Guidance

End User Devices Security Guidance: Windows 8 RT

Updated 14 October 2013

Contents

This guidance is applicable to devices running Windows 8 RT. Windows RT implements a different set of features to the Enterprise edition of Windows 8 and so is considered separately. This guidance was developed following testing performed on Microsoft Surface tablets.

1. Usage Scenario

Windows RT devices will be used remotely over Wi-Fi and 3G to connect back to the enterprise over a VPN. This enables a variety of remote working approaches such as

- accessing OFFICIAL email;
- creating, editing, 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 benefit from enterprise protective monitoring solutions.
- 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	The VPN can be disabled by the user and does not initiate automatically at boot. The Windows 8 IPsec VPN has been independently evaluated against the VPN Security Requirements.
2. Assured data-at-rest protection	Windows 8 RT 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 USB, 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	
12. Incident response	

2.1 Significant Risks:

The following significant risks have been identified:

- The VPN does not initiate automatically at boot, there is potential for the user to disable this at any time.
- Windows 8 RT Device Encryption has not been independently assured to Foundation Grade, and in Windows 8 RT does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance in the device encryption 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 and the recovery key is automatically stored on SkyDrive (but should be removed).
- 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 RT cannot be updated by using Windows Server Update Services.
- 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 RT devices via InTune is intrinsically dependent on Microsoft's online services. Trust in Microsoft's online services is essential for enterprise deployments of Windows RT 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

Use the native IPsec VPN client.

3.2 Assured data-at-rest protection

Use Windows 8 RT Device Encryption to provide full volume encryption. There is no password provided to decrypt the disk each boot.

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

3.7 Malicious code detection and prevention

Defender provides the ability to detect known malicious code for this platform. Content-based attacks can be filtered by scanning capabilities in the enterprise.

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 and Bluetooth, or using USB.

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

Event collection can be carried out using Windows Event Forwarding for central event log collection.

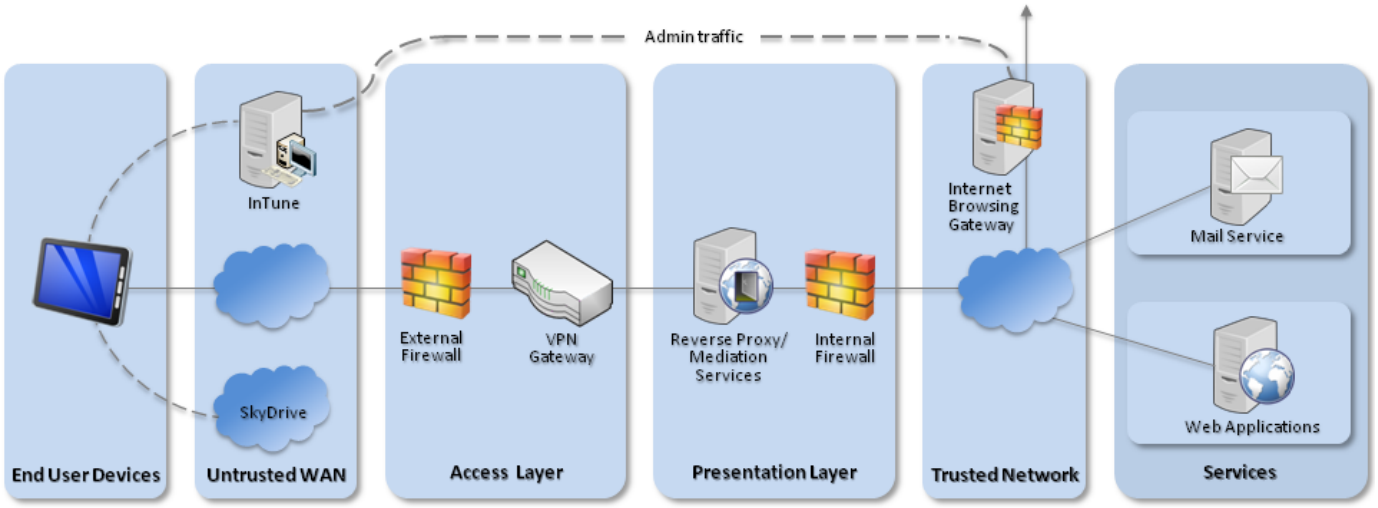
3.12 Incident response

Windows RT does not natively support remote wipe, however the combination of full disk encryption and

enterprise control of user credentials can be used to manage this security recommendation.

