SONY

Xperia™ dans l’entreprise : Guide de démarrage rapide

Découvrez comment mobiliser votre force de travail et comment déployer et gérer les smartphones et tablettes de Sony Mobile dans votre entreprise.

XPERIA

À propos de ce document

Ce guide Xperia™ dans l'entreprise décrit les services et fonctions professionnels que Sony Mobile propose dans sa gamme d'appareils Xperia. Pour obtenir des renseignements plus précis à propos des produits et des versions logicielles pris en charge, rendez-vous sur www.sonymobile.com/global-en/xperia/business/it-support/.

Limitations des services et fonctions

Il est possible que certains services et fonctions décrits dans ce document ne soient pas pris en charge dans tous les pays/régions ou par tous les réseaux et/ou opérateurs réseau dans toutes les régions. Veuillez contacter votre opérateur réseau ou votre fournisseur de services pour savoir si un service ou une fonction spécifiques sont utilisables et si des frais supplémentaires d'accès ou d'utilisation sont susceptibles de s'appliquer.

Limitations légales

Ce document fournit des informations générales à propos du développement d'une infrastructure informatique mobile d'entreprise. C'est un outil permettant d'aider votre entreprise à commencer à évaluer ses besoins. Il n'est pas destiné à être un guide unique pour le développement d'une infrastructure informatique mobile, il ne remplace pas le besoin d'avis de professionnels qualifiés, et il n'est en aucune manière conçu pour répondre aux besoins spécifiques de votre entreprise. Sony Mobile peut actualiser ce document à tout moment, sans notification préalable. Ce document et son contenu sont fournis « en l'état », son utilisation est par conséquent à vos propres risques. Sony Mobile décline expressément toutes garanties, expresses, implicites, statutaires ou autres. En continuant à lire et à apprécier ce document, vous convenez que Sony Mobile ne sera jamais responsable de tous dommages directs, indirects, spéciaux, consécutifs, ou punitifs, perte, ou préjudice que vous pourriez subir (y compris la perte de données, d'usage, de profits, et/ou d'opportunité commerciale), que Sony Mobile ait ou non été avisé et informé de la possibilité de ces dommages, perte ou préjudice.

Date de publication du document

1er décembre 2015.

Ce document est publié par :
Sony Mobile Communications Inc.,
1-8-15 Konan, Minato-ku, Tokyo 108-0075, Japon

www.sonymobile.com

Première version publiée (décembre 2015)

Révision 1.0

Introduction

Le fait d'équiper votre force de travail d'appareils portables présente de nombreux avantages. Grâce à la configuration « Bring Your Own device (BYOD) », les employés obtiennent les moyens d'accéder aux systèmes et données de l'entreprise sur les appareils portables, et cela peut accroître la productivité. Toutefois, la mobilité de la force de travail est synonyme de défis pour le service informatique en termes de :

- Sécurité des informations et du système afin d'empêcher les « fuites » ou les accès non autorisés ;
- Le contrôle des coûts pour connaître et limiter les coûts des appels, des SMS et du trafic des données ;
- Le déploiement et la gestion des appareils et des solutions BYOD ;
- l'assistance aux utilisateurs des appareils portables, à la fois sur et hors du site.

Le déploiement et la gestion des smartphones et tablettes Xperia dans votre entreprise sont facilités grâce à une combinaison de solutions de développement de Sony Mobile et de solutions de gestion des appareils portables de tiers leaders.

Ce document donne des conseils et recommandations aux services informatiques en ce qui concerne les considérations majeures que les entreprises doivent garder à l'esprit lorsqu'elles mettent en œuvre une stratégie de mobilité. Les thèmes suivants sont couverts :

- **Stratégie et politique de la mobilité**
- **Infrastructure**
- **Déploiement**
- **Configuration Wi-Fi des appareils**
- **Sécurité**
- **Synchronisation des courriels, du calendrier, et des contacts professionnels**
- **Gestion des appareils Xperia**

En résumé, il existe 10 bonnes pratiques qui vous permettront de prendre en mains Xperia dans l'entreprise :

1. Créer une politique de mobilité et vérifier qu'elle est bien connue et observée dans l'entreprise ;
2. Décider si les appareils sont fournis par l'entreprise, choisis d'après une liste de modèles approuvés, ou achetés par les employés ;
3. Avoir la possibilité de bloquer et d'effacer rapidement les appareils perdus ou volés ;
4. Être en mesure de forcer les verrouillages d'écran, identifiants de connexion sûrs et changement de mots de passe robustes sur tous les appareils portables ;
5. Activer le cryptage côté appareil ;
6. Décider des applications ou services que les utilisateurs ne sont pas autoriser à installer ou à utiliser ;
7. Maintenir les appareils et serveurs à niveau avec les toutes dernières mises à niveau et les tous derniers correctifs du logiciel ;
8. Pouvoir suivre et sécuriser les données sensibles ;
9. Garantir qu'il est possible de surveiller l'usage des applications et le trafic du réseau ;
10. Garantir qu'une assistance est disponible pour les utilisateurs des appareils portables.

