SONY

Xperia™ in Business
Mobile Device Management

Read about how Xperia™ devices can be administered in a corporate IT environment

Device management clients

March 2015

Exchange® ActiveSync®

The my Xperia service

Android for Work

Third party Mobile Device Management solutions

Device inventory

Xperia Configurator

Products covered

This document describes Xperia in Business enterprise services and features in Sony Mobile devices. Please refer to the tables at the end of this document for details about supported products and software versions.

Note: xxx in software versions denotes the number "001-999".

To find the software version of a device, select **About phone** in **Settings**.

Limitations to services and features

Some of the services and features described in this document might not be supported in all countries/regions or by all networks and/or service providers in all areas. Please contact your network operator or service provider to determine availability of any specific service or feature and whether additional access or usage fees apply.

Document release date

March 1, 2015

Mobile Device Management

Xperia™ devices that are deployed in your organisation's IT environment integrate easily with a number of device management solutions.

Device management clients

Xperia™ devices support device management with the built-in Microsoft® Exchange ActiveSync® (EAS) client, the free 'my Xperia' service from Sony Mobile, and the leading Mobile Device Management (MDM) third-party solutions. These solutions make it possible to manage both corporate-owned, and personal Xperia™ devices (using a Bring Your Own Device policy) over the air from a single management console.

When integrated into an MDM-enabled business IT environment, Xperia™ devices offer a comprehensive array of policies, device command/administration features, provisioning support, and device inventory collection functions. Xperia™ devices also support device management features such as wireless configuration, settings and software updating, enforcement of policies including adherence monitoring, and remote wiping and locking of devices.

Exchange ActiveSync®

Microsoft® Exchange ActiveSync® enables mobile devices to synchronise email messages, calendar and contacts with a Microsoft® Exchange Server. EAS also provides device management capabilities and the ability to control mobile devices in a server network. The Microsoft® Exchange ActiveSync® implementation in Xperia™ devices has support for Microsoft® Exchange ActiveSync® MDM features including security and device policies as well as device administration features.

Microsoft® Exchange ActiveSync® enabled Xperia devices that are deployed in a network can be controlled and monitored using Exchange Server with password policies such as mandatory PIN or password usage, minimum PIN or password length, and PIN and password resetting over the air. You can also control the number of incorrect PINs or passwords that can be entered before all data is deleted from the device. The support for Microsoft® Exchange ActiveSync® device administration in Xperia devices also gives administrators the ability to remotely perform a factory reset to wipe a device of all data and configurations.

The my Xperia service

Sony Mobile Communications offers a free-of-charge basic MDM service called my Xperia. The my Xperia service helps you to find a misplaced Xperia™ device, and protects its private information by locking or even remotely wiping all information on the device. The Locate function helps you to find your Xperia™ device by locating it on a map.

Mobile Device Management

my Xperia features:
- Locate device on a map
- Set a sound alert on the device
- Lock device
- Set new PIN and screen message
- Remote wipe (Factory reset)

Android for Work:
- Dedicated work profile with hardware based encryption and sharing restrictions to secure business data
- IT administrator has full control of all work related policies, profiles and data, from distributing apps to wiping business information
- Find and deploy business apps easily with Google Play and create apps quickly with the Android app framework
- AfW sorter in drawer menu to only show AfW apps on Homescreen

You can lock your device and replace the existing screen lock (e.g. pattern, PIN, password) on your device with a new PIN. When you lock the device, you can also write a message that will be displayed on the screen of your device when it is found. You can also display a phone number where the finder can reach you. If you want to make sure that nobody gets hold of any private information on your misplaced Xperia™ device, you can erase your data remotely. You can choose to wipe the data from the internal memory, the memory card, or both.

The my Xperia service uses the Google account on your device. If you are using several Google accounts on your device, you can sign in with any of them. You can connect several devices to the my Xperia service using the same Google account. The my Xperia service is available at myxperia. sonymobile.com.

Android for Work
Android for Work is a solution that creates a managed profile to separate business and personal space on a device. It keeps the data separate without requiring any changes to existing apps. The employer administers the managed profile and all apps in it, while the employee controls the private space.

Third party Mobile Device Management solutions
Xperia™ devices support all major MDM providers through the native Android device management APIs and the Sony Mobile APIs. Xperia™ devices have comprehensive support for over-the-air management of settings, policies, device and application commands, as well as provisioning and inventory.

