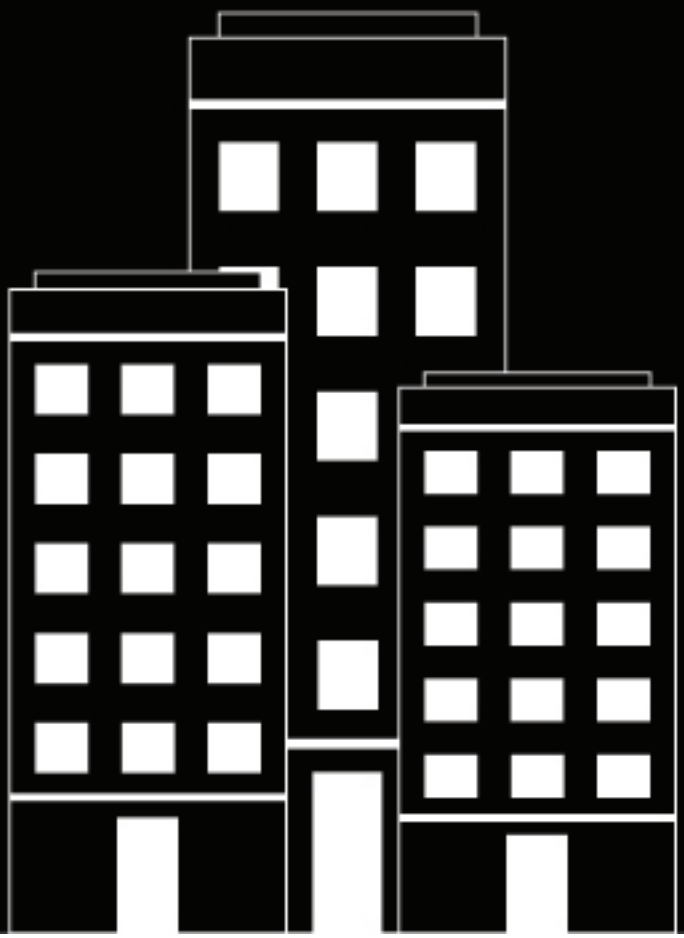

BlackBerry UES

Guide de l'utilisateur BlackBerry UES

Contents

Qu'est-ce que l'application CylancePROTECT Mobile ?

L'application CylancePROTECT Mobile vous permet de mieux connaître la sécurité de votre terminal mobile et de prendre des mesures pour résoudre les menaces sans intervention de l'administrateur.

L'application CylancePROTECT Mobile vous fournit :

- Une évaluation globale de la sécurité du terminal
- Liste des applications malveillantes ou chargées latéralement qui ont été détectées
- Alertes concernant les problèmes de réseau ou les paramètres de terminal qui présentent un risque pour la sécurité
- Capacité à détecter les URL malveillantes dans les messages texte
- Des options conviviales pour vous aider à prendre des mesures correctives, telles que désinstaller des applications malveillantes ou chargées latéralement et corriger les paramètres ou conditions du terminal

L'application CylancePROTECT Mobile analyse le terminal à intervalles réguliers pour identifier les menaces. Lorsque l'application détecte une menace, vous pouvez afficher les détails dans l'application. Dans la mesure du possible, l'application vous guide pour résoudre une menace et vous guide vers les paramètres du terminal où vous pouvez résoudre le problème. Pour plus d'informations, reportez-vous à Principales fonctionnalités de l'application CylancePROTECT Mobile.

Votre administrateur Cylance Endpoint Security peut configurer l'application CylancePROTECT Mobile pour vous envoyer une notification de terminal, une notification par e-mail ou aucune notification lorsqu'une menace est détectée. Vous pouvez toujours afficher les alertes actives dans l'application CylancePROTECT Mobile.