Stratégie et politique de la mobilité

Votre entreprise a besoin d'une stratégie de mobilité alignée avec la stratégie globale de l'entreprise ; si ce n'est pas le cas, elle n'apportera pas de valeur à votre entreprise. Vous devez définir quelles sont les applications et services que vous souhaitez rendre disponibles sur les appareils portables des utilisateurs, et pourquoi ; par conséquent, comprendre les scénarios que votre force de travail pourra consulter sur les appareils portables est un facteur clé du succès.

Vous devez évaluer les possibilités et les risques, puis créer une politique de mobilité pour les appareils BYOD et ceux appartenant à l'entreprise, selon votre configuration. Chaque entreprise doit définir les impératifs de sécurité, les problèmes de confidentialité et juridiques, puis créer une politique et des contrôles formels. Il faut également un plan de formation afin que les utilisateurs sachent à quoi s'attendre en termes d'obligations de sécurité, confidentialité et finances, ainsi qu'en termes d'assistance.

Contenu et objectifs de votre politique de mobilité

Le contenu sera différent pour chaque entreprise, selon divers facteurs, mais toutes les politiques de mobilité doivent contenir des sections qui traitent les éléments suivants :

- Spécifications de l'appareil ;
- Usage et accès aux appareils ;
- Applications ;
- Accès aux données organisationnelles ;
- Contrôles de sécurité obligatoires ;
- Termes financiers ;
- Responsabilité et confidentialité ;
- Sanctions en cas de non-conformité.

La politique de mobilité doit contenir une déclaration qui explique son rôle, son champs d'application et ses objectifs. Les objectifs de la politique pourraient consister à :

- Améliorer l'équilibre travail-vie personnelle ;
- Supporter le travail collaboratif ;
- Suppléer la productivité de l'entreprise ;
- Améliorer la gestion des coûts de la mobilité ;
- Améliorer la sécurité des données.

La politique devra stipuler des appareils approuvés et des niveaux d'assistance à aligner avec les différents appareils. Les appareils BYOD devront également être pris en compte (le cas échéant). La politique devra également stipuler quels sont les appareils que l'entreprise prendra en charge, selon les exigences en matière de sécurité, comme la prise en charge des numéros d'identification personnels (NIP), des verrouillages codés, du verrouillage automatique, du cryptage et de l'effacement à distance.

Accès aux applications et aux données

Cette section de la politique devra également détailler le niveau d'accès aux applications critiques. Il faudra répondre aux questions suivantes pour déterminer le niveau d'accès :

- Quelles sont les données auxquelles le personnel peut accéder depuis les appareils portables ?
- Quelles sont les exigences de sécurité à mettre en œuvre pour les appareils qui appartiennent aux employés ?
- Quel est le niveau d'assistance que le personnel peut attendre du service informatique ?
- Faut-il uniquement prendre en charge les applications logicielles organisationnelles ?
- Quelles solutions de gestion faut-il utiliser pour sécuriser et gérer les données organisationnelles accessibles dans un environnement BYOD ?

La politique peut stipuler que tous les appareils peuvent télécharger un logiciel approuvé depuis un portail spécifié ou que les applications logicielles doivent figurer sur une liste approuvée par l'entreprise. Toutes les autres applications peuvent exiger l'approbation du comité de la politique de mobilité. La politique peut également stipuler que l'entreprise ne prendra pas en charge les logiciels ajoutés par les utilisateurs.

Impératifs de sécurité

Pour la majorité des entreprises, la sécurité de la mobilité est essentielle. Cela est plus particulièrement vrai pour les appareils qui appartiennent au personnel. Par conséquent, la section « Sécurité » de la politique de mobilité doit être très détaillée. Les facteurs de sécurité qui doivent être pris en compte sont les suivants :

- Exigences en matière de mots de passe ;
- Cryptage des données ;
- Authentification de l'appareil ;
- Réseaux privés virtuels (VPN) ;
- Niveau d'effacement des données sur les appareils (total ou sélectif).

S'il vous sera possible d'effacer à distance les données des appareils perdus ou volés, précisez si vous effacerez toutes les données (y compris les données personnelles) ou si vous utiliserez une approche « bac à sable » qui sépare les données professionnelles des données personnelles, supprimant uniquement les informations de l'entreprise.

Questions de confidentialité et de responsabilité

Dans la majorité des politiques de mobilité, plus particulièrement dans les cas où les employés utilisent leurs propres appareils, il est important de concilier les questions de vie privée et de responsabilité et de créer un système qui minimise l'exposition des informations personnelles. La politique de confidentialité et les déclarations de responsabilité stipulent en règle générale les éléments suivants :

- L'entreprise n'assumera aucune responsabilité en ce qui concerne les appareils personnels ;
- L'entreprise ne tentera pas d'accéder aux informations privées de l'employé, mais pourrait le faire accidentellement ;

- Les membres du personnel sont personnellement responsables des frais de résiliation anticipés associés aux contrats et aux appareils portables personnels appartenant aux employés, s'ils choisissent de résilier leurs contrats avant la date de résiliation prévue.

