched.
Event collection for enterprise analysis	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. Administrators' deployment guide

To meet the principles outlined in the End User Devices Security Framework, several recommendations are given in the table below.

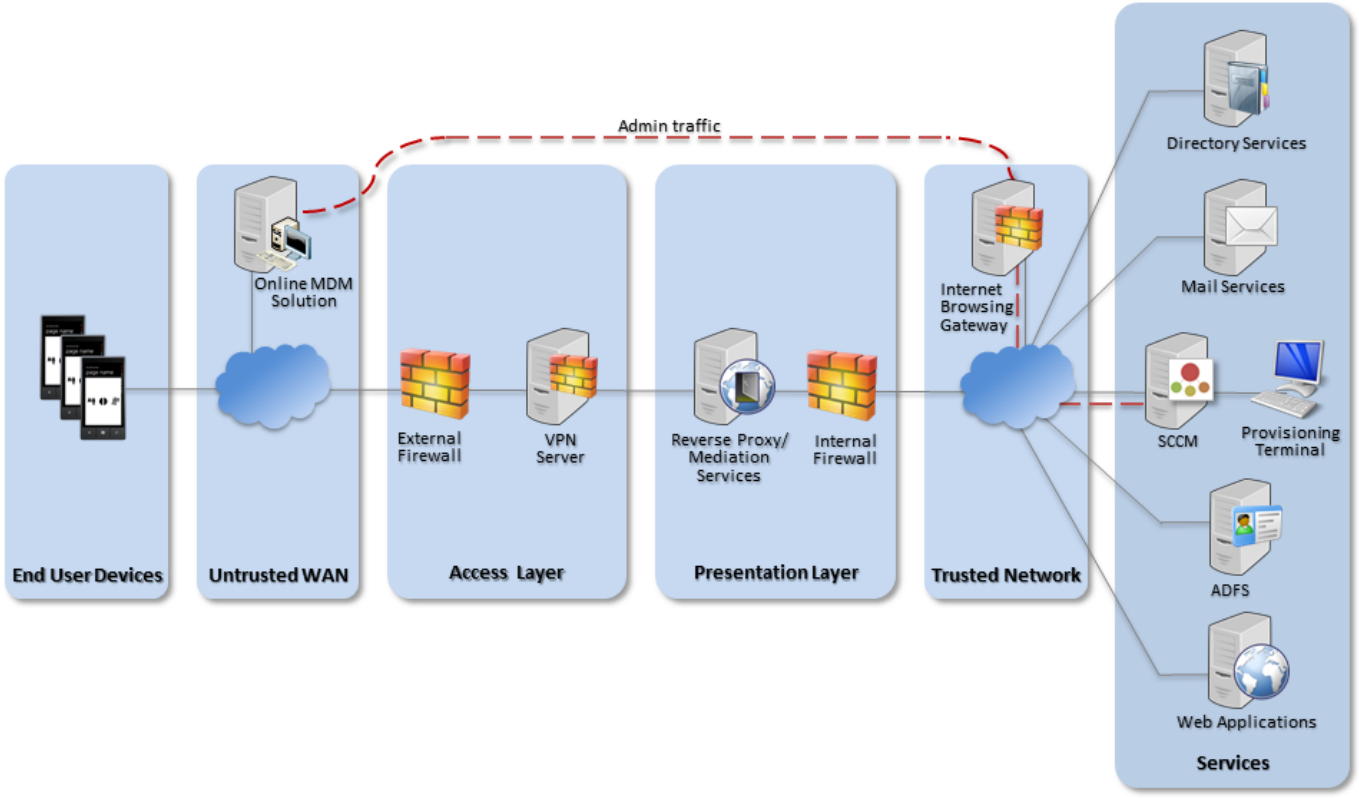
3.1 Overview

Security Principle	Explanation
Data in transit	Use the native IPsec VPN client, with AlwaysOn and DisableManualConfiguration settings. If a Foundation Grade assured VPN client for this platform becomes available, then this assured client should be used instead.
Data at rest	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. Email data can be protected whilst the screen is locked. Disable removable storage as non-application data stored on it is not encrypted.
Authentication	Use a strong 9-character password to authenticate the user to the device. This password unlocks a key which encrypts certificates and other credentials, giving access to enterprise services.
