MICROSOFT (MS) WINDOWS 10 MOBILE SUPPLEMENTAL PROCEDURES

Version 1, Release 3

27 October 2017

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a Windows 10 Mobile assessment, the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with Windows 10 Mobile, its associated network infrastructure, and the individual devices composing the system.

1.2 Mobile Policy Review

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website at:

http://iase.disa.mil/stigs/mobility/Pages/policies.aspx

Use the Mobility Policy Security Technical Implementation Guide (STIG) and the CMD Policy STIG to review the Smartphone Handheld asset.

2. WINDOWS 10 MOBILE IMPLEMENTATION CONSIDERATIONS

2.1 Windows 10 Mobile Device Disposal

For Windows 10 Mobile devices never exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures:

Note: Follow device manufacturer's instructions for wiping all user data and installed applications from device memory.

2.2 Enforcing Copy and Paste Policies with Windows Information Protection

A new data protection feature in the Windows 10 Mobile 1607 (August 2016) update provides advanced data loss protection capabilities. This feature is called Windows Information Protection (WIP).

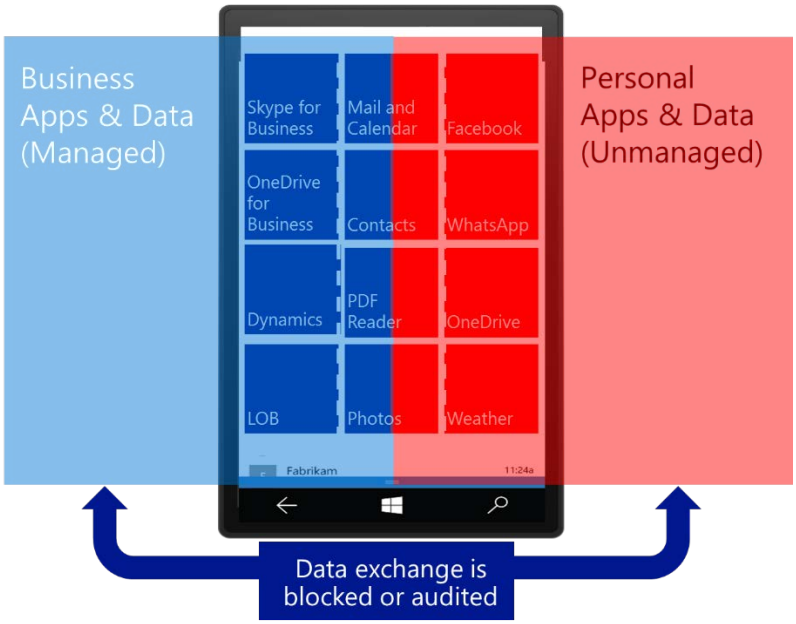
WIP protects data at rest where it rests on the device. It is seamlessly integrated into the platform so no mode switching is necessary between the operating system and an enterprise container. This also allows any application to be used without requiring a specialized application. Enterprise/DoD data is identifiable from personal data wherever it rests on the device. Also, unauthorized apps are prevented from accessing business data. DoD Command/Department/ Agency IT administrators have full control of keys and data and can remote wipe/revoke data on demand by revoking the key.

Note: Windows Information Protection solves previous concerns with saving/copying/synching DoD data to public/cloud network destinations such as OneDrive. This is one of the core design goals for this data protection technology.

Benefits of WIP include:

- Obvious separation between personal and DoD data, without requiring employees to switch environments or apps
- Additional data protection for existing line-of-business apps without a need to update the apps
- Ability to wipe corporate data from devices while leaving personal data alone
- Use of audit reports for tracking issues and remedial actions
- Integration with your existing management system (Microsoft Intune, System Center Configuration Manager, or your current mobile device management [MDM] system) to configure, deploy, and manage WIP for your company

Figure 2-1: WIP Data Protection Diagram



Two key policy controls govern the control of data:

1. **Network policies** – With network policies, DoD network spaces can be defined. By listing enterprise domain names, IP address ranges, proxy server lists, and public/cloud domain names, a map of network space can be defined to control encryption of any data stored on a mobile device that comes from those locations as well as to control the ability to copy or paste data from those DoD enterprise locations to a non-trusted location.

2. **Application policies** – These polices enable a list of managed applications to be defined. Applications in this list become authorized to access DoD data, and data that is saved from these applications is also encrypted automatically. Copy/paste of information from managed applications is also controlled so it can be blocked if required.

