Guidance

End User Devices Security Guidance: Windows Phone 8

Updated 14 October 2013

Contents

This guidance is applicable to devices running Windows Phone 8. This guidance was developed following testing performed on Nokia Lumia 820 (Windows Phone 8.0.10211.204), Nokia Lumia 620 (Windows Phone 8.0.102.11.204) and HTC 8X (Windows Phone 8.0.9903.10).

1. Usage Scenario

Windows Phone 8 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:

- As the device does not have a VPN, application level SSL connections are used to manage data transit back to the enterprise.
- Arbitrary third-party application installation by users is not permitted on the device. Procedural measures are in place to enable users to install trusted applications as approved and monitored by the enterprise.

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 Best Satisfy the Security Recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	[!] There is no VPN capability in Windows Phone 8. Per application SSL connections are required to manage data in transit.
2. Assured data-at-rest protection	Windows Phone 8 device encryption has not been independently assured to Foundation Grade. [!] It is not possible to set a passphrase to unlock the encryption key. Encryption keys protecting sensitive data remain in device memory when the device is locked.
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	The enterprise cannot prevent users from installing arbitrary applications from the Windows Store.
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	Interfaces such as Wi-Fi, and Bluetooth cannot be controlled by policy.
10. Device update policy	The enterprise cannot force the user to update Windows Store applications
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.
12. Incident response	

2.1 Significant Risks

The following significant risks have been identified:

- Windows Phone 8 does not support connection to a VPN and is thus unable to meet a number of the mandatory requirements for an assured VPN. There is therefore no ability to ensure all network traffic is returned to the enterprise network.
- The Device Encryption capability in Windows Phone has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products.
- It is not possible to set a passphrase to unlock the disk encryption key.
- The enterprise cannot prevent users from installing arbitrary applications from the Windows Store. A malicious or vulnerable application could exfiltrate or leak sensitive data from the device.
- For Windows Store Applications, there is a reliance on the user performing application updates as there are no centrally configured methods that allow enterprises to force updates to those applications. This may result in applications becoming outdated and exploitable by an attacker who could compromise data. Windows Phone 8 cannot be updated by an administrator using Windows Server Update Services.
- There is currently no mechanism which allows Windows Phone 8 devices to send logs to enterprise servers using native functionality, either via Exchange ActiveSync or Windows InTune. Therefore the ability for event collection for enterprise analysis is severely limited.
- There are no policy controls available to restrict the external interfaces a user can enable, meaning that external interfaces may be accidentally or deliberately enabled by the end-user. Enabling external interfaces means additional attack surface could be exposed and data could be inadvertently or maliciously leaked without enterprise visibility.
- Management of Windows Phone 8 devices via InTune is intrinsically dependent on Microsoft's online services. Trust in Microsoft's online services is essential for enterprise deployments of Windows Phone 8 devices.

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

There is no VPN capability in Windows Phone 8. Per application SSL connections are required to manage data in transit.

3.2 Assured data-at-rest protection

Device Encryption is used to provide full volume encryption. There is no password provided to decrypt the disk each boot.

3.3 Authentication

Use Device Encryption to provide full volume encryption. There is no password provided to decrypt the disk each boot.

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. Beyond that there is no mechanism to whitelist applications on Windows Phone devices.

3.7 Malicious code detection and prevention

There is no ability to detect known malicious code on this platform. Content-based attacks can be filtered by scanning capabilities in the enterprise.

Mechanisms in the Windows Store attempt to detect and remove malicious code, thereby providing mitigation to help prevent malicious applications being installed on devices via the store.

3.8 Security policy enforcement

Settings applied through InTune (or other MDM) cannot be modified by the user.

3.9 External interface protection

No technical controls exist to prevent users from enabling Wi-Fi, NFC and Bluetooth.

3.10 Device update policy

The enterprise cannot control when the Windows Store applications are updated. These updates rely on user interaction.

3.11 Event collection for enterprise analysis

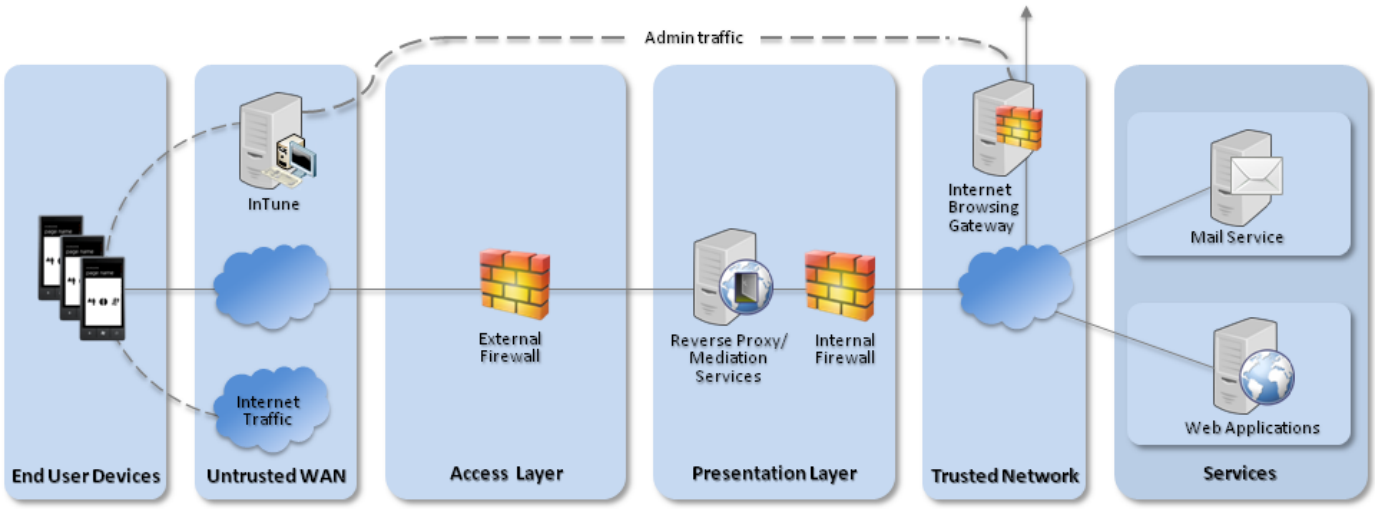
There is no facility for collecting logs remotely from a device, and collecting forensic log information from a device is very difficult.