Assistance aux utilisateurs des appareils portables

Les utilisateurs des appareils portables ont des besoins d'assistance différents de ceux des utilisateurs d'un ordinateur ordinaire. Pour déterminer un niveau d'assistance approprié, tenez compte des questions suivantes :

- Le service informatique assistera-t-il à la configuration initiale de l'appareil ?
- Le service informatique fournira-t-il une assistance de premier ou de second niveau ?
- Tous les appareils seront-ils pris en charge ?
- Quel est le niveau d'assistance pour les appareils qui appartiennent aux employés ?
- Les données et applications organisationnelles seront-elles seules prises en charge ?
- Comment l'appareil sera-t-il géré ?
- L'appareil sera-t-il entretenu sur les ondes hertziennes ou par synchronisation avec un ordinateur ou une application web ?
- Comment l'appareil sera-t-il sécurisé ? À l'aide de mots de passe, cryptage de l'appareil, verrouillage à distance, effacement et placement dans un « bac à sable », par exemple ?

Infrastructure

Avant de mettre en œuvre votre stratégie de mobilité, vous devez analyser les capacités techniques de l'infrastructure existante de votre entreprise. L'objectif de cette analyse est de comprendre si les exigences nécessaires sont déjà en place ou si certaines des technologies suivantes doivent être introduites ou mises à niveau :

- Accès au réseau ;
- Serveurs pour les courriels et autres applications ;
- Serveurs de réseaux privés virtuels (VPN).

Accès au réseau

Les appareils portables dépendent des connexions réseau sans fil ; par conséquent, un réseau Wi-Fi® bien conçu est essentiel. Lorsqu'il s'agit de la conception d'un réseau sans fil, vous devez tenir compte de trois problèmes principaux :

- **Couverture** – Les régions dans lesquelles mes utilisateurs auront besoin d'un accès sans fil sont-elles couvertes ?
- **Capacité** – Le débit aux points d'accès dans toute région donnée est-il suffisant pour prendre en charge mes utilisateurs ? Les points d'accès sont un support partagé ; par conséquent, plus nombreux sont les utilisateurs connectés, moins rapide est la vitesse qu'ils obtiennent.
- **Performance** – La distance entre les points d'accès est-elle optimale pour les appareils et applications que j'emploie ?

Lorsque la planification sera terminée, il faudra mettre en place l'alimentation et la configuration du réseau sans fil (et probablement celles du réseau câblé). Il faudra également prévoir de devoir éventuellement reconfigurer les routeurs, commutateurs et pare-feux du réseau existant, ainsi que les éléments du réseau sans fil, afin de pouvoir prendre en charge l'infrastructure mobile souhaitée.

Voici quelques exemples de fonctions de votre solution sans fil qui fournissent une bonne plateforme pour les appareils portables :

- Gestion centralisée ;
- Pare-feu intégré ;
- Intégration des services d'annuaire ;
- Visibilité de la couche 7 (couche d'application) ;
- Analyse du spectre ;
- Création d'une empreinte numérique pour l'application, l'appareil, et la version du système d'exploitation ;
- Haute capacité de l'équilibrage de charge ;
- Capacité d'ajuster les paramètres des canaux et de la puissance en temps réel ;
- Extensibilité ;
- Possibilité de communiquer avec des appareils de 2,4 et 5 GHz ;
- Visibilité du réseau sans fil en temps réel ;
- Définition des priorités de la qualité du service/application ;
- Redondance.

Les utilisateurs peuvent configurer leurs appareils afin qu'ils se connectent automatiquement sur les réseaux Wi-Fi disponibles. Il est possible d'accéder aux réseaux Wi-Fi qui exigent des informations d'identification de connexion ou d'autres informations depuis les paramètres Wi-Fi ou automatiquement configurés à l'aide de profils de configuration. Vous pouvez configurer les paramètres des réseaux sans fil, de sécurité, de proxy et d'authentification à l'aide des profils de configuration activés vers un appareil au moyen du service Xperia Configurator (décrit ultérieurement dans ce document), d'un logiciel tiers de gestion des appareils portables (GAP) ou de gestion de la mobilité d'entreprise (GME).

