MICROSOFT (MS) WINDOWS 10 MOBILE STIG CONFIGURATION TABLE

Version 1, Release 4

24 April 2020

Developed by Microsoft and DISA for the DoD

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	AboveLock	AllowActionCenterNotifications	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-200101	
Policy	AboveLock	AllowToasts			X	0		Local site can change setting based on mission needs.
Policy	Accounts	AllowAddingNonMicrosoftAccountsManually	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-910201	
Policy	Accounts	AllowMicrosoftAccountConnection			X	1		Local site can change setting based on mission needs.
Policy	Accounts	DomainNamesForEmailSync			X			Local site can change setting based on mission needs.
Policy	ApplicationManagement	AllowAllTrustedApps			X	0		Local site can change setting based on mission needs.
Policy	ApplicationManagement	AllowAppStoreAutoUpdate			X			Local site can change setting based on mission needs.
Policy	ApplicationManagement	Allow Developer Unlock	0 – Explicit deny 1 – Explicit allow unlock 65535 (default) – Not configured	X		0	MSWM-10-200303	
Policy	ApplicationManagement	AllowSharedUserAppData			X			Local site can change setting based on mission needs.
Policy	ApplicationManagement	AllowStore	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-200305	Supported on Windows 10

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								Mobile – AppLocker is replacement
Policy	ApplicationManagement	ApplicationRestrictions	XML data showing allowed product ID	X		Varies by MDM. Essentially, a list of ProductIDs needs to be compiled that corresponds to the allowed applications list. A list of ProductIDs for apps that can ship with Windows 10 Mobile can be found here: https://technet.microsoft.com/itpro/windows/manage/product-ids-in-windows-10-mobile	MSWM-10-200306 MSWM-10-202412	
Policy	ApplicationManagement	RequirePrivateStoreOnly			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	ApplicationManagement	RestrictAppDataToSystemVolume			**X**			Local site can change setting based on mission needs.
Policy	ApplicationManagement	RestrictAppToSystemVolume			**X**			Local site can change setting based on mission needs.
AppLocker	AppLocker	EnterpriseDataProtection	List of Windows Store Applications that are allowed to access DoD enterprise data.	**X**		Within MDM configuration for data protection/Windows Information Protection, this is the list of managed applications that are allowed to access data from DoD protected networks.	MSWM-10-911101	Should be used in conjunction with the settings in EnterpriseDataProtection policies.
Policy	Authentication	AllowFastReconnect			**X**			Local site can change setting based on mission needs.
Bitlocker	Bitlocker	EncryptionMethodByDriveType	3 = AES-CBC 128 4 = AES-CBC 256 6 = XTS-AES 128 7 = XTS-AES 256		**X**	3 (default) – XTS-AES 128-bit		Local site can change setting based on mission needs.
Policy	Bluetooth	AllowAdvertising	0 – Not allowed. When set to 0, the device will	**X**		0	MSWM-10-200512	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			not send out advertisements. To verify, use any Bluetooth LE app and enable it to do advertising. Then, verify that the advertisement is not received by the peripheral. 1 (default) – Allowed. When set to 1, the device will send out advertisements. To verify, use any Bluetooth LE app and enable it to do advertising. Then, verify that the advertisement is received by the peripheral.					
Policy	Bluetooth	AllowDiscoverableMode	0 – Not allowed. When set to 0, other devices will not be able to detect the device. To verify, open the Bluetooth control panel on the device. Then, go to another Bluetooth-enabled device, open the Bluetooth control panel, and verify that you cannot see the name of the device. 1 (default) – Allowed. When set to 1, other	**X**		0	MSWM-10-910502	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			devices will be able to detect the device. To verify, open the Bluetooth control panel on the device. Then, go to another Bluetooth-enabled device, open the Bluetooth control panel and verify that you can discover it. If this is not set or it is deleted, the default value of 1 (Allow) is used.					
Policy	Bluetooth	LocalDeviceName			**X**			Local site can change setting based on mission needs.
Policy	Bluetooth	ServicesAllowedList	Set a list of allowable services and profiles. String hex formatted array of Bluetooth service UUIDs in canonical format, delimited by semicolons. For example, {782AFCFC-7CAA-436C-8BF0-78CD0FFBD4AF}. The default value is an **empty string**.	**X**		{0000111E-0000-1000-8000-00805F9B34FB};{00001108-0000-1000-8000-00805F9B34FB};{00001101-0000-1000-8000-00805F9B34FB}	MSWM-10-500504	
	Browser	AllowBrowser			**X**			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
	Browser	AllowCookies			X			Local site can change setting based on mission needs.
	Browser	AllowDoNotTrack			X			Local site can change setting based on mission needs.
	Browser	AllowInPrivate			X			Local site can change setting based on mission needs.
Policy	Browser	AllowPasswordManager	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-910505	