L'application CylancePROTECT Mobile pour Android 2.3.0.1640 et les versions ultérieures vous avertit lorsqu'une nouvelle version de l'application est disponible dans Google Play. Au bout de 30 jours, l'application CylancePROTECT Mobile télécharge automatiquement la mise à jour et vous invite à terminer la mise à jour et à redémarrer l'application. Au bout de 60 jours, vous ne pourrez plus utiliser l'application tant que vous n'aurez pas répondu à l'invite de mise à niveau.

L'application CylancePROTECT Mobile pour iOS prend en charge les mises à jour automatiques à partir de l'App Store.

Principales fonctionnalités de l'application CylancePROTECT Mobile

L'application CylancePROTECT Mobile comporte des avertissements décrits dans les tableaux suivants.

Fonctionnalité de sécurité de l'application	Description
Applications malveillantes	Les applications sont analysées pour déterminer si elles sont potentiellement malveillantes. Si vous avez installé une application considérée comme malveillante, l'application CylancePROTECT Mobile envoie une notification de terminal.
Applications chargées latéralement	Les applications chargées latéralement sont des applications installées à partir de sources non officielles ou inconnues et considérées comme dangereuses, car elles ne suivent pas les mêmes restrictions ou protections que les applications distribuées via des boutiques d'applications officielles. L'application CylancePROTECT Mobile envoie une notification de terminal lorsqu'une application chargée latéralement est détectée.

Fonctionnalité de sécurité du terminal	Description
Options pour développeurs	Lorsque les options pour développeurs sont activées sur votre terminal, certains paramètres et options sensibles deviennent disponibles. L'application CylancePROTECT Mobile envoie une notification de terminal lorsque les options pour développeurs sont activées.
Détection racine	Si votre terminal est « débridé » ou « cracké », cela signifie qu'un utilisateur (vous ou une tierce personne) a exécuté un logiciel ou une action sur le terminal qui autorise l'accès racine au système d'exploitation du terminal. Vous (ou votre administrateur) devrez peut-être supprimer le logiciel de « débridage » du terminal ou exécuter certaines actions sur le terminal pour rétablir son état par défaut. L'application CylancePROTECT Mobile envoie une notification de terminal lorsqu'elle détecte qu'il est débridé ou cracké.
Cryptage de disque complet	Les données non chiffrées de votre terminal peuvent être facilement lues par un utilisateur non autorisé. L'application CylancePROTECT Mobile envoie une notification de terminal lorsque le chiffrement n'est pas activé.
Verrouillage de l'écran	Le verrouillage d'écran empêche tout accès non autorisé à votre terminal, par exemple en cas de perte ou de vol. L'application CylancePROTECT Mobile envoie une notification de terminal si aucun mot de passe de verrouillage d'écran ou aucune empreinte digitale n'ont été définis.
Attestation	L'intégrité et l'authenticité de l'application CylancePROTECT Mobile sur votre terminal sont régulièrement vérifiées. L'application CylancePROTECT Mobile envoie une notification de terminal si l'une de ces vérifications échoue. Sur les terminaux Samsung, les services cloud CylancePROTECT peuvent également utiliser l'attestation améliorée Samsung Knox à intervalles réguliers pour valider l'intégrité des terminaux. L'attestation améliorée Knox est basée sur le matériel et peut détecter la falsification des terminaux, le rootage, le déverrouillage OEM et la falsification de l'IMEI ou du numéro de série, en plus d'effectuer des contrôles d'intégrité des applications.
Système d'exploitation du terminal	L'administrateur peut restreindre certaines versions de système d'exploitation du terminal qui ne répondent pas aux exigences de sécurité de votre organisation. L'application CylancePROTECT Mobile envoie une notification de terminal lorsqu'elle détecte qu'une version limitée du système d'exploitation du terminal est exécutée.
Modèle du terminal	L'administrateur peut restreindre certains modèles de terminaux qui ne répondent pas aux exigences de sécurité de votre organisation. L'application CylancePROTECT Mobile envoie une notification de terminal lorsqu'elle détecte que le terminal exécute un modèle de système d'exploitation restreint.