Serveurs pour les courriels et autres applications

Les appareils Xperia prennent en charge les normes de l'industrie pour la configuration de l'accès aux services des courriels, du calendrier, et des contacts professionnels. Avec l'assistance complète de Microsoft® Exchange ActiveSync®, la synchronisation avec Microsoft® Outlook® et Exchange Servers est facile. Vous devez vérifier que le service ActiveSync® est à niveau et configuré pour prendre en charge tous les utilisateurs du réseau. Vous devez également vérifier que vous avez suffisamment de licences pour connecter des clients, et vous devez préparer votre réseau :

- Vérifiez que le port 443 est ouvert sur votre pare-feu. Si votre entreprise utilise Outlook Web Access, le port 443 est probablement déjà ouvert. Il est possible d'utiliser d'autres numéros de port, mais le 443 est le port par défaut pour SSL ;
- Vérifiez que le serveur Domain Name System (DNS) de votre réseau retourne une adresse unique extérieurement routable au serveur Exchange ActiveSync® pour les clients Intranet et Internet, afin d'autoriser l'appareil portable à utiliser la même adresse IP pour communiquer avec le serveur lorsque les deux types de connexions sont actifs ;
- Vérifiez qu'un certificat de serveur est installé sur le serveur d'accès au client et que les services IIS sont assignés au certificat. Dans les propriétés d'authentification du répertoire virtuel ActiveSync®, confirmez que SSL et l'authentification de base (seulement) sont activés.

Si vous n'utilisez pas Microsoft® Exchange ActiveSync®, il est également possible d'utiliser les appareils Xperia avec la majorité des autres serveurs standard, y compris IMAP, POP, SMTP, ainsi que tous services de Google™.

Serveur VPN

Indépendamment du serveur VPN que vous utilisez, vous devez configurer votre pare-feu afin d'autoriser le trafic VPN. Cela signifie d'autoriser les protocoles VPN que vous utiliserez à traverser le pare-feu. Ces protocoles comprennent normalement :

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Secure Socket Layer (SSL)

Vérifiez la documentation de votre VPN pour savoir quels sont les ports que vous devez ouvrir. Les VPN SSL utilisent généralement le port 443, qui est le port habituel pour les serveurs Web protégés par SSL, ce port devrait donc être déjà ouvert.

Il est important de suivre les bonnes pratiques en matière de sécurité lorsque vous configurez votre serveur VPN. Voici quelques recommandations :

- Utilisez des méthodes d'authentification qui fournissent une sécurité appropriée, par exemple : Extensible Authentication Protocol-Transport Level Security (EAP-TLS) ;
- Envisagez d'exiger que vos clients VPN distants s'identifient en utilisant plusieurs protocoles d'authentification sécurisés, comme EAP, plutôt que de leur permettre d'utiliser des protocoles comme Password Authentication Protocol (PAP) ou Challenge Handshake Authentication Protocol (CHAP) ;
- Les connexions Layer Two Tunneling Protocol (L2TP) sur Internet Protocol security (IPsec) sont recommandées pour le cryptage le plus robuste ;
- Mettez en œuvre et imposez une politique de mot de passe robuste afin de réduire le risque d'attaque par dictionnaire.

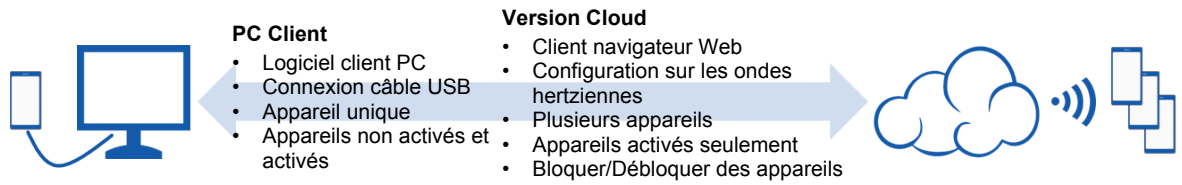
Déploiement

Le déploiement et la gestion des smartphones et tablettes Xperia exécutés sur Android™ dans votre entreprise sont facilités grâce à une combinaison de solutions de développement de Sony Mobile et de solutions de gestion des appareils portables (GAP) ou de gestion de la mobilité d'entreprise (GME) de tiers leaders. Il existe un grand choix de solutions GAP et GME disponibles pour prendre en charge différentes plateformes de serveur. Chaque solution propose différentes consoles et fonctions de gestion. Une solution GAP permet la distribution, la gestion et la configuration des politiques et des applications. Outre la gestion des appareils portables, une solution GME fournit également la gestion d'applications mobiles et la gestion de contenus mobiles. Vous trouverez des informations supplémentaires à propos des politiques et fonctions prises en charge dans les livres blancs Xperia dans l'entreprise à l'adresse suivante : http://www.sonymobile.com/global-en/xperia/business/it-support/.

Xperia Configurator

Outre les solutions GAP et GME de tiers, Sony propose Xperia Configurator. C'est un outil gratuit qui vous permet de configurer et de déployer facilement plusieurs appareils dans votre entreprise. C'est le compagnon professionnel parfait, car il vous permet de créer, construire et installer des profils de configuration sur les appareils Sony Mobile, y compris les smartphones et les tablettes. Xperia Configurator est disponible en version PC client et en version Cloud que vous trouverez à l'adresse suivante : http://www.sonymobile.com/global-en/xperia/business/it-support/.