3. **Data protection mode policy** – Once the network and application policies are defined, allowable actions can be specified that governs data. Those options are:

    a. **Block** – WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This can include sharing information across non-enterprise-protected apps in addition to sharing enterprise data among other people and devices outside of your enterprise. This is the setting recommended for use within DoD, described in MSWM-10-911101.
    b. **Override** – WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log.

c. **Silent** – WIP runs silently, logging inappropriate data sharing without blocking anything that would have been prompted for employee interaction while in Override mode. Unallowed actions, such as apps inappropriately trying to access a network resource or WIP-protected data, are still blocked.
d. **Off** – WIP is turned off and does not help to protect or audit your data.
e. After you turn off WIP, an attempt is made to decrypt any closed WIP-tagged files on the locally attached drives. THIS SETTING IS NOT RECOMMENDED.

A detailed introduction to WIP in Windows 10 can be found here:
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/protect-enterprise-data-using-wip

Guidance on Creating a WIP Configuration

In the validation procedure section for MSWM-10-911101, policies are listed that describe the combination of configuration settings required to implement a complete Windows Information Protection policy.

Here are further details on that procedure. These represent the minimum number of configuration settings required:

1. **Choose Enterprise Managed Applications** – Under Windows 10 Mobile, the only applications supported are called Store Apps. If an application should be granted permissions to access DoD data, it should be included in this list.

2. **Define DoD Network Protected Space** – As described earlier, WIP needs to understand your network topology so that it can automatically determine what data should be encrypted and protected from being moved or copied to untrusted locations. Here are the specific network categories that need to be included in the policy:

   a. **Enterprise IP Ranges** – This configuration is used to list IPv4 and/or IPv6 address ranges for protected DoD network space. If data is copied/saved/synched from a DoD server within those ranges, that data is automatically encrypted. If data is attempted to be moved, copied, saved, or synched from a source in those ranges to a non-trusted destination outside that list, it can be blocked (i.e., twitter.com, onedrive.live.com).