A wide range of device management tasks can be performed. You can, for example, enforce password policies, remotely wipe the internal memory and SD card of an Xperia™ device, or reset it to its factory settings.

Device provisioning abilities include remote configuration of HTTP proxy settings, Wi-Fi and APNs. Xperia™ devices support application inventory features that let you get a list of all apps installed on a device and retrieve information on the usage of individual apps. Furthermore, there is extensive support for hardware inventory features, making it possible to check what hardware is supported across the fleet of Xperia™ devices in your network. In addition, you can make an inventory of the IP network status of devices and get mobile network information for devices in the network.

Device inventory
With a large number of inventory management features supported by Xperia™ devices from Sony it is easy to keep track of the equipment used by an organisation. Administrators can get complete hardware and software inventory as well as mobile-specific information such as IP and mobile network status of managed devices.

Xperia Configurator
The Sony Xperia Configurator is a Windows software that allows you to create, construct and install configuration profiles on Sony devices. Xperia Configurator makes it easy to configure and deploy device policies and settings.

Mobile Device Management

Xperia Z series

PRODUCT	Xperia Z Xperia ZL Xperia ZR Xperia Tablet Z	Xperia Z1 Xperia Z1 Compact Xperia Z Ultra	Xperia Z2 Xperia Z2 Tablet	Xperia Z3 Xperia Z3 Compact Xperia Z3 Tablet Compact	Xperia Z4 Tablet
ANDROID VERSION	4.3.x	4.3.x	4.4.x	4.4.x	5.0.x
SOFTWARE VERSION	10.4.B.0.xxx	14.2.A.0.xxx	17.1.1.A.0.xxx	23.0.A.2.xxx 23.0.A.1.xxx (Tablet)	28.0.A.0.xxx
Allow HTML email	X	X	X	X	X
Max HTML email body truncation size	X	X	X	X	X
Max email body truncation size	X	X	X	X	X
Attachments enabled	X	X	X	X	X
Max attachment size	X	X	X	X	X
Max email age filter	X	X	X	X	X
Max calendar age filter	X	X	X	X	X
Password recovery enabled	X	X	X	X	X
Require password	X	X	X	X	X
Min password length	X	X	X	X	X
Min password complex characters	X	X	X	X	X
Require alphanumeric password	X	X	X	X	X
Max password failed attempts	X	X	X	X	X
Restrict password history	X	X	X	X	X
Password expiration	X	X	X	X	X
Max inactivity time lock	X	X	X	X	X
Require signed S/MIME messages	X	X	X	X	X
Require encrypted S/MIME messages	X	X	X	X	X
Require signed S/MIME algorithm	X	X	X	X	X
Require encryption S/MIME algorithm	X	X	X	X	X
Require device encryption	X	X	X	X	X
Allow camera	X	X	X	X	X
Prompt new password	X	X	X	X	X
Wipe device	X	X	X	X	X
Allow / Block / Quarantine (ABQ) list	X	X	X	X	X
Locate device	X	X	X	X	X
Sound an alert	X	X	X	X	X
Allow storage card	X	X	X	X	X
Allow Wi-Fi	X	X	X	X	X
Allow Bluetooth	X	X	X	X	X
Allow tethering	X	X	X	X	X
Allow desktop sync	X	X	X	X	X
Allow simple password	X	X	X	X	X
Allow browser	X	X	X	X	X
Application Black/White listing	X	X	X	X	X
Require storage card encryption	X	X	X	X	X
Allow IrDA	X	X	X	X	X
Allow roaming	X	X	X	X	X
Allow auto sync when roaming	X	X	X	X	X
Wipe storage card only	X	X	X	X	X
Add EAS account	X	X	X	X	X
VPN configuration	X	X	X	X	X
Track data usage	X	X	X	X	X
Get rooting status	X	X	X	X	X
Allow location providers			X	X	X
Allow sending SMS/MMS			X	X	X
Allow screen capture			X	X	X
Allow USB debugging			X	X	X
Allow USB mass storage			X	X	X
Allow Non-market app installation			X	X	X
Limit amount of roaming data			X	X	X
Install and remove email account (POP3, IMAP4)			X	X	X
Install certificate (VPN, Wi-Fi or S/MIME)			X	X	X
Packet filtering			X	X	X
Allow deactivation			X	X	X
Allow adding guest users			X	X	X