Policy	Browser	AllowSearchSuggestionsinAddressBar			X			Local site can change setting based on mission needs.
Policy	Browser	AllowSmartScreen			X			Local site can change setting based on mission needs.
Policy	Browser	EnterpriseModeSiteList			X			Local site can change setting based on mission needs.
Policy	Browser	FirstRunURL			X			Local site can change setting based on mission needs.
Policy	Browser	PreventSmartScreenPromptOverride			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Browser	PreventSmartScreenPromptOverrideForFiles			**X**			Local site can change setting based on mission needs.
Policy	Camera	AllowCamera			**X**			Local site can change setting based on mission needs.
Policy	Connectivity	AllowBluetooth			**X**	0		Local site can change setting based on mission needs.
Policy	Connectivity	AllowCellularDataRoaming			**X**			Local site can change setting based on mission needs.
Policy	Connectivity	AllowNFC	0 – Not allowed 1 (default) – Allowed	**X**		0	MSWM-10-910703	
Policy	Connectivity	AllowUSBConnection	Enables USB connection between the device and a computer to sync files with the device or to use developer tools to deploy or debug applications. Changing this policy does not affect USB charging. Both Media Transfer Protocol (MTP) and IP over USB are disabled when this policy is enforced.	**X**		0	MSWM-10-202608 MSWM-10-290704	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			The following list shows the supported values: • 0 – Not allowed. • 1 (default) – Allowed. Most restricted value is 0.					
Policy	Connectivity	AllowVPNOverCellular			**X**			Local site can change setting based on mission needs.
Policy	Connectivity	AllowVPNRoamingOverCellular			**X**			Local site can change setting based on mission needs.
Policy	Cryptography	AllowFipsAlgorithmPolicy			**X**			Local site can change setting based on mission needs.
Policy	Cryptography	TLSCipherSuites			**X**			Local site can change setting based on mission needs.
Policy	Device Lock	AllowIdleReturnWithoutPassword			**X**			Local site can change setting based on mission needs.
Policy	Device Lock	AllowScreenTimeoutWhileLocked UserConfig			**X**			Local site can change setting based on mission needs.
Policy	Device Lock	AllowSimpleDevicePassword	0 – Not allowed 1 (default) – Allowed	**X**		0	MSWM-10-201003	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Device Lock	AlphanumericDevicePasswordRequired			**X**	2		Local site can change setting based on mission needs.
Policy	Device Lock	DevicePasswordEnabled		**X**		0	MSWM-10-911005	
Policy	Device Lock	DevicePasswordExpiration			**X**			Local site can change setting based on mission needs.
Policy	Device Lock	DevicePasswordHistory			**X**			Local site can change setting based on mission needs.
Policy	Device Lock	MaxDevicePasswordFailedAttempts	An integer X where 0 <= X <= 999 for mobile devices. 0 (default) - The device is never wiped after an incorrect PIN or password is entered. Most secure value is 0 if all policy values = 0; otherwise, Min policy value is the most secure value.	**X**		10	MSWM-10-201008	
Policy	Device Lock	MaxInactivityTimeDeviceLock	An integer X where 0 <= X <= 999. 0 (default) - No timeout is defined. The default of "0" is interpreted as "No timeout is defined."	**X**		15	MSWM-10-201009	
Policy	Device Lock	MinDevicePasswordComplexCharacters			**X**			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Device Lock	ScreenTimeoutWhileLocked			X			Local site can change setting based on mission needs.
Policy	Device Lock	MinDevicePasswordLength	• An integer X where 4 <= X <= 16 for mobile devices and desktop. However, local accounts will always enforce a minimum password length of 6. • Not enforced. • The default value is 4 for mobile devices and desktop devices.	X		6	MSWM-10-201012	
EnterpriseDataProtection	Settings	EDPEnforcementLevel	0 (default) – Off / No protection (decrypts previously protected data). 1 – Silent mode (encrypt and audit only). 2 – Override mode (encrypt, prompt, and audit). 3 – Block mode (encrypt, block, and audit).	X		3	MSWM-10-911101	
EnterpriseDataProtection	Settings	EnterpriseProtectedDomainNames	List of protected domain names. The first name is the primary corporate identity, followed by additional enterprise domain names such as	X		Varies by DoD group. The first domain in the list must be the primary	MSWM-10-911101	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			email server domains. Examples: • disa.mil, mail.mil • dod.mil, army.dod.mil • contoso.com, contoso.net			enterprise ID. User identities from one of these domains is considered an enterprise managed account and data associated with it should be protected. For example, the domains for all email accounts owned by the enterprise would be expected to appear in this list.		
EnterpriseDataProtection	Settings	EDPShowIcons	0 (default) – No WIP overlays on icons or tiles. 1 – Show WIP overlays on protected files and apps that can only create enterprise content.	X*		1	MSWM-10-911101	* This setting could be optional; however, it is very valuable to be able to see that a file is encrypted with this policy by seeing the briefcase icon