   An example list is shown below:

```
10.0.0.0-10.255.255.255,157.54.0.0-157.54.255.255,
192.168.0.0-192.168.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff,
2001:4898:dc05::-2001:4898:dc05:ffff:ffff:ffff:ffff:ffff,
2a01:110::-2a01:110:7fff:ffff:ffff:ffff:ffff:ffff,
fd00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

   Note: Both IPv4 and IPv6 addresses do not need to be listed, but you need to include at least one of those address range types.

b. **Enterprise Protected Domain Names** – In this setting, protected domain names for your primary Command/Department/Agency networks are defined.

The first domain needs to be your primary identity, which corresponds to the top-level domain name for your organization. Examples could be: **disa.mil**, **army.mil** etc.

That domain name is then followed by other domains used for services like email, such as: **mail.mil**.

You can specify multiple domains owned by your Command/Department/Agency by separating them with the "|" character. With multiple domains, the first one is the one designated as your corporate identity, with all the additional ones being owned by the first one, for example, (disa.mil|mail.mil).

c. **Enterprise Network Domain Names** – This is the list of domains that compose the boundaries of the enterprise or essentially domains the computers use within your enterprise. Data from one of these domains that is sent to a device will be considered enterprise data and protected. These locations will be considered a safe destination for enterprise data to be shared to. This is a comma-separated list of domains, for example “contoso.sharepoint.com, fabrikam.com”.

Note: To be a considered a managed domain, IP addresses need to be bound to a particular domain and therefore must be included in the Enterprise IP Ranges policy.

3. **Protection Mode** – This policy is introduced earlier and shown to be configured with the **Block** setting:

a. Block – WIP looks for inappropriate data-sharing practices and stops the user from completing the action. This can include sharing information across non-enterprise-protected apps in addition to sharing enterprise data among other people and devices outside of your enterprise. This is the setting recommended for use within DoD, described in MSWM-10-911101, and with it prevents pasting/copying/synching data to non-trusted DoD network locations.

Note: While the default recommendation is to block all data from going to untrusted destinations, there may be scenarios where DoD personnel in their role need to share information in trusted locations. An example of that might be someone in a public relations role who might need to post a message to a sanctioned Twitter account. In those cases, defined users with those needs can be configured with the **Override** policy. In that situation, they would first be warned with a pop-up message that they are taking a potentially unsafe data protection action. They can acknowledge the warning and proceed and that data will be shared, but the action will be noted in the audit log.

4. **User Decryption** – This WIP policy setting should be set to “off/false/unchecked” so users cannot remove decryption from files previously encrypted. In a BYOD scenario, this is more typical if you give the users the trust to remove encryption from selected files

retrieved from protected network sources, but to block data leakage, this setting is required to be off.

Note: Be aware that when choosing this option, apps that use the Save As dialog box might encrypt new files as DoD data unless a different file save path is given during the original file creation. After this happens, decryption of work files becomes more difficult.

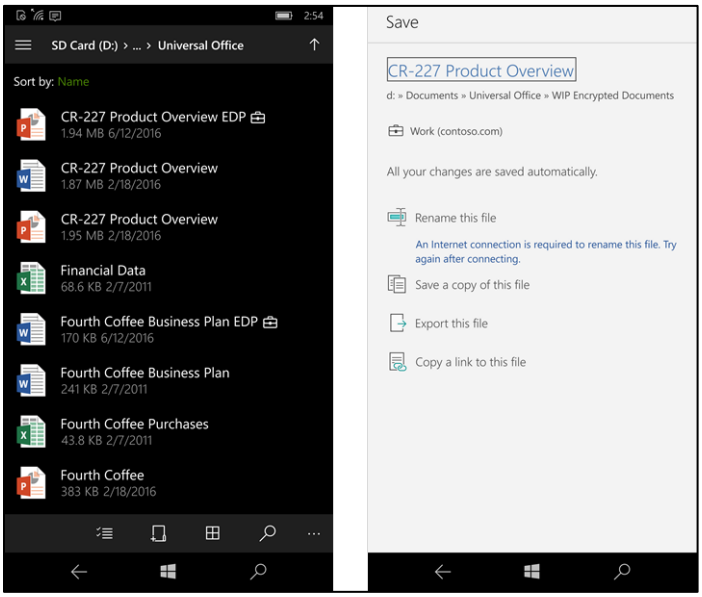
5. **Revoke encryption keys on unenroll** – This WIP policy setting should be enforced (if available) by setting it to "on/true/checked" to prevent encryption from being removed from files after MDM unenrollment. By revoking the keys if a device is unenrolled or removed from WIP, files previously encrypted will remain encrypted but will be inaccessible.