Fonctionnalité de protection réseau	Description
Sécurité Wi-Fi	Si votre terminal est connecté à un point d'accès Wi-Fi dont le protocole de chiffrement réseau est considéré comme non sécurisé, l'application CylancePROTECT Mobile envoie une notification de terminal.
Connexion réseau	L'application CylancePROTECT Mobile évalue sa connexion réseau aux services cloud CylancePROTECT Mobile pour déterminer si la connexion est sécurisée. Si la connexion est considérée comme dangereuse, l'application CylancePROTECT Mobile envoie une notification de terminal.

Fonctionnalité d'analyse des messages	Description
Analyse des messages texte	Lorsque vous recevez des SMS contenant des URL, celles-ci sont analysées pour déterminer si elles sont potentiellement malveillantes. L'application CylancePROTECT Mobile envoie une notification de terminal lorsqu'une URL malveillante est détectée.

Fonctionnalité CylanceGATEWAY	Description
Mode Travail	Activez le mode Travail dans l'application CylancePROTECT Mobile pour accéder aux ressources réseau en toute sécurité et protéger votre terminal contre les activités réseau suspectes et potentiellement malveillantes.

Installation et activation de l'application CylancePROTECT Mobile

Avant de commencer :

- Vous pourrez activer l'application CylancePROTECT Mobile lorsque l'administrateur vous aura envoyé un e-mail contenant des informations sur l'activation.
- L'administrateur vous a peut-être fourni des conseils si vous êtes un utilisateur d'annuaire ou BlackBerry Online Account . Si vous êtes un utilisateur BlackBerry Online Account et que vous ne connaissez pas vos informations d'identification, accédez à la page de réinitialisation du mot de passe de votre compte BlackBerry Online pour saisir votre adresse e-mail et suivez les instructions indiquées dans l'e-mail de réinitialisation du mot de passe pour définir un mot de passe que vous utiliserez pour activer l'application CylancePROTECT Mobile.
- JavaScript doit être activé dans votre navigateur mobile par défaut. L'application CylancePROTECT Mobile prend en charge Google Chrome, Samsung Internet et Safari.

1. Téléchargez et installez l'application CylancePROTECT Mobile à partir de App Store ou de Google Play.
2. Ouvrez l'application CylancePROTECT Mobile.
3. Lisez et acceptez la déclaration de confidentialité et les conditions générales BlackBerry.
4. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Activer l'application à l'aide d'un QR Code	**a.** Appuyez sur **Scanner le QR Code**. **b.** Scannez le QR Code figurant dans l'e-mail d'activation de l'application CylancePROTECT Mobile que vous avez reçu.
Utilisateur de répertoire : activez l'application à l'aide de votre adresse e-mail professionnelle et de votre mot de passe.	**a.** Appuyez sur **Se connecter avec vos informations d'identification de compte si votre administrateur vous le demande**. **b.** Lorsque vous êtes invité à saisir votre domaine personnalisé, saisissez le domaine figurant dans l'e-mail d'activation de l'application CylancePROTECT Mobile que vous avez reçu (option C). Appuyez sur **Suivant**. **c.** Dans le champ **Nom d'utilisateur**, saisissez votre adresse de messagerie professionnelle. Appuyez sur **Suivant**. **d.** Dans le champ **Mot de passe**, saisissez le mot de passe de votre messagerie professionnelle. Appuyez sur **Suivant**.
Utilisateur BlackBerry Online Account : activez l'application CylancePROTECT Mobile avec votre adresse de messagerie et votre mot de passe BlackBerry Online Account.	**a.** Appuyez sur **Se connecter avec vos informations d'identification de compte si votre administrateur vous le demande**. **b.** Lorsque vous êtes invité à saisir votre domaine personnalisé, saisissez le domaine figurant dans l'e-mail d'activation de l'application CylancePROTECT Mobile que vous avez reçu (option C). Appuyez sur **Suivant**. **c.** Dans le champ **Nom d'utilisateur**, saisissez l'adresse électronique de votre BlackBerry Online Account. Appuyez sur **Suivant**. **d.** Dans le champ **Mot de passe**, saisissez le mot de passe de votre BlackBerry Online Account. Appuyez sur **Suivant**.