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								next to files in the File Manager application.
EnterpriseDataProtection	Settings	RequireProtectionUnderLockConfig	0 (default) – Not enforced 1 – Enforced	X		1	MSWM-10-911101	This setting is only supported in Windows 10 Mobile.
EnterpriseDataProtection	Settings	RevokeOnUnenroll	0 – Do not revoke keys. 1 (default) – Revoke keys.	X		1	MSWM-10-911101	
Policy	Experience	AllowCortana	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-911102	
Policy	Experience	AllowDeviceDiscovery			X			Local site can change setting based on mission needs.
Policy	Experience	AllowManualMDMUnenrollment	0 – Not allowed 1 (default) – Allowed	X		0	MSWM-10-911104	
Policy	Experience	AllowScreenCapture			X			Local site can change setting based on mission needs.
Policy	Experience	AllowSIMErrorDialogPromptWhenNoSIM			X			Local site can change setting based on mission needs.
Policy	Experience	AllowSyncMySettings	0 – Sync settings is disallowed. 1 (default) – Sync settings allowed.	X		0	MSWM-10-911107 MSWM-10-202507	
Policy	Experience	AllowTaskSwitcher			X			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Experience	AllowVoiceRecording			**X**			Local site can change setting based on mission needs.
Policy	Experience	DoNotShowFeedbackNotifications	0 (default) – Feedback notifications are not disabled. The actual state of feedback notifications on the device will then depend on what GP has configured or what the user has configured locally. 1 – Feedback notifications are disabled.		**X**			Local site can change setting based on mission needs.
Policy	NetworkIsolation	EnterpriseCloudResources			**X**			Local site can change setting based on mission needs.
Policy	NetworkIsolation	EnterpriseInternalProxyServers			**X**			Local site can change setting based on mission needs.
Policy	NetworkIsolation	EnterpriseIPRange	Sets the enterprise IP ranges that define the computers in the enterprise network. Data that comes from those computers will be considered part of the enterprise and protected. These locations will be	**X**		This varies within DoD groups. Site-specific IP ranges need to be defined.	MSWM-10-911101	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			considered a safe destination for enterprise data to be shared to. This is a **comma-separated list** of IPv4 and IPv6 ranges.			Example of IPv4 and IPv6 ranges: 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		
Policy	NetworkIsolation	EnterpriseIPRangesAreAuthoritative			**X**			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	NetworkIsolation	EnterpriseNetworkDomainNames	This is the list of domains that compose the boundaries of the 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: The client requires domain name to be canonical, otherwise the setting will be rejected by the client.	X		This varies by DoD group. Examples would be: 1) corp.contoso.com,region.contoso.com 2) corp.contoso.com,region.contoso.com 3) army.dod.mil, eur.army.mil	MSWM-10-911101	
Policy	NetworkIsolation	EnterpriseProxyServers			X			Local site can change setting based on mission needs.
Policy	NetworkIsolation	EnterpriseProxyServersAreAuthoritative			X			Local site can change setting based on mission needs.
Policy	NetworkIsolation	NeutralResources			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Privacy	AllowAutoAcceptPairingAndPrivacyConsentPrompts			**X**			**Local site can change setting based on mission needs.**
Policy	Privacy	AllowInputPersonalization			**X**			**Local site can change setting based on mission needs.**
Policy	Privacy	DisableAdvertisingId			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessAccountInfo			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessAccountInfo_ForceAllowTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessAccountInfo_ForceDenyTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessAccountInfo_UserInControlOfTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCalendar			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCalendar_ForceAllowTheseApps			**X**			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Privacy	LetAppsAccessCalendar_ForceDenyTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCalendar_UserInControlOfTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCallHistory			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCallHistory_ForceAllowTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCallHistory_ForceDenyTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCallHistory_UserInControlOfTheseApps			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCamera			**X**			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCamera_ForceAllowTheseApps			**X**			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Privacy	LetAppsAccessCamera_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessCamera_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessContacts			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessContacts_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessContacts_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessContacts_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessEmail			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessEmail_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessEmail_ForceDenyTheseApps			X			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Privacy	LetAppsAccessEmail_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessLocation			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessLocation_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessLocation_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessLocation_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMessaging			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMessaging_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMessaging_ForceDenyTheseApps			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Privacy	LetAppsAccessMessaging_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMicrophone			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMicrophone_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMicrophone_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMicrophone_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMotion			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMotion_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMotion_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessMotion_UserInControlOfTheseApps			X			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Privacy	LetAppsAccessNotifications			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessNotifications_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessNotifications_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessNotifications_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessPhone			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessPhone_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessPhone_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessPhone_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Privacy	LetAppsAccessRadios			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessRadios_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessRadios_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessRadios_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTasks			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTasks_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTasks_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTasks_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTrustedDevices			X			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Privacy	LetAppsAccessTrustedDevices_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTrustedDevices_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsAccessTrustedDevices_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsGetDiagnosticInfo			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsGetDiagnosticInfo_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsGetDiagnosticInfo_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsGetDiagnosticInfo_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsRunInBackground			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Privacy	LetAppsRunInBackground_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsRunInBackground_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsRunInBackground_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsSyncWithDevices			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsSyncWithDevices_ForceAllowTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsSyncWithDevices_ForceDenyTheseApps			X			Local site can change setting based on mission needs.
Policy	Privacy	LetAppsSyncWithDevices_UserInControlOfTheseApps			X			Local site can change setting based on mission needs.
Policy	Search	AllowIndexingEncryptedStoresOrItems			X			Local site can change setting based on mission needs.
Policy	Search	AllowSearchToUseLocation			X			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Search	AllowUsingDiacritics			**X**			Local site can change setting based on mission needs.
Policy	Search	AlwaysUseAutoLangDetection			**X**			Local site can change setting based on mission needs.
Policy	Search	SafeSearchPermissions			**X**			Local site can change setting based on mission needs.
Policy	Security	AllowAddProvisioningPackage			**X**			Local site can change setting based on mission needs.
Policy	Security	AllowManualRootCertificateInstallation			**X**			Local site can change setting based on mission needs.
Policy	Security	AllowRemoveProvisioningPackages			**X**			Local site can change setting based on mission needs.
Policy	Security	AntiTheftMode			**X**			
Policy	Security	RequireDeviceEncryption	0 (default) – Encryption is not required. 1 – Encryption is required.	**X**		1	MSWM-10-201405	
Policy	Security	RequireProvisioningPackageSignature			**X**			Local site can change setting