6. **Prevent corporate data from being accessed by apps when the device is locked** – Also known as protection under PIN lock, this policy should be enforced by setting it to "on/true/checked". When used, this policy encrypts local DoD data using a key that is protected by a user's PIN code on a locked device. Apps will not be able to read enterprise data when the device is locked.

   Note: Even though the key is thrown away when the device is locked, it is still possible to receive email, and when the device is unlocked, the key is recreated and access to protected data is restored.

7. **Show the WIP icon overlay** – While this is an optional policy setting under MSWM-10-911101, if this setting is set to "on/true/checked", a WIP icon overlay that looks like a briefcase appears next to files in File Manager as well as on Save As dialogs. This is a valuable visual indicator to identify encryption of files. Examples are shown in the screenshots below:

Figure 2-2: WIP Icon Overlay



8. **Data Recovery Agent (DRA) Certificate** – After you create and deploy your WIP policy to your users, Windows will begin to encrypt DoD sourced data on users' local device storage. If somehow the users' local encryption keys are lost or revoked, the encrypted data can become unrecoverable. To help avoid this possibility, the DRA certificate lets Windows use an included public key to encrypt the local data, while your IT group in your Command/Department/Agency can maintain the private key that can unencrypt the data.

   Note: On a Windows 10 Mobile, there is no native capability to recover encrypted data stored in main device storage. Only if encrypted files were copied to a desktop via a USB connection or stored on a removable storage drive mounted on a desktop could a recovery be done leveraging the DRA certificate; however, both of those data connection methods are prohibited in the Windows 10 Mobile STIG.

   a. **Instructions for creating your DRA recovery certificate** – For more information about how to find and export your data recovery certificate, see the Data Recovery and Encrypting File System (EFS) topic: https://technet.microsoft.com/en-us/library/cc512680.aspx

      For more information about creating and verifying your EFS DRA certificate, see the Create and Verify an EFS DRA certificate article: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-and-verify-an-efs-dra-certificate

   b. In the WIP policy setting for a data recovery certificate, use the Browse (or equivalent) button to Upload a DRA certificate created with the procedures above to allow recovery of encrypted data box.

Final Note: Several MDMs support the WIP policy today in their admin consoles, including AirWatch (8.3.1.0 or higher), MobileIron (Core 9.1.0.0 Build 1723 or higher) and Microsoft Intune. While Intune is not an approved MDM within DoD, instructions for creating a WIP policy can be found at this link: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-intune

2.3 Onboard Trusted Platform Module (TPM)

Windows 10 Mobile devices include TPM 2.0, which is implemented in firmware on the Qualcomm processor. TPM is used for cryptographic operations such as managing BitLocker encryption of data at rest on main storage. Keys and certificates can be protected by TPM as well as PIN protected to enable two-factor authentication for things like derived credentials.

2.4 Windows 10 Mobile Enterprise Edition

As sold at retail, Windows 10 Mobile is the shipping edition of Windows 10 Mobile. While the majority of enterprise features are built into the core edition of Windows 10 Mobile, there are additional controls that can be employed if using the Windows 10 Mobile Enterprise edition.

This parallels additional capabilities found in Windows 10 Enterprise versus Windows 10 Professional on the desktop.

Three STIG requirements (MSWM-10-201901, MSWM-10-501706, and MSWM-10-912419) leverage Windows 10 Mobile Enterprise edition and require it to achieve the maximum control. For DoD customers with a Software Assurance (SA) plan for Windows 10 Enterprise edition, the SA plan includes rights for Windows 10 Mobile Enterprise. The license needed to upgrade Windows 10 Mobile devices to Windows 10 Mobile Enterprise can be found on the Microsoft Volume Licensing Service Center (VLSC).