Tâche	Étapes
Activez l'application CylancePROTECT Mobile à l'aide d'un mot de passe d'activation.	**a.** Appuyez sur **Saisir les informations d'identification fournies dans votre e-mail d'activation**. **b.** Dans le champ **Domaine personnalisé**, saisissez le domaine figurant dans l'e-mail d'activation de l'application CylancePROTECT Mobile que vous avez reçu (option B). **c.** Dans le champ **Nom d'utilisateur**, saisissez votre nom d'utilisateur. **d.** Dans le champ **Mot de passe d'activation**, saisissez le mot de passe d'activation. **e.** Sélectionnez **Continuer**.

5. Selon la configuration de votre administrateur, vous pouvez recevoir plusieurs invites pour activer et autoriser l'accès à différentes fonctionnalités. Complétez les invites et accordez les autorisations d'accès si nécessaire, puis suivez les instructions supplémentaires qui s'affichent.

   Pour détecter les modifications apportées au réseau pour la fonctionnalité de protection Wi-Fi, vous devez autoriser en permanence les autorisations de localisation en arrière-plan.

À la fin :

- Vous devez autoriser l'activité en arrière-plan pour l'application CylancePROTECT Mobile.
- Vous pouvez répéter ces étapes pour installer et activer l'application CylancePROTECT Mobile sur d'autres terminaux.
- L'application CylancePROTECT Mobile pour Android avertit lorsqu'une nouvelle version de l'application est disponible dans Google Play. Au bout de 30 jours, l'application télécharge automatiquement la mise à jour et vous invite à terminer la mise à jour et à redémarrer l'application. Au bout de 60 jours, vous ne pourrez plus utiliser l'application tant que vous n'aurez pas répondu à l'invite de mise à niveau.
- L'application CylancePROTECT Mobile pour iOS prend en charge les mises à jour automatiques à partir de l'App Store.
- Consultez Activer le mode Travail et Activer la fonction d'analyse des messages.

Activer le mode Travail

Si votre administrateur a configuré la fonction CylanceGATEWAY pour vous, vous pouvez activer le mode Travail dans l'application CylancePROTECT Mobile pour accéder aux ressources réseau en toute sécurité et protéger votre terminal contre toute activité réseau suspecte et potentiellement malveillante. Lorsque vous activez la fonction, elle configure un accès sécurisé pour analyser l'activité du réseau et applique les stratégies d'accès réseau gérées par votre administrateur.

Avant de commencer : Vous devez autoriser les autorisations d'emplacement en arrière-plan à tout moment pour l'application CylancePROTECT Mobile.

1. Dans l'application CylancePROTECT Mobile, effectuez l'une des opérations suivantes :
   - Activez le paramètre **Mode Travail**.
   - Appuyez sur **Activer pour travailler en toute sécurité** > **Activer le mode Travail**.
2. Sélectionnez **OK**.
3. Dans la boîte de dialogue **Demande de connexion**, appuyez sur **OK** pour confirmer.

Une fois la connexion établie, l'état « Activé » s'affiche.

À la fin :

- Si votre administrateur vous demande d'activer les connexions TCP pour la fonction CylanceGATEWAY, appuyez sur ou sur l'écran CylanceGATEWAY, puis sélectionnez l'option **Utiliser TCP**.
- Pour afficher les avertissements relatifs à une activité réseau suspecte, appuyez sur **Afficher les avertissements**. Dans l'écran **Avertissements**, vous pouvez également choisir de désactiver le son des notifications d'avertissement.

Activer la fonction d'analyse des messages

Vous activez la fonction d'analyse des messages dans l'application CylancePROTECT Mobile pour lui permettre d'analyser les SMS entrants et de rechercher les URL potentiellement malveillantes. Seules les URL des messages sont évaluées.