Mobile Device Management

PRODUCT	Xperia Z Xperia ZL Xperia ZR Xperia Tablet Z	Xperia Z1 Xperia Z1 Compact Xperia Z Ultra	Xperia Z2 Xperia Z2 Tablet	Xperia Z3 Xperia Z3 Compact Xperia Z3 Tablet Compact	Xperia Z4 Tablet
Allow application installation or uninstallation			X	X	X
Allow POP/IMAP email			X	X	X
Allow consumer email			X	X	X
One time password			X	X	X
Device lockout			X	X	X
Allow microphone					X
Allow backgroud data					X
Allow data usage (Mobile Data)					X
Allow access to device settings					X
Allow voice roaming					X
Allow sync data in accounts					X
Allow NFC					X
Remove and list certificates					X
List VPN profiles					X
MDM Silent Installation					X
AXSEED SAP MDM Support ver.1.0					X
MDM for prototype information protection					X
Device Configurator (PC tool)			X	X	X
Device Configurator (Cloud tool)					X
FIPS 140-2 Certification					X
E-SDK device tracker (MDM)			X	X	X
SE Linux policies					X
Enhanced PIM					X
Enterprise Single sign on (SSO)					X
Enterprise Home screen					X
Automatic peripheral detect					X

Xperia E, T and M series

PRODUCT	Xperia E3	Xperia T2 Ultra Xperia T2 Ultra Dual	Xperia T3	Xperia M2 Xperia M2 Dual Xperia M2 Aqua	Xperia M4 Aqua
ANDROID VERSION	4.4.x	4.3.x	4.4.x	4.4.x	5.0.x
SOFTWARE VERSION	18.4.C.1.xxx	19.0.1.A.0.xxx 19.0.D.0.xxx (Dual)	18.1.A.1.xxx	18.3.C.0.xxx	26.1.A.0.xxx
Allow HTML email	X	X	X	X	X
Max HTML email body truncation size	X	X	X	X	X
Max email body truncation size	X	X	X	X	X
Attachments enabled	X	X	X	X	X
Max attachment size	X	X	X	X	X
Max email age filter	X	X	X	X	X
Max calendar age filter	X	X	X	X	X
Password recovery enabled	X	X	X	X	X
Require password	X	X	X	X	X
Min password length	X	X	X	X	X
Min password complex characters	X	X	X	X	X
Require alphanumeric password	X	X	X	X	X
Max password failed attempts	X	X	X	X	X
Restrict password history	X	X	X	X	X
Password expiration	X	X	X	X	X
Max inactivity time lock	X	X	X	X	X
Require signed S/MIME messages	X	X	X	X	X
Require encrypted S/MIME messages	X	X	X	X	X
Require signed S/MIME algorithm	X	X	X	X	X
Require encryption S/MIME algorithm	X	X	X	X	X
Require device encryption	X	X	X	X	X
Allow camera	X	X	X	X	X
Prompt new password	X	X	X	X	X
Wipe device	X	X	X	X	X
Allow / Block / Quarantine (ABQ) list	X	X	X	X	X
Locate device	X	X	X	X	X

Mobile Device Management

PRODUCT	Xperia E3	Xperia T2 Ultra Xperia T2 Ultra Dual	Xperia T3	Xperia M2 Xperia M2 Dual Xperia M2 Aqua	Xperia M4 Aqua
Sound an alert	X	X	X	X	X
Allow storage card	X	X	X	X	X
Allow Wi-Fi	X	X	X	X	X
Allow Bluetooth	X	X	X	X	X
Allow tethering	X	X	X	X	X
Allow desktop sync	X	X	X	X	X
Allow simple password	X	X	X	X	
Allow browser	X	X	X	X	X
Application Black/White listing	X	X	X	X	X
Require storage card encryption	X	X	X	X	X
Allow IrDA	X	X	X	X	X
Allow roaming	X	X	X	X	
Allow auto sync when roaming	X	X	X	X	
Wipe storage card only	X	X	X	X	
Add EAS account	X	X	X	X	X
VPN configuration	X	X	X	X	
Track data usage	X	X	X	X	
Get rooting status		X	X		X
Allow location providers	X		X	X	X
Allow sending SMS/MMS			X		X
Allow screen capture	X		X	X	
Allow USB debugging	X		X	X	
Allow USB mass storage	X		X	X	X
Allow Non-market app installation	X		X	X	X
Limit amount of roaming data			X		X
Install and remove email account (POP3, IMAP4)	X	X	X	X	X
Install certificate (VPN, Wi-Fi or S/MIME)	X		X	X	
Packet filtering			X		X
Allow deactivation			X		
Allow adding guest users			X		
Allow application installation or uninstallation			X		
Allow POP/IMAP email			X		
Allow consumer email			X		
One time password			X		X
Device lockout			X		
Allow microphone					
Allow backgroud data					
Allow data usage (Mobile Data)					
Allow access to device settings					
Allow voice roaming					
Allow sync data in accounts					
Allow NFC					
Remove and list certificates					
List VPN profiles					
MDM Silent Installation					
AXSEED SAP MDM Support ver.1.0					
MDM for prototype information protection					
Device Configurator (PC tool)					
Device Configurator (Cloud tool)					
FIPS 140-2 Certification					
E-SDK device tracker (MDM)					
SE Linux policies					
Enhanced PIM					
Enterprise Single sign on (SSO)					
Enterprise Home screen					
Automatic peripheral detect					