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
								based on mission needs.
Policy	Security	RequireRetrieveHealthCertificateOnBoot			**X**			Local site can change setting based on mission needs.
Policy	Settings	AllowDataSense			**X**			Local site can change setting based on mission needs.
Policy	Settings	AllowDateTime			**X**			Local site can change setting based on mission needs.
Policy	Settings	AllowVPN			**X**			Local site can change setting based on mission needs.
Policy	Settings	AllowYourAccount			**X**			Local site can change setting based on mission needs.
Policy	System	AllowBuildPreview	This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and		**X**			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			installing Windows preview software.					
Policy	System	AllowEmbeddedMode			**X**			Local site can change setting based on mission needs.
Policy	System	AllowExperimentation			**X**			Local site can change setting based on mission needs.
Policy	System	AllowLocation			**X**			Local site can change setting based on mission needs.
Bitlocker	Bitlocker		0 (default) – Storage cards do not need to be encrypted. 1 – Require Storage cards to be encrypted. Disabling this policy will not turn off the encryption on the system card, but the user will no longer be prompted to turn it on.	**X**		1	MSWM-10-201705	New for Windows 10 Mobile 1703
Policy	System	AllowTelemetry	0 – No telemetry data is sent from OS components. **Note**: This value is only applicable to enterprise and server devices. Using this setting on other	**X**		0	MSWM-10-501706	**Note**: To set the telemetry value = 0, this requires Windows 10