Xperia Configurator Cloud est une version de l'outil de configuration basée sur le Cloud que vous pouvez utiliser pour créer, configurer et installer des profils de configuration sur les ondes hertziennes pour un groupe d'appareils de Sony Mobile. L'interface utilisateur de Xperia Configurator Cloud est accessible depuis un navigateur Internet, l'outil fonctionne avec les appareils Xperia qui ont un compte Xperia Configurator Cloud activé.



Gestion des appareils portables (GAP) et Gestion de la mobilité d'entreprise (GME)

Bien que l'assistance pour la gestion et la configuration de base puissent être les premières étapes pour les administrateurs des services informatiques, la recherche d'une plateforme GAP ou GME qui prend en charge la gestion au niveau de l'application, le partage des fichiers mobiles, la navigation sécurisée, les courriels sécurisés et autres possibilités est essentielle pour garantir une assistance pour de futures intégrations mobiles dans l'environnement de l'entreprise. Une solution GAP/GME donne à votre entreprise la possibilité d'inscrire en toute sécurité des appareils dans l'environnement de l'entreprise, de configurer sans fil et de mettre à jour les paramètres, de surveiller l'observance de la politique, de déployer des applications, et d'effacer ou de bloquer à distance les appareils gérés.

Configuration Wi-Fi des appareils

Vous devez régler les paramètres de sécurité de votre appareil de façon à correspondre à la méthode d'authentification et de cryptage utilisée par votre routeur Wi-Fi. Certaines connexions Wi-Fi sécurisées exigent soit une authentification du serveur, soit une authentification mutuelle. Afin de pouvoir utiliser ces connexions, vous devez acquérir et installer les fichiers de certificat sur l'appareil. Vous pouvez configurer les paramètres Wi-Fi et installer les certificats manuellement, à l'aide de Xperia Configurator ou d'une solution GAP/GME d'un tiers. Vous devrez configurer différents paramètres en fonction de l'installation Wi-Fi :

Paramètre	Ouvert	WEP	WPA	EAP-PEAP	EAP-TLS	EAP-TTLS	EAP-PWD	EAP-SIM	EAP-AKA
SSID réseau	X	X	X	X	X	X	X	X	X
Utiliser IP statique	X	X	X	X	X	X	X	X	X
Clé WEP		X							
Clé prépartagée			X						
Mot de passe EAP				X		X	X		
Seconde phase EAP				X		X			
Certificat CA				X	X	X			
Certificat client					X				
Identité				X	X	X	X		
Identité anonyme				X		X			

Vous trouverez ci-après une brève explication des types d'installation Wi-Fi que vous pouvez choisir :

- **Ouverte** – Pas de protocoles de cryptage.
- **WEP** – Wired Equivalent Privacy est une norme obsolète. Elle n'est pas recommandée pour les réseaux sécurisés.
- **WPA (WPA2 PSK)** – Wi-Fi Protected Access II Pre-Shared Key est conçu pour les réseaux domestiques et les petites entreprises et n'exige aucun serveur d'authentification.
- **EAP-PEAP** – Extensible Authentication Protocol-Protected Extensible Authentication Protocol encapsule EAP dans un tunnel Transport Layer Security (TLS) potentiellement crypté et authentifié.
- **EAP-TLS** – EAP-Transport Layer Security exige un certificat côté client pour fournir sa puissance d'authentification.
- **EAP-TTLS** – EAP-Tunnelled Transport Layer Security est un protocole EAP qui étend TLS. Le client peut, mais ne doit pas être obligatoirement authentifié au moyen d'un certificatPKI signé CA vers le serveur. Cela simplifie considérablement la procédure d'installation, car aucun certificat n'est nécessaire pour chaque client.
- **EAP-PWD** – EAP-Password est une méthode qui utilise un mot de passe partagé pour l'authentification.
- **EAP-SIM** – Utilise la carte SIM de l'appareil pour fournir une authentification mutuelle entre le client et le réseau. La communication entre la carte SIM et le centre d'authentification remplace le besoin d'un mot de passe prédéfini.
- **EAP-AKA** – EAP-Authentication and Key Agreement est un mécanisme pour l'authentification et la distribution de la clé de session en utilisant UMTS Subscriber Identity Module (USIM).

Sécurité

De l'avis d'un administrateur des services informatiques, la sécurité des appareils portables utilisés sur le terrain couvre trois domaines principaux :

- **Sécurité de l'appareil** – Protection de l'accès (mots de passe, codes NIP, modèles de déverrouillage d'écran, etc.).
- **Stockage sécurisé** – Cryptage des données et outils permettant de rechercher, bloquer et effacer un appareil perdu.
- **Sécurité du réseau** – Communication sécurisée au moyen de connexions VPN.
- **Certificats numériques** – Authentification et autorisation des utilisateurs.

