SONY

Xperia™ in Business
Mobile Device Management

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

Device management clients

Exchange® ActiveSync®

The my Xperia service

Third party Mobile Device Management solutions

Device inventory

Dual persona

Xperia™ Z1
Xperia™ Z1 Compact
Xperia™ Z Ultra

This White paper is published by:

Sony Mobile Communications AB,
SE-221 88 Lund, Sweden

www.sonymobile.com

First released version (January 2014)

Products covered

The services and features described in this document require the following combination of products and software versions:

Xperia™ Z1
Software version (build number): 14.2.A.0.xxx

Xperia™ Z1 Compact
Software version (build number): 14.2.A.0.xxx

Xperia™ Z Ultra
Software version (build number): 14.2.A.0.xxx

Android version: 4.3.x

Note: xxx in software versions denotes a 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

January 10, 2014

Mobile Device Management

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

Passcode policies supported:
- Password recovery enabled
- Require password
- Allow simple password
- Min password length
- Min password complex characters
- Require alphanumeric password
- Max password failed attempts
- Restrict password history
- Password expiration timeout
- Max inactivity time lock

Device policies supported:
- Allow Wi-Fi®
- Allow Bluetooth™
- Allow storage card
- Allow browser
- Allow tethering
- Allow desktop sync
- Application blacklist/whitelist
- Require storage card encryption
- Allow roaming
- Require device encryption
- Allow camera
- Allow / Block / Quarantine (ABQ) list
- Unapproved in ROM application list

Device commands supported:
- Add EAS account
- VPN configuration
- Track data usage
- Wipe storage card only
- Get rooting status
- Prompt new password
- Lock device
- Wipe device
- Locate device
- Sound an alert

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)

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

Inventory management features supported:

Device information
- Hardware inventory (Manufacturer, Device model, Device features, Serial number, IMEI)
- Operating software inventory (OS version, Kernel version, Baseband version, Software build number)

Apps information
- Installed apps
- App information (ID, name, version, content, resources)
- Individual app usage
- Running apps
- Running services

Network information
- Subscriber ID
- Phone number
- SIM card ID (ICCID)
- Subscriber carrier network
- Current carrier network
- Data roaming setting (on/off)
- Wi-Fi information (SSID, MAC and IP addresses)
- Proxy hostname and port
- Bluetooth information (ID, MAC address, paired devices)

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.

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, reboot the device, or reset it to its factory settings. You can also remotely remove or disable individual applications on devices.

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.

Mobile Device Management

The Dual persona support on Sony Xperia™ devices enables:

- Separation of personal and corporate data
- A dedicated workspace for corporate applications and data
- Increased mobile device security by isolation of corporate assets from personal assets
- Full access to enterprise services for employees on the go

Dual persona

Xperia™ devices from Sony are VMware® Ready and can be used with the VMware Horizon Mobile virtualisation software to enable dual personas. After installing the VMware Switch client, the device can run a corporate workspace that is controlled and managed by the IT department. This workspace is completely separate from the employee's personal information, applications and data on the device.

The dual persona approach gives full control over corporate data on personally owned or corporate-owned mobile devices, without the need to unnecessarily manage the entire device. The personal and the corporate personas run securely and simultaneously but in isolation from each other. Each persona is a complete mobile workspace with its own set of applications and policies. Corporate data on the device remains under IT control. At the same time, employees retain the freedom to use their devices as they see fit—with the privacy of their personal information intact.

The enterprise mobile workspace can be easily controlled and customised. IT administrators can quickly and easily provision pre-configured applications and enterprise services over the air to employee devices through a dedicated workspace. Native application support within the corporate workspace enables any application file package, including ones developed in-house, to be deployed to an employee's corporate workspace without modification.

Trademarks and acknowledgements

Visit www.sonymobile.com for more information.