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 architecture for Windows 8 RT deployments

5. Deployment Process

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

1. 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 supporting the required settings.
2. Procure, deploy and configure other network components, including an approved IPsec VPN Gateway.
3. Set up the configuration profiles for the end-user devices in accordance with the settings later in this chapter.

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 VPN endpoint and reverse proxy),
    2. VPN client certificate (for authentication to the enterprise VPN endpoint),
    3. SSL client certificate (for authentication to the reverse proxy for intranet services)
2. Configure on-device security settings as a local administrator using local policy as described in the configuration section.
3. Configure the local administrator account to be a Microsoft account to turn the device encryption on.
4. Store the recovery key in a safe place and then log onto SkyDrive and remove the recovery key from there.
5. Disassociate the local administrator account from the Microsoft account.
6. Create a local user account and log onto the device as the account.
7. Configure the VPN client to connect to the enterprise VPN endpoint using the device-specific client certificate that has been loaded onto the device.
8. Enrol the device into Windows InTune.
9. (OPTIONAL) Deploy a Company Portal app signed with a code-signing certificate to Windows InTune
10. Install applications required for enterprise productivity and uninstall any applications pre-loaded by the manufacturer of the device that are not required.
11. 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 for 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
Windows RT	
Allow Picture Password and Pin	No
Exchange ActiveSync	
Allow Mobile Devices That Don't Fully Support These Settings to Synchronise with Exchange	No
Encryption	
Require Encryption on Storage Devices	Yes

7.2 Exchange ActiveSync

The following table outlines the recommended policy settings for Exchange ActiveSync. Only the General and Password tabs apply to Windows 8 RT devices, all other tabs should be left with their defaults 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	No (Not supported on RT devices, if this is set to Yes then the device will not sync)
Allow Simple Password	No
Number of Failed Attempts Allowed	5
Minimum Password Length	10
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 Computer Settings

The following changes need to be made to the device as a local administrator account using Local policy editor.

Local Policy	**Value**
Computer Configuration > Administrative Templates > System > Removable Storage Access > Set All Removable Storage Classes	Enabled
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Enforce Password History	8
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Maximum Password Age	90
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum Password Age	3
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum Password Length	10
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Password Must Meet Complexity Requirements	Enabled
Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Store Passwords Using Reversible Encryption	Disabled
Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy > Account Lockout Duration	30 Minutes
Computer Configuration > Windows Settings > Security Settings > Account Policies >	5 invalid logon attempts

Account Lockout Threshold	
Computer Configuration > Windows Settings > Security Settings > Account Policies > Reset Account Lockout Counter after	30 minutes
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Accounts: Block Microsoft Accounts	Users can't add Microsoft Accounts
Computer Configuration > Administrative Templates > Network > Network Isolation > Intranet Proxy Servers for Apps	Enabled, Configure with Reverse Proxy Address

7.4 Local Policy User Settings

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

Local Policy	**Value**
PC Settings > Personalise > Lock Screen Apps	Unselect Mail and Calendar
PC Settings > Users > Sign-In Options	Always Require a Password
PC Settings > Wireless > Bluetooth	Off
PC Settings > Privacy	Turn all off
Control Panel > All Control Panel Items > Action Center > Change Action Center Settings > Customer Experience Improvement Programme Settings	No, I don't want to participate in the program

7.5 VPN Profile

The deployed VPN solution should be configured to negotiate the following parameters.

Setting	**Value**
IKE DH Group	2 (1024-bit)
IKE Encryption Algorithm	AES-128
IKE Hash Algorithm	SHA-1
IKE Authentication Method	RSA X.509
IPsec Encryption	AES-128

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 RT deployments.

8.1 SkyDrive

SkyDrive is incorporated into many applications available for use by the Windows 8 RT 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, People and Store applications to work, a user must authenticate to these apps using a Microsoft account.

Legal Information