Secure boot	This requirement is met by the platform without additional configuration.
Platform integrity and application sandboxing	This requirement is met by the platform without additional configuration.
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.
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.
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.
External interface protection	Wi-Fi, NFC, Bluetooth, removable storage and USB Sync can all be disabled.
Device updates	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.

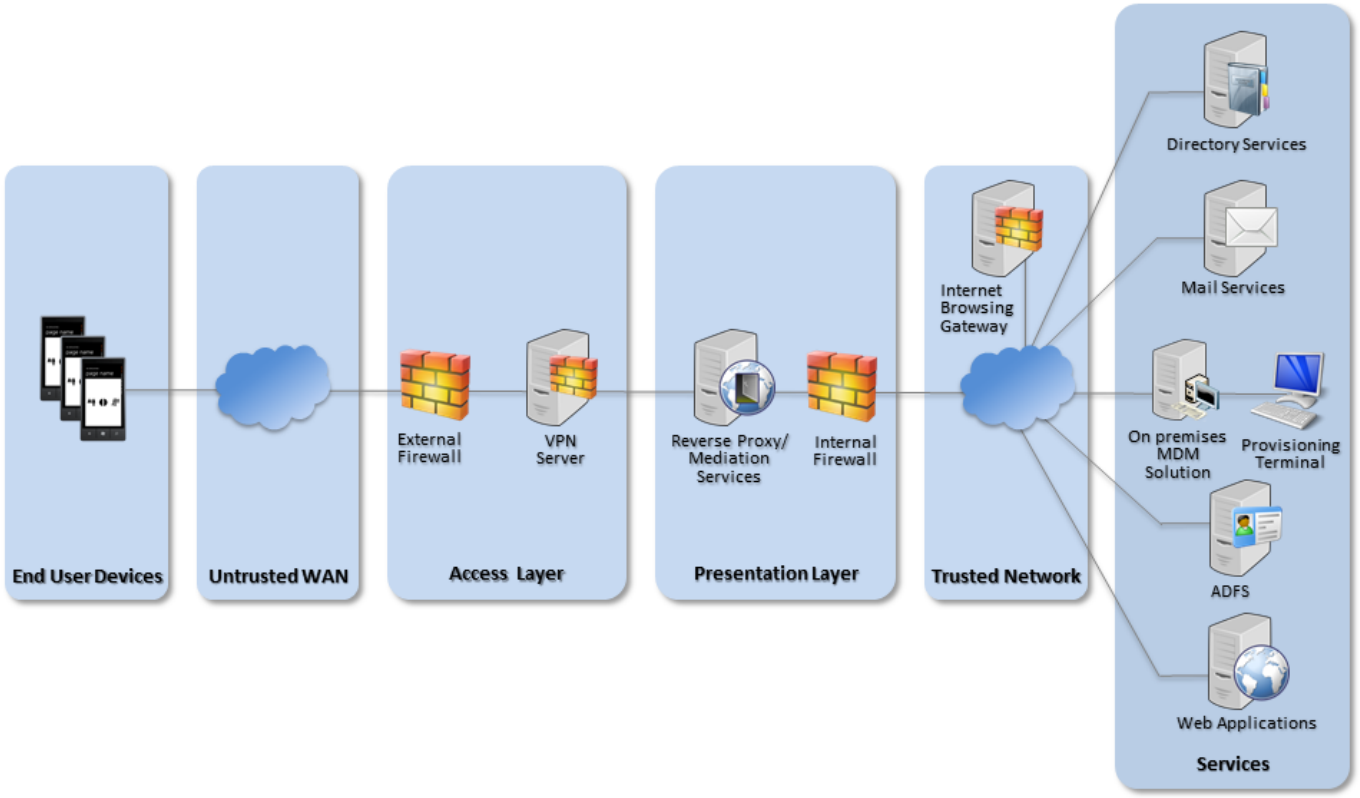
Event collection	There is no facility for collecting logs remotely from a device, and collecting forensic log information from a device is very difficult.
Incident response	Windows Phone 8.1 devices can be locked, wiped, and configured remotely by MDM. In the event of a compromised device, a full device 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.