Information on upgrade procedures can be found here:
https://technet.microsoft.com/itpro/windows/deploy/windows-10-edition-upgrades

2.5 Windows 10 Mobile Update Process

In enterprise IT environments, the desire to provide users with the latest technologies needs to be balanced with the need for manageability and cost control. In the past, many enterprises managed their Windows deployments homogeneously and performed large-scale upgrades to new releases of Windows (often in parallel with large-scale hardware upgrades) about every three to six years. Today, the rapid evolution of Windows as a platform is forcing Windows users to rethink their upgrade strategies, including keeping a significant portion of their enterprise's devices current with the latest release of Windows. Microsoft has created new ways to deliver and install feature upgrades and servicing updates that simplify deployments and ongoing management, broaden the base of employees who can be kept current with the latest Windows capabilities and experiences, and lower total cost of ownership. In addition, Microsoft has implemented new servicing options:

- Servicing options – referred to as Current Branch (CB), Current Branch for Business (CBB), and Long-Term Servicing Branch (LTSB) – provide pragmatic solutions to keep more devices more current in enterprise environments than was previously possible.

Within DoD, both Windows 10 and Windows 10 Mobile are being deployed using the CBB servicing model, which is new releases of Windows 10, fully patched and updated. In the past, operating system builds for phones after their release had to go through an additional testing period before approval and release by a mobile operator. With the new servicing model, Microsoft works with the original equipment manufacturers (OEMs) and mobile operators during the OS development process. Upon the release of a Windows 10 update, it is immediately available to all in-market Windows 10 desktops, and then after additional testing with mobile operators, Windows 10 Mobile is released to all phones directly from Microsoft update servers.

2.6 Windows Hello – Biometrics

MSWM-10-202801 provides a control that restricts the use of biometrics; however, Microsoft Lumia 950/950XL devices include a Windows 10 technology called Windows Hello that is native authentication supporting fingerprint, iris scanning, and facial recognition. Lumia 950 devices have iris scanners on board that allow the user to log on to their device. These

enrollments leverage a biometric template that is only locally stored and cryptographically bound to the device; it does not roam across the network. Currently, there are no released Windows 10 Mobile devices that support fingerprint authentication. All biometric sign-on options are backed by a PIN so that if the biometric input cannot be completed successfully, a PIN can always be used as a fallback.

In March 2015, the Information Assurance Directorate (IAD) released the unclassified technical brief "(U) Risk Discussion for Biometrics on Mobile Devices". The IAD technical brief provides information on criteria to use when performing a risk acceptance of a biometric authentication system for a mobile device and states, "The use of biometrics, prior to establishing requirements that can be used to validate implementations, creates a strategic risk that biometric templates could be harvested from weak implementations."

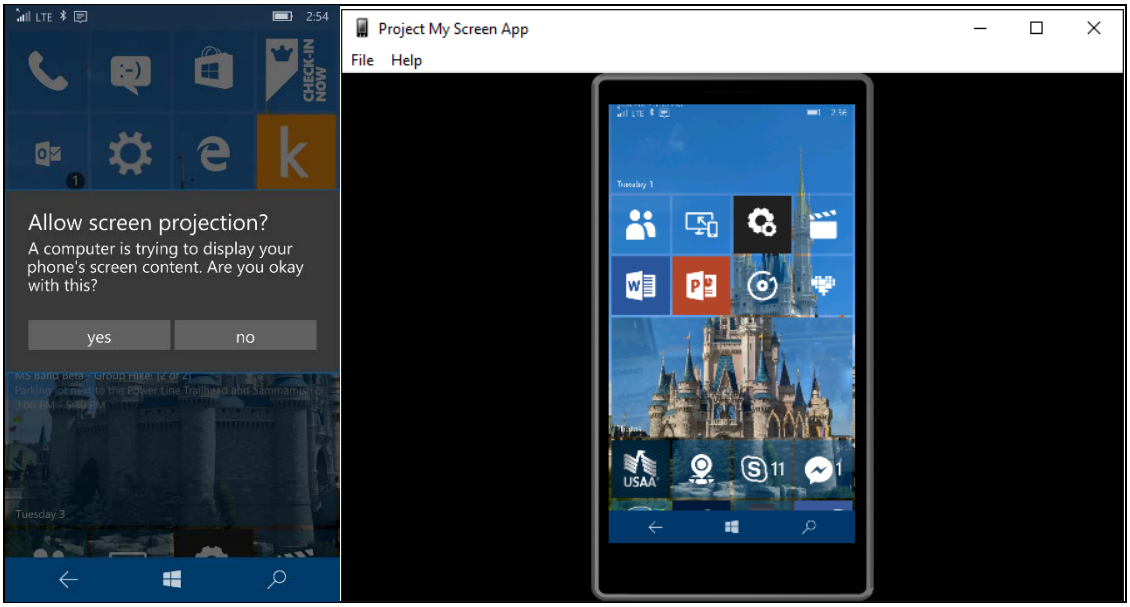
Version 3.0 of the Protection Profile for Mobile Device Fundamentals (PPMDF), to be released in 2016, includes new design requirements and assurance activities for fingerprint biometric authentication systems.

To date, no evaluation has been conducted on the biometric components of Windows 10 Mobile devices; therefore, any Authorizing Official (AO) implementing biometric authentication on Windows 10 Mobile devices is accepting an unknown risk.

2.7 Screen Mirroring