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			devices is equivalent to setting the value of 1. 1 – Sends basic telemetry data. 2 – Sends enhanced telemetry data including usage and insights data. 3 (default) – Sends full telemetry data including diagnostic data, such as system state.					Mobile Enterprise.
Policy	System	AllowUserToResetPhone			**X**			Local site can change setting based on mission needs.
Policy	TextInput	AllowLinguisticDataCollection			**X**			Local site can change setting based on mission needs.
Policy	Update	AllowAutoUpdate	0 – Notify the user before downloading the update. 1 – Auto install the update and then notify the user to schedule a device restart. 2 (default) – Auto install and restart. 3 – Auto install and restart at a specified time. 4 – Auto install and restart without end-user control.	**X**		1	MSWM-10-201901	**Note**: To use the AllowAutoUpdate setting, this requires Windows 10 Mobile Enterprise.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			5 – Turn off automatic updates. NOTE: This option should be used only for systems under regulatory compliance, as you will not get security updates as well.					
Policy	Update	AllowNonMicrosoftSignedUpdate			**X**			Local site can change setting based on mission needs.
Policy	Update	AllowUpdateService			**X**			Local site can change setting based on mission needs.
Policy	Update	DeferUpdatePeriod			**X**			Local site can change setting based on mission needs.
Policy	Update		The following list shows the supported values: 16 (default) – User gets all applicable upgrades from Current Branch (CB). 32 – User gets upgrades from Current Branch for Business (CBB).	**X**		32	MSWM-10-201901	Added in Windows 10, version 1607. Allows the IT admin to set which branch a device receives their updates from.
Policy	Update	DeferUpgradePeriod			**X**			
Policy	Update	PauseDeferrals			**X**			

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Update		0 (default) – User gets upgrades from Current Branch. 1 – User gets upgrades from Current Branch for Business.		X			
Policy	Update	RequireUpdateApproval			X			Local site can change setting based on mission needs.
Policy	Update	ScheduledInstallDay			X			Local site can change setting based on mission needs.
Policy	Update	ScheduleInstallTime			X			Local site can change setting based on mission needs.
Policy	Update	UpdateServiceUrl			X			Local site can change setting based on mission needs.
Policy	Wi-Fi	AllowAutoConnectToWiFiSenseHotspots			X			Local site can change setting based on mission needs.
Policy	Wi-Fi	AllowInternetSharing	0 – Do not allow the use of Internet Sharing. 1 (default) – Allow the use of Internet Sharing.		X			Local site can change setting based on mission needs.
Policy	Wi-Fi	AllowManualWiFiConfiguration			X			Local site can change setting based on mission needs.

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
Policy	Wi-Fi	AllowWiFi			**X**			Local site can change setting based on mission needs.
Policy	Wi-Fi	WLANScanMode			**X**			Local site can change setting based on mission needs.
Policy	Wi-Fi	DisableWirelessRemoteConnectionsExceptHotspot			**X**			Local site can change setting based on mission needs.
RemoteWipe	RemoteWipe	doWipe			**X**			Local site can change setting based on mission needs.
RemoteWipe	RemoteWipe	doWipePersistProvisionedData						Local site can change setting based on mission needs.
Reporting	SecurityAuditing	RetrieveByTimeRange			**X**			Local site can change setting based on mission needs.
Reporting	SecurityAuditing	RetrieveByCount			**X**			Local site can change setting based on mission needs.
WindowsSecurityAuditing	WindowsSecurityAuditing - ConfigurationSettings	EnableSecurityAuditing	Specifies whether to enable or disable auditing for the device. Value type is boolean. If true, a default set of audit	**X**		True	MSWM-10-203003	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			events will be captured to a log file for upload; if false, auditing is disabled and events are not logged. Default value is **false**.					
WindowsLicensing	WindowsLicensing	UpgradeEditionWithLicense	The upgrade is handled via a licensing key available from the Microsoft Volume Licensing Service Center (VLSC). The process for upgrading is described here: https://technet.microsoft.com/itpro/windows/deploy/windows-10-edition-upgrades	**X**		Licensing Key for Windows 10 Mobile Enterprise	MSWM-10-912419	
PassportForWork	Biometrics	UseBiometrics	Boolean value used to enable or disable the use of biometric gestures, such as face and fingerprint, as an alternative to the PIN gesture for Passport. Users must still configure a PIN if they configure biometric gestures to use in case of failures. This node was added in Windows 10, version 1511.	**X**		False	MSWM-10-202801	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			Default value is **true**. If you set this policy to true, biometric gestures are enabled for use with Passport. If you set this policy to false, biometric gestures are disabled for use with Passport.					
VPNv2	VPN	Lockdown/Split-tunnel	Configure VPN profile with desired connection settings. Include the Lockdown option: VPNv2/ProfileName/LockDown Lockdown profile: Valid values: • False (default) – This is not a LockDown profile. • True – This is a LockDown profile. When the LockDown profile is turned on, it does the following things: • First, it automatically becomes an "always on" profile. • Second, it can never be disconnected.	**X**		True	MSWM-10-202901 MSWM-10-202409 MSWM-10-202418	

CSP Name	Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments
			• Third, if the profile is not connected, the user has no network. • Fourth, no other profiles may be connected or modified. Include the Split-tunnel option: Policies/SplitTunnel Valid values: • False – All traffic goes to the VPN gateway in force tunnel mode. • True – Only the specific traffic goes to the VPN gateway.					