3.2 Recommended network architecture

The diagrams below show recommended ways of integrating Windows Phone devices and server components into an organisation's walled garden network architecture.



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

3.3 Preparation for deployment

To prepare the enterprise infrastructure:

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).

3.4 Device provisioning steps

To provision each device to the enterprise infrastructure:

1. Assign the policies to users and devices using the MDM management interface
2. Add the mobile user into the MDM and assign the required access groups. If using Intune this can be done via Azure Active Directory sync (AAD sync), configuring it to federate identity rather than synchronising passwords to the cloud.
3. Load the enterprise CA certificate and the user's SSL client certificate on the device. They should be stored in the machine store – in the TPM if available. Client certificates can be provisioned either by using a SCEP profile or directly from the provisioning terminal.
4. Supply the device to the user. After the user follows the enrolment steps, they can install the company portal app by downloading it from the company store or via the workplace join setting.

4. Recommended policies and settings

The following table shows a recommended set of policies that will result in a reasonable balance between technical risk and usability. Organisations are encouraged to adjust these policies in consultation with their risk owners to maximise these devices' business benefit whilst still ensuring that each of the twelve security principles are addressed. For full details of what each policy controls, see the platform vendor's documentation.

Settings not listed in this section are either not applicable to this mode or should be chosen according to organisational policy and requirements.

Password section

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	10
Minutes of inactivity before screen turns off	5
Password complexity	Strong

Require password type	Alphanumeric
Minimum number of character sets	3
Allow simple passwords	No
Accounts and Synchronization section	
Allow Microsoft account	Disabled
Email section	
Allow non-Microsoft account	Disabled
Encryption section	
Require encryption on mobile device	Yes
Hardware section	
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)	
VPN//Policies/ConnectionType	AlwaysOn
Connectivity/AllowManualVPNConfiguration	0
DataProtection/RequireProtectionUnderLockConfig	1
Security/AllowManualRootCertificateInstallation	0
ApplicationManagement/ApplicationRestrictions	[Permitted app whitelist]
ApplicationManagement/AllowDeveloperUnlock	0
Search/AllowStoringImagesFromVisionSearch	0
Experience/AllowManualMDMUnenrollment	0
Experience/AllowSyncMySettings	0
System/AllowTelemetry	0
Enterprise Owned devices	

System/AllowUserToResetPhone	0

4.1 VPN profile

A VPN profile should be configured 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.

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

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.

5. Enterprise considerations

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

5.1 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.

5.2 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.

5.3 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.

5.4 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.

6. Change history

6.1 September 2015

Windows Phone 8.1 Update 2 introduced some updates that have security implications, including changes to the VPN that allow it to be locked into an always-on mode. This has mitigated the previous residual risk that “The VPN can be disabled by the user”. This risk has been removed from the guidance.

In addition the platform features an update to e-mail protection ensuring that they are encrypted when the phone is locked. The password requirements have been altered to reflect updated password guidance.

New settings

Setting	Configuration
VPN/Policies/ConnectionType	AlwaysOn
Connectivity/AllowManualVPNConfiguration	0
DataProtection/RequireProtectionUnderLockConfig	1

Settings that have a different configuration

Setting	Previous configuration	Updated configuration
Number of repeated sign-in failures to allow before the device is wiped	5	10

Settings that have been removed

Setting	Configuration
DeviceLock /DevicePasswordExpiration	90

Legal information