3.12 Incident response

Windows Phone 8 devices can be locked, wiped, and configured remotely by InTune.

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 diagram describes the recommended architecture for this platform.



Recommended network architecture forWindows Phone 8 deployments

5. Deployment Process

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

1. Procure and provision an APN (Access Point Name) from a chosen mobile operator, obtaining SIM cards from

the carrier that are exclusively provisioned to use the procured APN for their cellular data connection.

2. Deploy SCCM with Windows InTune Connector onto a dedicated mobile device management terminal for Windows InTune in the Unified Configuration, or alternatively manage devices via Windows InTune in a cloud configuration or another MDM solution supporting the required settings.
3. Deploy a Company Portal app signed with a code-signing certificate to Windows InTune
4. Procure, deploy and configure other network components.
5. Set up the configuration profiles for the end-user devices in accordance with the settings later in this guidance.

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:

1. Load the following certificates into the machine store on the device, using the provisioning terminal:
    1. Enterprise CA certificate (used to validate the server certificates presented by the Exchange server and reverse proxy),
    2. SSL client certificate (for authentication to the reverse proxy for intranet services)
2. Using either the unified configuration or the cloud configuration apply these profiles to provisioned devices.
3. Provision the Windows Phone 8 device via the Company Apps option within the device settings, choosing ‘Add account’, entering the company credentials, then installing the Company Portal app.
4. Install apps required for enterprise productivity and uninstall any applications pre-loaded by the manufacturer of the device that are not required.
5. Connect device to Exchange account.
6. Configure on device security settings as the local user using the settings as described in the configuration section.

7. Policy Recommendations

7.1 Windows InTune (or other MDM)

The following table outlines the recommended policy settings when using Windows InTune (or other MDM).

Configuration Rule	Configuration Setting
Password	
Require a password to unlock mobile devices	Yes
Require Password Type	Alphanumeric

Minimum Number of Character Sets	3
Minimum Password Length	9
Allow Simple Passwords	No
Number of Repeated Sign-in Failures Before the Device is Wiped	5
Minutes of Inactivity Before Device Screen is Locked	1
Password Expiration	90
Remember Password History	Yes
Prevent Reuse of Previous Passwords	8
Exchange ActiveSync	
Allow Mobile Devices That Don't Fully Support These Settings to Synchronise with exchange	No
Encryption	
Require Encryption on Storage Devices (Not supported on WP8 devices, if this is not set to No the device will not sync)	Yes

7.2 Exchange ActiveSync

The following table outlines the recommended policy settings when using Exchange ActiveSync. Only the 'General' and 'Password' tabs apply to Windows Phone 8 devices; all other tabs should be left with their defaults or else the device will not synchronise as it contravenes the "Allow Non-Provisionable Devices" rule.

Configuration Rule	**Configuration Setting**
General	
Allow Non-Provisionable Devices	False
Refresh Interval (Hours)	24
Password	
Require Password	True
Require Alphanumeric Password	True
Minimal Number of Character Sets	3
Enable Password Recovery	No

Require Encryption on Device	Yes
Require Encryption on Storage Card (Not supported on WP8 devices, if this is not set to No the device will not sync)	No
Allow Simple Password	No
Number of Failed Attempts Allowed	5
Minimum Password Length	9
Time Without User Input before Password Must Be Re-Entered (In Minutes)	1
Password Expiration (days)	90
Enforce Password History	8

7.3 Local Policy User Settings

The following changes need to be made to the local user using PC settings options.

Local Policy	Value
Wi-Fi should be turned off unless needed by going to Settings > Wi-Fi	Off
Bluetooth should be turned off unless needed by going to Settings > Bluetooth	Off

8. Enterprise Considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for Windows Phone 8 deployments.

8.1 SkyDrive

SkyDrive is incorporated into many applications available for use by the Windows Phone 8 device such as Microsoft Office 2013. Procedural controls are necessary to prevent users from authenticating to SkyDrive and storing sensitive files within the Microsoft cloud.

For the Mail, Contacts and Store applications to work, a user must authenticate to these apps using a Microsoft account.

8.2 Windows InTune Cloud

When provisioning Windows Phone 8 devices with Windows InTune cloud service this moves the control of the devices to a cloud service. This may add additional risks to a deployment from the use of this cloud service.

Legal Information