Miracast is a screen mirroring technology that allows a tablet or smartphone screen to be projected on a TV or monitor via a Wi-Fi connection to a wireless router. Windows 10 Mobile includes two types of screen mirroring solutions. The first is Project My Screen. This technology allows a Windows 10 Mobile phone to be connected via USB to a desktop and, once connected, if the companion Project My Screen desktop app is installed and run, an offer is presented on the phone to Allow Screen Projection:

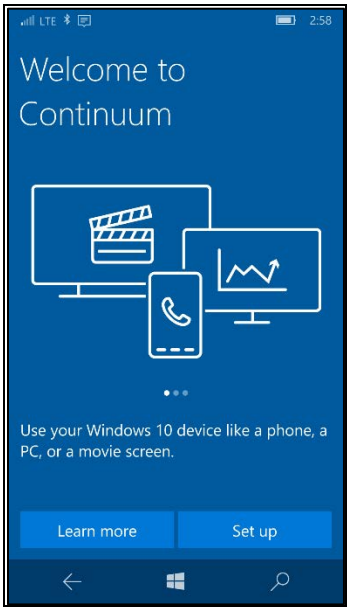
Figure 2-3: Screen Mirroring – Allow Screen Projection



If the "Allow screen projection" message "yes" button is selected, the phone's display shows up on the desktop.

The other option is using Continuum. This app ships with Windows 10 Mobile and offers the ability to wirelessly project the screen to an external monitor or through a display dock via a USB-C cable:

Figure 2-4: Continuum App with Windows 10 Mobile



Users should be trained to not use the wireless options unless using an approved DoD screen mirroring technology with FIPS 140-2 validated Wi-Fi. Continuum or Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2 validated Wi-Fi clients.

Screen mirroring via USB is disabled because the STIG requires device USB connections to be disabled (see requirements MSWM-10-200704 and MSWM-10-202608).

2.8 STIG Mapping for Rugged/Embedded Phones

This STIG targets Windows 10 Mobile, which is the standard Mobile Operating System (OS) shipping on Windows 10 phones. A number of rugged handheld phones are used for field force tasks using such capabilities as bar code or Radio-Frequency Identification (RFID) scanning. The most current versions of these devices are running Windows 10 Internet of Things (IoT) Mobile Enterprise. That OS is directly equivalent to Windows 10 Mobile Enterprise, which has additional recommended security controls (see STIG requirement MSWM-10-912419). Therefore, if rugged devices are used in DoD that come with Windows 10 IoT Mobile Enterprise, they can be considered comparable and acceptable for use within DoD.

3. CORE AND PREINSTALLED APPLICATIONS

3.1 Application Management on DoD Windows 10 Mobile Devices

Windows 10 Mobile supports the installation of applications from these three paths:

- Windows Store
- Private applications deployed by MDM
- Side-loaded applications available to developers over a local USB connection

The last option for developers is prohibited in the STIG (see requirement MSWM-10-200303).

DISA has not completed a risk assessment for obtaining apps directly from the Windows Store; therefore, the STIG blocks direct access (see requirement MSWM-10-200305). The only way applications (work and personal) can get onto a phone is either having been preinstalled or pushed down via an MDM.

If desired applications are already bundled with Windows 10 Mobiles devices as listed in Appendix A, no further steps are necessary to use them other than including them in the whitelist. However, if personally desirable applications need to be added to DoD-approved application catalogs, they can be downloaded or purchased from the Windows Store for Business.

With the Windows Store for Business, organizations can make volume purchases of Windows apps. The Store for Business provides app purchases based on organizational identity, flexible distribution options, and the ability to reclaim or reuse licenses. Organizations can also use the Store for Business to create a private store for their employees that includes apps from the store, as well as private Line-of-Business (LOB) apps. The following links provide documentation on these processes for MDM/app administrators:

Windows Store for Business overview

https://technet.microsoft.com/itpro/windows/whats-new/windows-store-for-business-overview

Distribute apps to your employees from the Windows Store for Business

https://technet.microsoft.com/itpro/windows/manage/distribute-apps-to-your-employees-windows-store-for-business

Sign up for Windows Store for Business

https://technet.microsoft.com/itpro/windows/manage/sign-up-windows-store-for-business

Microsoft recommends the DoD acquire applications available with offline licenses. Offline-licensed applications have these advantages:

- **Do not have access to Windows Store services** – If your employees do not have access to the Internet and Windows Store services, downloading offline-licensed apps and deploying them with imaging is an alternative to online-licensed apps.
- **Use imaging to manage devices in your organization** – Offline-licensed apps can be added to images and deployed with Deployment Image Servicing and Management (DISM) or Windows Imaging and Configuration Designer (ICD)
- **Employees do not have Azure Active Directory (AD) accounts** – Azure AD accounts are required for employees who install apps assigned to them from Store for Business or who claim apps from a private store.

3.2 Finding Application Product IDs for Use in Whitelists

Applications are listed in the application whitelist by Product IDs. If an application is not listed in Appendix A, its Product ID, for example, skype, can be obtained by following this procedure:

1. Go to this site to see the online catalog of phone apps in the Windows Store: https://www.microsoft.com/en-us/store/apps/windows-phone?icid=en_US_Store_UH_apps_WinPho
2. Search for the name of an application or browse through the categories on that page.
3. Type “skype” in the search box and click the search magnifying glass:

4. In the results, select the last link titled “Skype”.
5. Verify that you are on the right product and if not, go back to Step 3 and do another search.
6. Look at the URL in the address bar of your browser and copy that URL to Notepad or a similar editor. In this case, the URL is: https://www.microsoft.com/en-us/store/apps/skype/9wzdncrfj364
7. Note the store application ID at the very end of that URL, which is: **9wzdncrfj364**
8. Retrieve additional information for that application using the Windows Store for Business API; using that same text editor, copy and paste this URL into the editor: https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/APPID/applockerdata
9. Replace the APPID part of the URL with the store application ID — in this case Skype: https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/9wzdncrfj364/applockerdata
10. Copy that complete URL back to your browser and navigate to it.
11. Depending on your browser, a message similar to the following is presented:

12. Choose to save the .json file locally to your desktop and then open that up in a text editor:

    {

    "packageFamilyName": "Microsoft.SkypeApp_kzf8qxf38zg5c",

    "packageIdentityName": "Microsoft.SkypeApp",

    "windowsPhoneLegacyId": "**c3f8e570-68b3-4d6a-bdbb-c0a3f4360a51**",

    "publisherCertificateName": "CN=Skype Software Sarl, O=Microsoft Corporation, L=Luxembourg, S=Luxembourg, C=LU"

    }
13. Note the .Json file value of the “windowsPhoneLegacyId”, which is: **c3f8e570-68b3-4d6a-bdbb-c0a3f4360a51**
14. This product ID can now be shared with your MDM administrator to add to the whitelist of allowed applications.

3.3 Disabled Applications

Table A-1 lists core and preinstalled applications that are recommended to be disabled. Risk in using these apps in the DoD environment is considered to be high or not fully known, or the app provides a feature that is not considered useful in the DoD environment. AOs should fully vet these apps, using the Application Software Protection Profile (APPSWPP), prior to approving their use. These apps are disabled by not including them on the application whitelist.

3.4 Enabled Applications

Table A-2 lists core and preinstalled applications that are recommended for approval. AOs should consider vetting these apps using the APPSWPP. Approved apps should be included on the application whitelist.

APPENDIX A: APPLICATION LISTS

Table A-1: Applications Recommended for Disapproval

Application Package Name	Product ID	Application User Model ID (AUMID)
Contact Support	0DB5FCFF-4544-458A-B320-E352DFD9CA2B	Windows.ContactSupport_cw5n1h2txyewy!App
Cortana	FD68DCF4-166F-4C55-A4CA-348020F71B94	Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI
OneDrive	AD543082-80EC-45BB-AA02-FFE7F4182BA8	Microsoft.MicrosoftSkydrive_8wekyb3d8bbwe!App
OneNote	CA05B3AB-F157-450C-8C49-A1F127F5E71D	Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim
Wallet	587A4577-7868-4745-A29E-F996203F1462	Microsoft.MicrosoftWallet_8wekyb3d8bbwe!App
Windows Feedback	7604089D-D13F-4A2D-9998-33FC02B63CE3	Microsoft.WindowsFeedback_8wekyb3d8bbwe!App
Xbox	B806836F-EEBE-41C9-8669-19E243B81B83	Microsoft.XboxApp_8wekyb3d8bbwe!Microsoft.XboxApp
Amazon App	351DECC7-EA2F-E011-854C-00237DE2DB9E	
AT&T Address Book	F5374978-12F0-4637-9563-D80A08C5F113	
AT&T FamilyMap	6F3EDD9B-5CBC-DF11-9EAE-00237DE2DB9E	
AT&T Locker	4C158C11-0C27-4DEF-BA1F-83231A3E83D4	
AT&T Navigator	B2D00458-5FBC-DF11-9EAE-00237DE2DB9E	
AT&T Ready2Go	136196B3-E135-47F7-AD84-BF168DD04D0D	978F2567.ATTReady2Go_922x43c0p1h60!App

Application Package Name	Product ID	Application User Model ID (AUMID)
myAT&T	4CC12D74-5EBC-DF11-9EAE-00237DE2DB9E	
Mobile TV	7E7CC86E-E1C0-476A-AC88-DB3C9FFFFABB	
YPmobile	B46A3AF4-2AAE-E011-A53C-78E7D1FA76F8	

Table B-2: Applications Recommended for Approval

Application Package Name	Product ID	Application User Model ID (AUMID)
Alarms and Clock	44F7D2B4-553D-4BEC-A8B7-634CE897ED5F	Microsoft.WindowsAlarms_8wekyb3d8bbwe!App
Calculator	B58171C6-C70C-4266-A2E8-8F9C994F4456	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App
Camera	F0D8FEFD-31CD-43A1-A45A-D0276DB069F1	Microsoft.WindowsCamera_8wekyb3d8bbwe!App
Excel	EAD3E7C0-FAE6-4603-8699-6A448138F4DC	Microsoft.Office.Excel_8wekyb3d8bbwe!microsoft.excel
Facebook	82A23635-5BD9-DF11-A844-00237DE2DB9E	Microsoft.MSFacebook_8wekyb3d8bbwe!x82a236355bd9df11a84400237de2db9e
File Explorer	C5E2524A-EA46-4F67-841F-6A9465D9D515	c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2txyewy!App
FM Radio	F725010E-455D-4C09-AC48-BCDEF0D4B626	N/A
Get Started	B3726308-3D74-4A14-A84C-867C8C735C3C	Microsoft.Getstarted_8wekyb3d8bbwe!App
Groove Music	D2B6A184-DA39-4C9A-9E0A-8B589B03DEC0	Microsoft.ZuneMusic_8wekyb3d8bbwe!Microsoft.ZuneMusic
Maps	ED27A07E-AF57-416B-BC0C-2596B622EF7D	Microsoft.WindowsMaps_8wekyb3d8bbwe!App

Application Package Name	Product ID	Application User Model ID (AUMID)
Messaging	27E26F40-E031-48A6-B130-D1F20388991A	Microsoft.Messaging_8wekyb3d8bbwe!x27e26f40ye031y48a6yb130yd1f20388991ax
Microsoft Edge	395589FB-5884-4709-B9DF-F7D558663FFD	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge
Money	1E0440F1-7ABF-4B9A-863D-177970EEFB5E	Microsoft.BingFinance_8wekyb3d8bbwe!AppexFinance
Movies and TV	6AFFE59E-0467-4701-851F-7AC026E21665	Microsoft.ZuneVideo_8wekyb3d8bbwe!Microsoft.ZuneVideo
News	9C3E8CAD-6702-4842-8F61-B8B33CC9CAF1	Microsoft.BingNews_8wekyb3d8bbwe!AppexNews
Outlook Calendar	A558FEBA-85D7-4665-B5D8-A2FF9C19799B	Microsoft.WindowsCommunicationsApps_8wekyb3d8bbwe!Microsoft.WindowsLive.Calendar
Outlook Mail	A558FEBA-85D7-4665-B5D8-A2FF9C19799B	Microsoft.WindowsCommunicationsApps_8wekyb3d8bbwe!Microsoft.WindowsLive.Mail
People	60BE1FB8-3291-4B21-BD39-2221AB166481	Microsoft.People_8wekyb3d8bbwe!xb94d6231y84ddy49a8yace3ybc955e769e85x
Phone (dialer)	F41B5D0E-EE94-4F47-9CFE-3D3934C5A2C7	Microsoft.CommsPhone_8wekyb3d8bbwe!App
Photos	FCA55E1B-B9A4-4289-882F-084EF4145005	Microsoft.Windows.Photos_8wekyb3d8bbwe!App
Podcasts	C3215724-B279-4206-8C3E-61D1A9D63ED3	Microsoft.MSPodcast_8wekyb3d8bbwe!xc3215724yb279y4206y8c3ey61d1a9d63ed3x
PowerPoint	B50483C4-8046-4E1B-81BA-590B24935798	Microsoft.Office.PowerPoint_8wekyb3d8bbwe!microsoft.pptim
Settings	2A4E62D8-8809-4787-89F8-69D0F01654FB	2a4e62d8-8809-4787-89f8-69d0f01654fb_8wekyb3d8bbwe!App
Skype	C3F8E570-68B3-4D6A-BDBB-C0A3F4360A51	Microsoft.SkypeApp_kzf8qxf38zg5c!Skype.AppId

Application Package Name	Product ID	Application User Model ID (AUMID)
Skype Video	27E26F40-E031-48A6-B130-D1F20388991A	Microsoft.Messaging_8wekyb3d8bbwe!App
Sports	0F4C8C7E-7114-4E1E-A84C-50664DB13B17	Microsoft.BingSports_8wekyb3d8bbwe!Appex Sports
Storage	5B04B775-356B-4AA0-AAF8-6491FFEA564D	N/A
Store	7D47D89A-7900-47C5-93F2-46EB6D94C159	Microsoft.WindowsStore_8wekyb3d8bbwe!App
Voice Recorder	7311B9C5-A4E9-4C74-BC3C-55B06BA95AD0	Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe!App
Weather	63C2A117-8604-44E7-8CEF-DF10BE3A57C8	Microsoft.BingWeather_8wekyb3d8bbwe!App
Word	258F115C-48F4-4ADB-9A68-1387E634459B	Microsoft.Office.Word_8wekyb3d8bbwe!microsoft.word