Mobile Device Management

Android for Work feature overview
Devices with Android 5.0 and higher support methods according to the table below.

	Can be called from regular (non owner) Device Admin	Can be called from a Device Owner	Can be called from a Profile Owner
Set network independent global HTTP proxy		Yes	
List installed user CA certificates	Yes	Yes	Yes
Uninstall all user CA certificates	Yes	Yes	Yes
Get CA certificate alias	Yes	Yes	Yes
Install certificate and private key pair		Yes	Yes
Allow screen capture		Yes	Yes
Allow network time required		Yes	
Add default application handler		Yes	Yes
Set application restrictions		Yes	Yes
Set TrustAgent (lock screen agent) features	Yes	Yes	Yes
Allow managed profile caller ID			Yes
Add cross profile application handler			Yes
Set permitted accessibility services		Yes	Yes
Set permitted input methods		Yes	Yes
Create/delete/switch user		Yes	
Allow modify accounts		Yes	Yes
Allow configure wifi		Yes	Yes
Allow install applications		Yes	Yes
Allow uninstallation of applications		Yes	Yes
Allow share location		Yes	Yes
Allow install from unknown sources		Yes	Yes
Allow configure bluetooth		Yes	Yes
Allow USB file transfer		Yes	Yes
Allow configure credentials		Yes	Yes
Allow remove user		Yes	Yes
Allow debugging features		Yes	Yes
Allow configure VPN		Yes	Yes
Allow configure tethering		Yes	Yes
Allow factory reset		Yes	Yes
Allow add user		Yes	Yes
Ensure verify applications		Yes	Yes
Allow configure cell broadcasts		Yes	Yes

	Can be called from regular (non owner) Device Admin	Can be called from a Device Owner	Can be called from a Profile Owner
Allow configure mobile networks		Yes	Yes
Allow application control		Yes	Yes
Allow mount physical media		Yes	Yes
Allow unmute microphone		Yes	Yes
Allow adjust volume		Yes	Yes
Allow outgoing calls		Yes	Yes
Allow incoming and outgoing SMS		Yes	Yes
Allow create windows		Yes	Yes
Allow cross profile copy and paste		Yes	Yes
Allow outgoing NFC		Yes	Yes
Set application hidden		Yes	Yes
Enable system application		Yes	Yes
Allow account management per account type			Yes
Set lock task		Yes	
Enable ADB		Yes	
Enable network time		Yes	
Enable network time zone		Yes	
Enable bluetooth		Yes	
Enable data roaming		Yes	
Enable development settings		Yes	
Set ringer mode		Yes	
Set network preference(s)		Yes	
Enable USB mass storage		Yes	
Enable wifi		Yes	
Enable wifi sleep policy		Yes	
Set default input method		Yes	Yes
Skip application first user hints		Yes	Yes
Set location mode accuracy		Yes	
Set administrator permission provider			Yes
Mute master volume		Yes	Yes
Block application uninstallations by user		Yes	Yes
Allow cross platform widget provider			Yes

Trademarks and acknowledgements

All product and company names mentioned herein are the trademarks or registered trademarks of their respective owners. Any rights not expressly granted herein are reserved. All other trademarks are property of their respective owners.

Visit www.sonymobile.com for more information.