Protection de l'accès

Votre politique de mobilité doit obliger l'utilisateur à appliquer la sécurité du mot de passe sur l'appareil. Utilisez Xperia Configurator ou la solution GAP/GME d'un tiers pour appliquer les paramètres qui répondent à vos besoins en matière de sécurité :

- **Autoriser un mot de passe simple** – Permettre la définition d'un mot de passe simple sur l'appareil.
- **Historique du mot de passe** – Définir le nombre d'entrées à retenir dans l'historique du mot de passe. Cela empêche l'utilisateur de réutiliser ces mots de passe.
- **Qualité du mot de passe** – Définir la qualité requise pour les mots de passe sur l'appareil :
    - **Non spécifiée** – Aucunes restrictions sur la qualité du mot de passe ne seront définies.
    - **Reconnaissance faciale** – L'option « Reconnaissance faciale » est le plus faible niveau de sécurité de la méthode de déverrouillage du téléphone qui peut être utilisé sur l'appareil (un NIP, un modèle ou un mot de passe alphanumérique sont également autorisés).
      Remarque ! La fonction « Reconnaissance faciale » nécessite un appareil Xperia avec la version Android 4.0 ou ultérieure, équipé d'une caméra avant.
    - **Quelque chose** – Un mot de passe doit être défini, mais aucunes restrictions du mot de passe ne sont appliquées.
    - **Numérique** – Les mots de passe qui comportent des caractères numériques, alphabétiques et spéciaux sont autorisés.
    - **Alphabétique** – Les mots de passe qui comportent des caractères alphabétiques, numériques et spéciaux sont autorisés.
    - **Alphanumérique** – Le mot de passe doit comporter des caractères alphabétiques et numériques.
    - **Complexe** – Le mot de passe doit satisfaire les exigences de complexité prédéfinies. Vous pouvez définir le nombre minimal (0 à 5) de caractères complexes requis.
- **Longueur minimale du mot de passe** – Définissez la longueur minimale du mot de passe dans une plage de 4 à 16 caractères.
- **Durée maximale avant le verrouillage automatique** – Définissez un intervalle de temps (de 15 secondes à 10 minutes) pour retarder le verrouillage automatique de l'appareil. Vous pouvez également définir aucune limite de temps.

Cryptage

Un mot de passe robuste combiné à un cryptage efficace garantit la protection robuste des données sensibles stockées sur les appareils Xperia, cela permet de bloquer et d'effacer à distance le contenu d'un appareil perdu afin de protéger les informations sensibles.

Il est possible de crypter les données de l'appareil, afin de garantir quel seul un utilisateur possédant la clé correcte puisse les lire, et que seul un mot de passe permette d'accéder aux données. Les appareils Xperia proposent un cryptage complet de toutes les données de l'utilisateur dans la mémoire interne (mémoire de l'appareil et stockage interne), ainsi que sur toute carte mémoire externe. Cela signifie que toutes les données enregistrées par et vers les applications (par exemple, messages, pièces jointes et contacts professionnels) sont protégées contre un accès non autorisé.

Avertissement ! Le cryptage est irréversible. Le seul moyen de retourner à un appareil en état non crypté est d'effectuer une réinitialisation aux données d'usine, ce qui efface toutes les données de l'appareil. Si l'utilisateur oublie le NIP numérique ou le mot de passe, ou s'il souhaite annuler le cryptage de l'appareil, il devra effectuer une réinitialisation aux données d'usine de la mémoire interne. Toute carte mémoire externe cryptée devra également être formatée.

Toutefois, si vous avez votre NIP et votre mot de passe et souhaitez annuler le cryptage de votre appareil, vous pouvez conserver les informations stockées sur votre appareil Xperia en les copiant sur un ordinateur. Vous devrez ensuite effectuer une réinitialisation aux données d'usine de la mémoire interne (mémoire de l'appareil et stockage interne) de l'appareil Xperia et effacer la carte mémoire externe. Après avoir effectué la réinitialisation de l'appareil Xperia et le formatage de la carte mémoire externe, vous pourrez recopier les informations sur votre appareil Xperia et sur la carte mémoire.

Le cryptage peut être activé sur l'appareil par l'utilisateur, ou il peut être imposé par le service informatique de votre entreprise au moyen de Microsoft® Exchange ActiveSync® (EAS) ou de solutions GAP/GME. Vous pouvez également utiliser les profils créés à l'aide de Xperia Configurator pour imposer le cryptage.

Pour crypter manuellement les informations sur un appareil

Avertissement ! Si vous interrompez le processus de cryptage, vous perdrez toutes les données de l'appareil !

1. Depuis l'écran d'accueil, tapez sur l'icône de l'écran Application.
2. Recherchez et tapez sur **Paramètres**.
3. Tapez sur **Sécurité** > **Crypter le téléphone**. L'option **Crypter le téléphone** n'est pas disponible si l'appareil n'est pas suffisamment chargé et si votre appareil n'est pas branché sur un chargeur.
4. Si vous souhaitez crypter le contenu de la carte mémoire externe, cochez la case **Crypter la carte SD**.
5. Tapez sur **Suivant**.
6. Entrez le NIP ou le mot de passe de l'écran de verrouillage, puis tapez sur **OK**.
7. Tapez sur **Crypter**. Le processus de cryptage démarre et peut durer au moins une heure. Il est possible que l'appareil redémarre plusieurs fois pendant le processus.