Pour les terminaux iOS, seuls les messages provenant d'expéditeurs inconnus (contacts qui ne figurent pas sur la liste de contacts du terminal) sont analysés. Les messages contenant des URL potentiellement malveillantes sont filtrés dans le dossier des courriers indésirables.

Pour les terminaux Android, tous les messages provenant de contacts connus et d'expéditeurs inconnus sont analysés. Les messages contenant des URL potentiellement malveillantes sont répertoriés dans l'application CylancePROTECT Mobile, mais vous devez les supprimer manuellement dans l'application de messagerie par défaut.

Sur votre terminal mobile, effectuez l'une des opérations suivantes :

Terminal	Étapes
iOS	**a.** Ouvrez **Paramètres** dans l'application. **b.** Accédez à **Messages** > **Filtrage des messages** > **Inconnu et Courrier indésirable**. **c.** Dans la section **Filtrage des messages**, activez le paramètre **Filtrer les expéditeurs inconnus**. **d.** Dans la section **Filtrage des SMS**, appuyez sur **Protect**. **e.** Sélectionnez **Activer**. Ces instructions sont également disponibles dans l'application CylancePROTECT Mobile depuis **Intégrité du terminal** > **Analyse des messages**. Si vous utilisez l'application iMessage, activez l'option **Envoyer un SMS** dans l'application.
Android	**a.** Dans l'application CylancePROTECT Mobile, appuyez sur **Intégrité du terminal**. **b.** Appuyez sur le champ **Analyse des messages** pour le développer. **c.** Activez la fonction d'analyse des messages. **d.** Sur l'écran **Autoriser l'analyse des messages**, appuyez sur **Autoriser**. **e.** Sélectionnez **OK**.

Dans l'application CylancePROTECT Mobile, le message d'état « Analyse activée » s'affiche.

Résoudre les menaces mobiles

Lorsque l'application CylancePROTECT Mobile détecte des menaces mobiles sur votre terminal, vous recevez une notification de terminal. Vous pouvez ouvrir l'application CylancePROTECT Mobile pour identifier rapidement les menaces et les résoudre.

1. Ouvrez l'application CylancePROTECT Mobile.
2. Cliquez sur **Intégrité du terminal**.
3. Développez l'une des sections suivantes :
   - Sécurité de l'application
   - Sécurité des terminaux
   - Protection réseau
4. Utilisez le tableau suivant pour résoudre les menaces détectées sur le terminal.

Fonctionnalité	Plateforme	Description	Résolution
Sécurité de l'application			
Applications malveillantes	Android	Développez la section pour afficher la liste des applications malveillantes détectées par l'application.	Cliquez sur **Corriger** pour désinstaller une application malveillante du système d'exploitation du terminal.
Applications chargées latéralement	Android iOS	Les applications chargées latéralement sont des applications qui ont été installées à partir de sources inconnues ou non fiables. Sur les terminaux Android, développez la section pour afficher la liste de toutes les applications chargées latéralement que l'application a détectées. Sur les terminaux iOS, développez la section pour afficher la liste des profils de développeurs d'applications tiers approuvés et installés sur votre terminal.	Cliquez sur **Corriger** pour afficher les instructions de suppression de l'application chargée latéralement. Sur les terminaux Android, vous êtes dirigé vers les paramètres du terminal pour désinstaller l'application. Sur les terminaux iOS, vous êtes dirigé vers l'application Paramètres pour supprimer le profil d'application approuvé de votre terminal.
Sécurité des terminaux			
Options pour développeurs	Android	Les options pour développeur indique si le mode développeur est activé sur le terminal.	Appuyez sur **Corriger** pour afficher les instructions de désactivation du mode développeur. Vous êtes dirigé vers les paramètres du terminal pour désactiver le mode développeur.

