SONY

Xperia™ in Business

Enterprise Mobility Management

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

October 2016

XPERIA

About this document

Products covered

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

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.

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.

Document release date

October 15, 2016

This White paper is published by:

Sony Mobile Communications Inc., 4–12–3 Higashi-Shinagawa, Shinagawa-ku, Tokyo, 140–0002, Japan

www.sonymobile.com

First released version (October 2016)

This document is published by Sony Mobile Communications Inc., without any warranty*. Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to programs and/or equipment may be made by Sony Mobile Communications Inc. at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Printed versions are to be regarded as temporary reference copies only.

*All implied warranties, including without limitation the implied warranties of merchantability or fitness for a particular purpose, are excluded. In no event shall Sony or its licensors be liable for incidental or consequential damages of any nature, including but not limited to lost profits or commercial loss, arising out of the use of the information in this document.

Contents

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 several options for device management that make it possible to manage both corporate-owned, and personal Xperia devices:

- Xperia Configurator, a free tool from Sony Mobile.
- The built-in Microsoft® Exchange ActiveSync® (EAS) client.
- The free ‘my Xperia’ service from Sony Mobile.
- Leading Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) third party solutions.

When integrated into an EMM- or 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 monitoring, and remote wiping and locking of devices.

Xperia™ Configurator

To address the needs of small and medium-sized businesses (SMBs) and Bring Your Own Device (BYOD) users, Sony has developed the Xperia Configurator. The Xperia Configurator is a free tool that lets you create, construct and deploy multiple configuration profiles on Xperia devices throughout your business. Xperia Configurator is available in a PC client version and a cloud version. They can be found at www.sonymobile.com/global-en/xperia/business/it-support/.

Xperia Configurator Cloud (XCC) is the cloud-based version of the configurator tool. It can be used to remotely create, configure and install configuration profiles over the air on one or more Xperia devices. The user interface of Xperia Configurator Cloud is accessible from the latest versions of most web browsers. The tool works with Xperia devices that have an activated Xperia Configurator Cloud account. To register an account and login, go to https://xperiaconfiguratorcloud.sonymobile.com.

By introducing over the air deployment of configuration files, instead of the USB approach common with alternative market solutions, the XCC platform makes mass-deployment and volume planning of your company’s devices easy and efficient. Another key characteristic of XCC, compared to similar tools available on the market, is the ability to have multiple administrators. If the organisation for example is present on multiple sites, local differences can be adjusted in the device configurations. XCC has the capability to set a tree structure consisting of a super user (account owner) and associated sub-layers of IT administrators. This means that large enterprises or even mobile operators can create unique configurations per company, per site, per department or any other applicable profile.

XCC allows the IT administrator to fully utilise the Sony Enterprise SDK, which in addition to standard Android™ APIs also includes a range of Sony Xperia specific device policies. These policies can be set remotely on all Xperia devices that has the XCC phone enabler installed.

XCC profiles support the following settings:

- General – Profile name and description.
- Password – Password settings and management.
- Restrictions – Restrict which device functions that can be used.
- Wi-Fi – Configure Wi-Fi network connections.
- VPN – Configure a network connection via VPN.
- Email – Select which email account(s) to use for the device.
- Exchange ActiveSync – Set Exchange server connections via Exchange ActiveSync.
- Single Sign on – Configure a Single sign on account.
- Digital certificates – Import and add digital certificates for the device.
- Security & Privacy – Set the security and privacy settings on the device.
- Applications – Select which applications (APK files) and external apps to install on the device.
- Shortcuts – Add home screen shortcuts on the device.

Microsoft® 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. See the Product overview White paper for details about supported policies and 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 all data and configurations on a device.

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.

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.

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)

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.

Android™ for Work

Android for Work introduces the concept of a Device Owner and Profile Owner to support the corporate owned and Bring Your Own Device (BYOD) enterprise use cases, respectively. It is a solution that creates a managed profile (the Work 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.

The Profile Owner is a special case of a device administrator, who can only manage the corporate space on a user's personal device to support the BYOD use case. The user can easily access both the personal and the Work Profile. The Profile Owner can't be deactivated by the user; however, the user is always able to view and validate the settings being enforced within the Work Profile. The user can choose to remove the Work Profile and the Profile Owner from the device whenever they desire.

A Device Owner is like a Profile Owner, but scoped to the whole device. The Device Owner is the device administrator in the corporate-owned device use case.

Installation of applications within the Work Profile is possible via Google Play for Work in the Work Profile. Applications can either be downloaded and installed manually from the managed Play Store app (pull), or installed automatically as a result of an action from an EMM/MDM (push). When the user opens the Play Store app in the Work Profile, it only displays the apps which the IT administrator has specified the user can access. The user can install these applications, but not any others.

Android for Work lets the administrator set policies on a per-application basis, where the app developer has made this available. For example, an app could allow an IT administrator to remotely control the availability of features, configure settings, or set in-app credentials. The setApplicationRestrictions method allows EMMs to configure these restrictions via the DevicePolicyManager class. Google Chrome™ is an example of an enterprise-managed app that implements policies and configurations that can be fully managed according to enterprise policies and restrictions.

Android for Work features:

- Profile management – The Work Profile separates and protects work data from personal apps and content. Business data is secured with hardware-based encryption and sharing restrictions.
- Data leakage prevention – Admins can apply policies to restrict the flow of data and prevent information from being shared.
- Device management – Companies can apply management to an entire device with Work Managed Device capabilities.
- Remote wipe of business data – Work apps and data can be remotely wiped without affecting personal apps and content.
- Google Play for Work – Business apps are securely deployed and managed via Google Play for Work.
- Unknown sources – Admins can block app downloads from third-party marketplaces.
- VPN – Secure networking can be applied to the device, Work Profile or specific business apps.
- Deploy Google Play apps – Apps can be deployed to the Work Profile or Work Managed Devices without wrapping through Google Play for Work.
- Approve work apps – IT can define approved business applications that users can download from the Google Play for Work app.
- Securely distribute internal apps – Companies can privately distribute internally developed apps through Google Play for Work, self-hosted or hosted by Google.