Connexions VPN

Les appareils Xperia contiennent un client VPN qui fournit une connexion distante sûre aux serveurs de votre entreprise, à l'aide de protocoles standard de l'industrie et de l'authentification de l'utilisateur. Les connexions VPN peuvent être configurées de nombreuses manières, selon le réseau. Certains réseaux peuvent exiger l'installation d'un certificat de sécurité sur l'appareil avant d'autoriser l'accès.

Les connexions VPN peuvent être soit configurées manuellement sur l'appareil, à l'aide de Xperia Configurator, ou en utilisant une solution GAP/GME d'un tiers. Après avoir sélectionné un **nom de connexion** et un **type VPN**, vous devrez configurer la connexion. Vous devrez configurer différents paramètres en fonction du type VPN :

Paramètre	PPTP	L2TP/IPSec PSK	L2TP/IPSec RSA	L2TP/IPSec Xauth PSK	L2TP/IPSec Xauth RSA	L2TP/IPSec Hybrid RSA
Serveur VPN	X	X	X	X	X	X
Nom d'utilisateur	X	X	X	X	X	X
Mot de passe de l'utilisateur	X	X	X	X	X	X
Domaine de recherche DNS	X	X	X	X	X	X
Serveurs DNS	X	X	X	X	X	X
Itinéraires de transfert	X	X	X	X	X	X
Cryptage activé	X					
Secret L2TP		X	X			
Identificateur IPSec		X		X		
Clé de l'utilisateur prépartagée		X		X		
Certificat de l'utilisateur			X		X	
Certificat CA			X		X	X
Certificat du serveur			X		X	X

Voici une courte explication des paramètres :

- **Nom de connexion** – Un nom de compte VPN qui sera affiché sur l'appareil.
- **Type VPN** – Le type de connexion VPN.
- **Serveur VPN** – Le nom d'hôte ou l'adresse IP du serveur VPN.
- **Nom d'utilisateur** – Nom d'utilisateur pour la certification de la connexion.
- **Mot de passe de l'utilisateur** – Mot de passe de l'utilisateur pour la certification de la connexion.
- **Domaine de recherche DNS** – Le domaine de recherche DNS pour la certification de la connexion.
- **Serveurs DNS** – Les noms d'hôte ou adresses IP des serveurs DNS.
- **Itinéraires de transfert** – Les itinéraires de transfert internes.
- **Cryptage activé** – Case à cocher qui vous permet d'activer le cryptage.
- **Secret L2TP** – Le secret L2TP pour la certification de la connexion.
- **Identificateur IPSec** – Définissez l'identificateur IPSec.
- **Clé de l'utilisateur prépartagée** – La clé de l'utilisateur prépartagée pour l'authentification.
- **Certificat de l'utilisateur** – Sélectionnez un certificat à utiliser.
- **Certificat CA** – Sélectionnez un certificat CA à utiliser.
- **Certificat du serveur** – Sélectionnez un certificat de serveur à utiliser.

Pour ajouter manuellement un VPN sur un appareil Xperia

1. Depuis l'écran d'accueil, tapez sur l'icône de l'écran Application.
2. Recherchez et tapez sur **Paramètres** > **Plus…** > **VPN**.
3. Si vous y êtes invité, entrez un mot de passe pour le stockage des identifiants.
4. Tapez sur l'icône « Plus ».
5. Pour afficher plus d'options, cochez la case **Afficher les options avancées**.
6. Sélectionnez le type de VPN à ajouter.
7. Saisissez les paramètres de votre VPN.
8. Tapez sur **Enregistrer**.

Certificats numériques

Certaines connexions Wi-Fi sécurisées exigent soit une authentification du serveur, soit une authentification mutuelle. Afin de pouvoir utiliser ces connexions, vous devez acquérir et installer les deux fichiers de certificat sur l'appareil.

- **Certificat CA** – Active la configuration de l'authentification du serveur.
- **Certificat client** – Active la configuration de l'authentification mutuelle avec le certificat CA.

Vous pouvez installer manuellement les fichiers du certificat sur l'appareil, à l'aide de Xperia Configurator, ou en utilisant une solution GAP/GME d'un tiers.

Pour installer manuellement les fichiers du certificat sur un appareil Xperia

1. **Ordinateur :** Copiez les deux fichiers du certificat vers le dossier racine du stockage interne, ou vers le dossier racine de la carte mémoire si aucun stockage interne n'est disponible.
2. **Appareil Xperia :** Depuis l'écran d'accueil, tapez sur l'icône de l'écran Application.
3. Recherchez et tapez sur **Paramètres** > **Sécurité** > **Installer depuis le stockage interne** ou **Installer depuis la carte SD** (selon l'emplacement où vous avez copié les fichiers).
4. Dans la liste des certificats disponibles, sélectionnez les fichiers applicables pour les installer.
5. S'il s'agit d'un certificat client, entrez, lorsque vous y serez invité, le mot de passe défini lors de la création du fichier PKCS #12.