Fonctionnalité	Plateforme	Description	Résolution
Détection racine	Android iOS	La détection racine affiche une notification si l'application détecte que le terminal est « débridé » ou « cracké ».	Aucune action dans l'application. Vous devez contacter votre administrateur pour résoudre le problème.
Cryptage de disque complet	Android	Le cryptage de disque complet indique si le cryptage de disque est activé sur le terminal.	Appuyez sur **Corriger** pour afficher les instructions d'activation du cryptage de disque. Vous êtes dirigé vers les paramètres du terminal pour activer le cryptage de disque.
Verrouillage de l'écran	Android iOS	Le verrouillage de l'écran indique si une option de verrouillage de l'écran (par exemple, un mot de passe ou une empreinte digitale) est actuellement activée sur le terminal.	Appuyez sur **Corriger** pour afficher les instructions d'activation du verrouillage d'écran. Sur les terminaux Android, vous êtes invité à accéder aux paramètres du terminal pour activer le verrouillage d'écran.

Fonctionnalité	Plateforme	Description	Résolution
Attestation du terminal	Android iOS	Sur les terminaux Android, une notification s'affiche si l'application CylancePROTECT Mobile échoue à l'une des opérations suivantes : • Attestation SafetyNet • Attestation de certificat matérielle • Niveau de sécurité de l'attestation matérielle inférieur à ce qui est configuré dans la stratégie CylancePROTECT Mobile • Le niveau du correctif de sécurité de l'attestation matérielle est inférieur à ce qui est configuré dans la stratégie CylancePROTECT Mobile • L'état de démarrage de l'attestation matérielle n'est pas vérifié Sur les terminaux iOS, une notification s'affiche si l'application CylancePROTECT Mobile échoue à une vérification d'intégrité à l'aide de l'infrastructure Apple DeviceCheck.	Pour les terminaux Android, si le niveau du correctif de sécurité ne correspond pas au correctif minimal configuré, appuyez sur **Corriger** pour rechercher les mises à jour logicielles. Pour les autres alertes d'attestation et les vérifications d'intégrité, il n'y a aucune action dans l'application. Vous devez contacter votre administrateur pour résoudre le problème.
Système d'exploitation du terminal	Android iOS	Le système d'exploitation du terminal indique si le système d'exploitation du terminal répond aux exigences de la stratégie CylancePROTECT qui vous est attribuée.	Appuyez sur **Corriger** pour afficher les instructions de mise à niveau du système d'exploitation. Sur les terminaux Android, vous êtes dirigé vers les paramètres du terminal pour mettre à niveau le système d'exploitation.
Modèle du terminal	Android iOS	Le modèle du terminal indique si le modèle du terminal répond aux exigences de la stratégie CylancePROTECT qui vous est attribuée.	Il n'y a aucune action à effectuer dans l'application. Vous devez contacter votre administrateur pour résoudre le problème.
Protection réseau			

Fonctionnalité	Plateforme	Description	Résolution
Connexion réseau	Android iOS	La connexion réseau indique si le réseau actuel est dangereux.	Appuyez sur **Corriger** pour afficher les instructions de déconnexion du réseau dangereux. Sur les terminaux Android, il existe une option permettant d'accéder aux paramètres du terminal pour vous déconnecter du réseau.
Sécurité Wi-Fi	Android	La sécurité Wi-Fi indique si le réseau Wi-Fi actuel n'est pas sécurisé.	Appuyez sur **Corriger** pour afficher les instructions de déconnexion du réseau Wi-Fi. Sur les terminaux Android, il existe une option permettant d'accéder aux paramètres du terminal pour vous déconnecter du réseau Wi-Fi.
Fonctions d'analyse des messages			
Messages de logiciels malveillants détectés	Android iOS	Identifiez les messages SMS contenant des URL potentiellement malveillantes.	Sur les terminaux Android, appuyez sur **Corriger** pour accéder à l'application de messagerie par défaut et supprimer les messages texte. Sur les terminaux iOS, les messages texte sont automatiquement filtrés dans le dossier de courrier indésirable.