Vous trouverez la liste complète des fonctions de sécurité prises en charge par les appareils Xperia dans les livres blancs Xperia dans l'entreprise à l'adresse suivante : http://www.sonymobile.com/global-en/xperia/business/it-support/.

Synchronisation des courriels, du calendrier, et des contacts professionnels

Fournir un accès par courriel sur les appareils qui appartiennent aux employés est souvent la première étape de la création d'une force de travail mobile. Il est facile de donner un accès aux événements du calendrier et au carnet d'adresses de l'entreprise aux appareils BYOD et à ceux appartenant à l'entreprise. Que votre entreprise utilise Microsoft® Exchange, Lotus Notes, Google apps ou d'autres services majeurs, les appareils Xperia ont tous les capacités qu'il vous faut pour synchroniser les données.

Vous trouverez des informations supplémentaires à propos des options de synchronisation prises en charge par les appareils Xperia dans les livres blancs Xperia dans l'entreprise à l'adresse suivante : http://www.sonymobile.com/global-en/xperia/business/it-support/.

Il est possible de configurer manuellement les comptes pour la synchronisation des courriels, les événements du calendrier et les contacts professionnels sur l'appareil ou à l'aide de Xperia Configurator, ou une solution GAP/GME d'un tiers.

Pour configurer manuellement un compte de courriel, un calendrier et des contacts professionnels sur un appareil Xperia.

1. Depuis l'écran d'accueil, tapez sur l'icône de l'écran Application.
2. Recherchez et tapez sur **Paramètres > Comptes.**
3. Vérifiez que la case « Activer la synchronisation automatique » est cochée afin de permettre la synchronisation automatique des données en fonction de l'intervalle de synchronisation défini.
4. Tapez sur **Ajouter un compte > Exchange ActiveSync.**
5. Saisissez votre adresse e-mail professionnelle et votre mot de passe.
6. Tapez sur **Suivant**.
7. Suivez les étapes pour configurer votre compte et sélectionnez une fréquence de synchronisation. Si les réglages du compte courriel professionnel ne sont pas trouvés automatiquement, terminez la configuration manuellement. Entrez les informations requises, par exemple un domaine, un nom d'utilisateur, un mot de passe et un serveur.
8. Lorsque la configuration sera terminée, entrez un nom pour ce compte professionnel afin qu'il soit facilement identifiable, puis tapez sur **Terminé.**

Si vous avez établi une politique qui exige un certain niveau de sécurité, l'utilisateur sera invité à activer l'administrateur de l'appareil afin que votre serveur d'entreprise puisse contrôler certaines fonctions de sécurité de l'appareil. Les administrateurs des appareils sont généralement le courriel, le calendrier ou d'autres applications que vous autorisez à implémenter les règles de sécurité sur l'appareil lorsque vous vous connectez aux services d'entreprise qui l'exigent.

Gestion des appareils Xperia

Une fois vos utilisateurs équipés et utilisant les appareils, vous disposerez d'une vaste gamme de possibilités administrative vous permettant de gérer les appareils pendant tout leur cycle de vie. Ces possibilités comprennent l'interrogation des appareils à des fins d'information, l'initiation des commandes de sécurité (comme l'effacement à distance) et l'exécution de tâches spécifiques associées aux applications. Les appareils Xperia prennent en charge la gestion d'appareils avec Microsoft® Exchange ActiveSync® (EAS) client intégré, le Xperia Configurator gratuit et les services « my Xperia » de Sony Mobile, ainsi que les solutions de gestion des appareils portables (GAP) ou de gestion de la mobilité d'entreprise (GME) de tiers. Ces solutions permettent de gérer les appareils Xperia appartenant à l'entreprise et les appareils personnels (utilisant une politique BYOD) sur les ondes hertziennes depuis une seule console de gestion.

S'ils sont intégrés dans un environnement informatique professionnel fonctionnant avec une solution GAP/GME, les appareils Xperia proposent un éventail complet de politiques, des fonctions de commande/administration de l'appareil, ainsi que des fonctions d'assistance technique et de collecte de l'inventaire de l'appareil. Les appareils Xperia prennent en charge les politiques de mobilité en proposant :

- Inventaire de l'application
- Configuration de l'appareil
- Protection des données
- Distribution du certificat
- Réinitialisation du mot de passe à distance
- Suivi de l'emplacement de l'appareil
- Effacement et blocage des appareils à distance
- Mise à jour des paramètres et du logiciel

Pour obtenir la liste complète des fonctions et politiques prises en charge, consultez le document de présentation du produit que vous trouverez sur : www.sonymobile.com/global-en/xperia/business/it-support/.

Marques et remerciements

Pour plus d’informations, visitez www.sonymobile.com.