Menaces mobiles détectées par l'application CylancePROTECT Mobile

Les menaces suivantes peuvent s'afficher dans l'application CylancePROTECT Mobile :

Menace de sécurité mobile	Niveau de risque	Couleur
Applications malveillantes	Élevé	Rouge
Applications chargées latéralement	Élevé	Rouge
Sécurité du terminal : options de développement	Moyen	Jaune
Sécurité du terminal : verrouillage de l'écran	Moyen	Jaune

Menace de sécurité mobile	Niveau de risque	Couleur
Sécurité des terminaux : terminal compromis ou débridé	Élevé	Rouge
Sécurité du terminal : chiffrement complet du disque	Moyen	Jaune
Sécurité des terminaux : attestation	Élevé	Rouge
Sécurité des terminaux : niveau du correctif de sécurité	Moyen	Jaune
Sécurité des terminaux : système d'exploitation du terminal	Moyen	Jaune
Sécurité des terminaux : modèle de terminal	Moyen	Jaune
Protection réseau : connexion réseau	Élevé	Rouge
Protection réseau : sécurité Wi-Fi	Moyen	Jaune
Analyse des messages SMS (s'affiche uniquement pour Android)	Moyen	Jaune

Désactiver l'application CylancePROTECT Mobile

Lorsque vous désactivez l'application, votre terminal ne reçoit plus de notifications pour vous avertir des risques de sécurité. La fonctionnalité CylanceGATEWAY ne sera pas non plus disponible pour accéder aux ressources et applications professionnelles.

Avant de commencer : Vérifiez que votre terminal est connecté au réseau sans fil.

Sur l'écran d'accueil de l'application CylancePROTECT Mobile, effectuez l'une des opérations suivantes :

Terminal	Étapes
iOS	**a.** Sélectionnez . **b.** Sélectionnez **Désactiver**. **c.** Sélectionnez **Désactiver** à nouveau.
Android	**a.** Sélectionnez . **b.** Sélectionnez **Désactiver**. **c.** Sélectionnez **Désactiver** à nouveau. **d.** Sélectionnez **OK**.

À la fin : Supprimez l'application CylancePROTECT Mobile de votre terminal.

Signaler un problème à BlackBerry

1. Sur l'écran d'accueil de l'application CylancePROTECT Mobile, sélectionnez .
2. Appuyez sur **Signaler un problème**.
3. Saisissez un commentaire concernant le problème.
4. Sélectionnez **Envoyer**.

Que sont les agents Cylance Endpoint Security ?

Les agents Cylance Endpoint Security s'exécutent sur des ordinateurs de bureau et sont généralement déployés par un administrateur pour être automatiquement installés sur votre terminal. Le tableau suivant répertorie et décrit les agents de bureau et leur utilisation.

Agent	Ce qu'il fait	Comment l'utiliser
CylancePROTECT Desktop	CylancePROTECT Desktop détecte et bloque les programmes malveillants avant qu'ils n'affectent un terminal.	Votre administrateur le déploie pour l'installer automatiquement sur votre terminal ou fournit des instructions pour l'installer manuellement. CylancePROTECT Desktop s'exécute en arrière-plan sur votre terminal après votre connexion.
CylanceOPTICS	CylanceOPTICS est une solution de détection de point de terminaison et de réponse qui collecte et examine les données d'analyse approfondie des terminaux afin d'identifier et de résoudre les menaces avant qu'elles n'affectent les utilisateurs et les données de votre entreprise.	Votre administrateur le déploie pour l'installer automatiquement sur votre terminal ou fournit des instructions pour l'installer manuellement. CylanceOPTICS s'exécute en arrière-plan sur votre terminal après votre connexion.
CylanceGATEWAY (agent de bureau)	CylanceGATEWAY fournit un accès sécurisé aux applications, services et ressources sur site et dans le cloud de votre entreprise sans nécessiter de VPN traditionnel. Il protège également les terminaux en permettant à votre entreprise de bloquer les connexions à des destinations Internet dangereuses et potentiellement malveillantes.	Votre administrateur le déploie pour l'installer automatiquement sur votre terminal ou fournit des instructions pour l'installer manuellement. Vous devez activer CylanceGATEWAY à l'aide de vos identifiants de répertoire ou des identifiants BlackBerry Online Account. Une fois CylanceGATEWAY activé, vous activez le mode Travail à partir de l'agent.

Agent	Ce qu'il fait	Comment l'utiliser
CylanceAVERT	CylanceAVERT identifie et classe les fichiers sensibles trouvés dans l'environnement de votre entreprise. Si ces fichiers sensibles sont impliqués dans une tentative d'exfiltrer les données par le biais de diverses sources (USB, lecteur réseau, e-mails ou téléchargements de navigateurs), CylanceAVERT peut prendre une mesure corrective spécifiée par votre administrateur pour protéger vos données.	Votre administrateur le déploie pour l'installer automatiquement sur votre terminal ou fournit des instructions pour l'installer manuellement. CylanceAVERT s'exécute en arrière-plan sur votre terminal après votre connexion.

Activez le mode Travail dans l'agent CylanceGATEWAY

Si l'administrateur a configuré CylanceGATEWAY pour vous, vous pouvez activer le mode Travail dans l'agent CylanceGATEWAY sur les terminaux Windows et macOS pour accéder aux ressources réseau en toute sécurité et protéger votre terminal contre toute activité réseau suspecte et potentiellement malveillante. Lorsque vous activez le mode Travail, CylanceGATEWAY établit des connexions sécurisées entre votre terminal et le réseau de votre organisation, analyse votre activité réseau et applique les stratégies d'accès réseau gérées par l'administrateur.

Avant de commencer :

- Installer l'agent CylanceGATEWAY. Pour télécharger l'agent, rendez-vous sur le site Web de BlackBerry et faites défiler l'écran jusqu'à la section Télécharger CylanceGATEWAY.
- Activez l'agent à l'aide de votre annuaire ou de vos informations d'identification BlackBerry Online Account. Pour plus d'informations sur l'activation de l'agent, consultez l'e-mail d'activation CylanceGATEWAY que vous avez reçu de l'administrateur.

1. Sur votre ordinateur, ouvrez l'agent CylanceGATEWAY.
2. Cliquez sur **Activer le mode Travail**.
3. Suivez les instructions indiquées sur l'écran.

Lorsque la connexion est établie, l'état Mode Travail activé s'affiche.

À la fin : Vous pouvez configurer des règles pour l'agent CylanceGATEWAY.

Paramètres de l'agent CylanceGATEWAY

Vous pouvez configurer des paramètres pour l'agent CylanceGATEWAY. Les noms des paramètres peuvent varier en fonction du système d'exploitation du terminal.

Paramètre	Description
Désactiver	Cliquez sur ce bouton pour désactiver l'agent CylanceGATEWAY. Lorsque l'agent est désactivé, il ne peut pas recevoir les mises à jour de stratégie de CylanceGATEWAY.

Paramètre	Description
Signaler un problème	Cliquez sur ce bouton pour envoyer un rapport de problème à BlackBerry.
Utiliser TCP	Sélectionnez cette option pour utiliser TCP pour les connexions à CylanceGATEWAY si le pare-feu de votre organisation n'autorise pas les connexions UDP.
Lancer CylanceGATEWAY automatiquement lorsque je me connecte à cet ordinateur	Sélectionnez cette option pour démarrer l'agent CylanceGATEWAY chaque fois que vous vous connectez à votre terminal Windows ou macOS.
Connecter le Mode travail automatiquement au démarrage de CylanceGATEWAY	Sélectionnez cette option pour activer le mode Travail chaque fois que l'agent CylanceGATEWAY démarre.

Important : Si vous souhaitez que l'agent CylanceGATEWAY démarre et active automatiquement le Mode travail chaque fois que vous vous connectez à votre terminal Windows ou macOS, vous devez cocher les cases **Lancer CylanceGATEWAY lorsque je me connecte à cet ordinateur** et **Connecter le Mode travail automatiquement au lancement de CylanceGATEWAY**.

Informations juridiques

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada