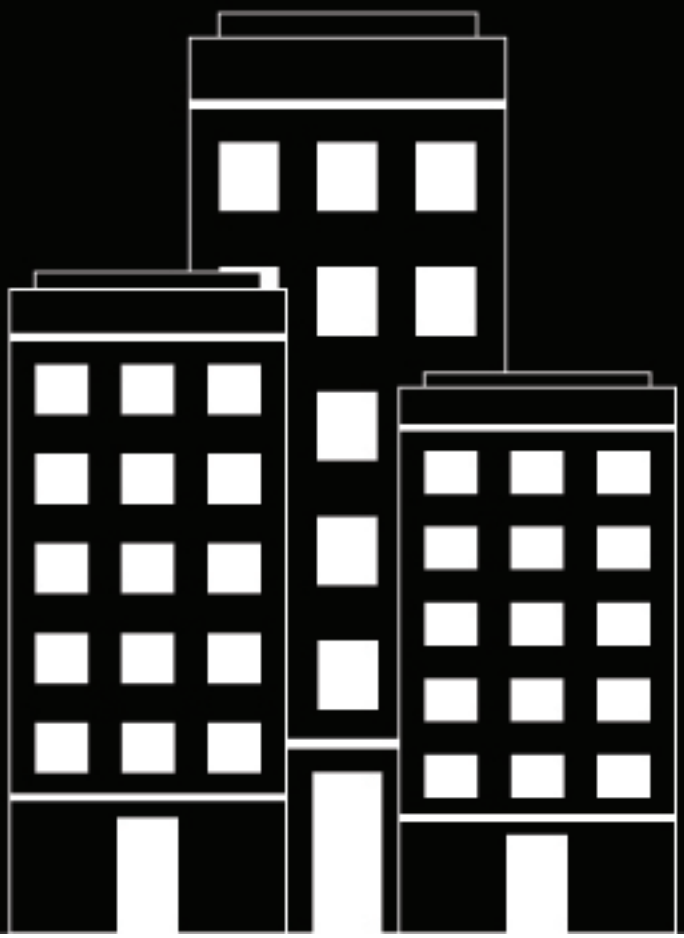

BlackBerry UES

BlackBerry UES-Benutzerhandbuch

Contents

Was ist die CylancePROTECT Mobile-App?

Die CylancePROTECT Mobile-App ermöglicht Ihnen eine stärkere Wahrnehmung der Sicherheit Ihres Mobilgeräts und versetzt Sie in die Lage, Maßnahmen zur Lösung von Bedrohungen zu ergreifen, ohne dass ein Administrator eingreifen muss.

Die CylancePROTECT Mobile-App bietet Ihnen:

- Eine allgemeine Sicherheitsbewertung des Geräts
- Eine Liste der erkannten schädlichen oder Sideloading-Apps
- Warnungen zu Netzwerkproblemen oder Geräteeinstellungen, die ein Sicherheitsrisiko darstellen
- Die Möglichkeit, schädliche URLs in Textnachrichten zu erkennen
- Benutzerfreundliche Optionen, anhand derer Sie Korrekturmaßnahmen ergreifen können, z. B. die Deinstallation schädlicher oder Sideloading-Apps und die Korrektur von Geräteeinstellungen oder -bedingungen

Die CylancePROTECT Mobile-App scannt das Gerät in regelmäßigen Abständen, um Bedrohungen zu identifizieren. Wenn die App eine Bedrohung erkennt, können Sie entsprechende Details in der App anzeigen. Wenn möglich, führt Sie die App zur Lösung einer Bedrohung und zu den Geräteeinstellungen, mit denen Sie das Problem beheben können. Weitere Informationen finden Sie unter Wichtige Funktionen der CylancePROTECT Mobile-App.

Ihr Cylance Endpoint Security-Administrator kann die CylancePROTECT Mobile-App so konfigurieren, dass Sie eine Gerätebenachrichtigung, eine E-Mail-Benachrichtigung oder keine Benachrichtigung erhalten, wenn eine Bedrohung erkannt wird. Sie können jederzeit alle aktiven Warnmeldungen in der CylancePROTECT Mobile-App anzeigen.

Die CylancePROTECT Mobile-App für Android Version 2.3.0.1640 und höher benachrichtigt Sie, wenn eine neue Version der App in Google Play verfügbar ist. Nach 30 Tagen lädt die CylancePROTECT Mobile-App das Update automatisch herunter und fordert Sie auf, das Update abzuschließen und die App neu zu starten. Nach 60 Tagen können Sie die App erst dann verwenden, wenn Sie auf die Aktualisierungsaufforderung reagiert haben.

Die CylancePROTECT Mobile-App für iOS unterstützt automatische Updates aus dem App Store.

Wichtige Funktionen der CylancePROTECT Mobile-App

Die CylancePROTECT Mobile-App enthält Warnungen, die in den folgenden Tabellen beschrieben sind.

App-Sicherheitsfunktion	Beschreibung
Schädliche Apps	Apps werden analysiert, um festzustellen, ob sie potenziell schädlich sind. Wenn Sie eine App installiert haben, die als bösartig angesehen wird, sendet die CylancePROTECT Mobile-App eine Gerätebenachrichtigung.
Apps mit Seitenladefunktion	Sideloading-Apps sind Apps, die von inoffiziellen oder unbekannten Quellen installiert werden. Sie gelten als unsicher, da sie nicht denselben Einschränkungen oder Schutzvorkehrungen unterliegen wie Apps, die über offizielle App Stores verteilt werden. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn eine Sideloading-App erkannt wird.

Gerätesicherheitsfunktion	Beschreibung
Entwickleroptionen	Wenn Entwickleroptionen auf Ihrem Gerät aktiviert sind, stehen einige sensible Einstellungen und Optionen zur Verfügung. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn Entwickleroptionen aktiviert sind.
Root-Erkennung	Falls auf Ihrem Gerät ein Rooting oder Jailbreak auftritt, bedeutet dies, entweder Sie oder eine andere Person haben auf dem Gerät eine Software oder eine Aktion ausgeführt, die dem Benutzer Stammzugriff auf das Betriebssystem des Geräts gewährt. Sie oder Ihr Administrator müssen die Rooting-Software vom Gerät entfernen oder eine Aktion auf dem Gerät ausführen, um den Standardzustand des Geräts wiederherzustellen. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn sie auf dem Gerät ein Rooting oder Jailbreak erkennt.
Verschlüsselung des gesamten Datenträgers	Unverschlüsselte Daten auf Ihrem Gerät können von nicht autorisierten Benutzern leicht gelesen werden. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn die Verschlüsselung nicht aktiviert ist.
Bildschirmsperre	Das Einrichten einer Bildschirmsperre verhindert den unbefugten Zugriff auf Ihr Gerät, z. B., wenn Ihr Gerät verloren geht oder gestohlen wird. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn kein Kennwort für die Bildschirmsperre oder kein Fingerabdruck festgelegt worden ist.
Nachweis	Die CylancePROTECT Mobile-App auf Ihrem Gerät wird regelmäßig auf Integrität und Authentizität überprüft. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn Ihr Gerät eine dieser Prüfungen nicht besteht. Auf Samsung-Geräten können die CylancePROTECT Cloud-Dienste die Integrität der Geräte auch in regelmäßigen Abständen mithilfe von Samsung Knox Enhanced Attestation validieren. Knox Enhanced Attestation arbeitet hardwarebasiert und kann Gerätemanipulationen, Rooting, OEM-Entsperrung und Fälschung von IMEI- oder Seriennummern sowie die Durchführung von App-Zustandsprüfungen erkennen.
Gerätebetriebssystem	Ihr Administrator kann einige Gerätebetriebssystemversionen einschränken, die nicht den Sicherheitsanforderungen Ihres Unternehmens entsprechen. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn sie erkennt, dass auf dem Gerät eine eingeschränkte Gerätebetriebssystemversion ausgeführt wird.
Gerätemodell	Ihr Administrator kann einige Gerätemodelle einschränken, die nicht den Sicherheitsanforderungen Ihres Unternehmens entsprechen. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn sie erkennt, dass auf dem Gerät ein eingeschränktes Gerätemodell ausgeführt wird.

Netzwerkschutzfunktion	Beschreibung
Wi-Fi-Sicherheit	Wenn Ihr Gerät mit einem Wi-Fi-Zugriffspunkt verbunden ist, dessen Netzwerk-Verschlüsselungsprotokoll als unsicher gilt, sendet die CylancePROTECT Mobile-App eine Gerätebenachrichtigung.
Netzwerkverbindung	Die CylancePROTECT Mobile-App wertet die Netzwerkverbindung zu den CylancePROTECT Mobile-Cloud-Diensten aus, um festzustellen, ob die Verbindung sicher ist. Wenn die Verbindung als unsicher betrachtet wird, sendet die CylancePROTECT Mobile-App eine Gerätebenachrichtigung.

Nachrichtenscanfunktion	Beschreibung
SMS-Nachrichtenscan	Wenn Sie SMS-Nachrichten mit URLs erhalten, werden diese überprüft, um festzustellen, ob sie potenziell schädlich sind. Die CylancePROTECT Mobile-App sendet eine Gerätebenachrichtigung, wenn eine schädliche URL erkannt wird.

CylanceGATEWAY-Funktion	Beschreibung
Arbeitsmodus	Aktivieren Sie den Arbeitsmodus in der CylancePROTECT Mobile-App, um sicher auf Netzwerkressourcen zuzugreifen und Ihr Gerät vor verdächtigen und potenziell schädlichen Netzwerkaktivitäten zu schützen.

Installieren und Aktivieren der CylancePROTECT Mobile-App

Bevor Sie beginnen:

- Sie können die CylancePROTECT Mobile-App aktivieren, wenn Sie eine Aktivierungs-E-Mail von Ihrem Administrator erhalten haben, die Informationen zur Aktivierung der App enthält.
- Ihr Administrator hat Ihnen möglicherweise mitgeteilt, ob Sie ein Verzeichnis- oder BlackBerry Online Account-Benutzer sind. Wenn Sie ein BlackBerry Online Account-Benutzer sind und Ihre Anmeldedaten nicht kennen, navigieren Sie zur Seite Zurücksetzen des Kennworts für das BlackBerry Online-Konto, um Ihre E-Mail-Adresse einzugeben. Befolgen Sie die Anweisungen zum Zurücksetzen des Kennworts in der E-Mail, um ein Kennwort festzulegen, das Sie zum Aktivieren der CylancePROTECT Mobile-App verwenden möchten.
- In Ihrem mobilen Standardbrowser muss JavaScript aktiviert sein. Die CylancePROTECT Mobile-App unterstützt Google Chrome, Samsung Internet und Safari.

1. Sie können die CylancePROTECT Mobile-App von App Store oder Google Play herunterladen und installieren.
2. Öffnen Sie die CylancePROTECT Mobile-App.
3. Lesen und akzeptieren Sie den BlackBerry-Datenschutzhinweis und die Geschäftsbedingungen.
4. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren der App mit einem QR Code	**a.** Tippen Sie auf **QR-Code scannen**. **b.** Scannen Sie den QR Code aus der erhaltenen Aktivierungs-E-Mail für die CylancePROTECT Mobile-App.
Verzeichnisbenutzer: Aktivieren der App mit Ihrer geschäftlichen E-Mail-Adresse und Ihrem Kennwort	**a.** Tippen Sie auf **Melden Sie sich mit Ihren Kontoanmeldedaten an, wie von Ihrem Administrator angewiesen**. **b.** Wenn Sie zur Eingabe Ihrer benutzerdefinierten Domäne aufgefordert werden, geben Sie die Domäne aus der erhaltenen Aktivierungs-E-Mail für die CylancePROTECT Mobile-App ein (Option C). Tippen Sie auf **Weiter**. **c.** Geben Sie in das Feld **Benutzername** Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. **d.** Geben Sie in das Feld **Kennwort** Ihr geschäftliches E-Mail-Kennwort ein. Tippen Sie auf **Weiter**.
BlackBerry Online Account-Benutzer: Aktivieren der CylancePROTECT Mobile-App mit Ihrer E-Mail-Adresse für den BlackBerry Online Account und Ihrem Kennwort	**a.** Tippen Sie auf **Melden Sie sich mit Ihren Kontoanmeldedaten an, wie von Ihrem Administrator angewiesen**. **b.** Wenn Sie zur Eingabe Ihrer benutzerdefinierten Domäne aufgefordert werden, geben Sie die Domäne aus der erhaltenen Aktivierungs-E-Mail für die CylancePROTECT Mobile-App ein (Option C). Tippen Sie auf **Weiter**. **c.** Geben Sie in das Feld **Benutzername** die E-Mail-Adresse für Ihren BlackBerry Online Account ein. Tippen Sie auf **Weiter**. **d.** Geben Sie in das Feld **Kennwort** das Kennwort für Ihren BlackBerry Online Account ein. Tippen Sie auf **Weiter**.

Aufgabe	Schritte
Aktivieren der CylancePROTECT Mobile-App mit einem Aktivierungskennwort	**a.** Tippen Sie auf **Anmeldedaten aus Ihrer Aktivierungs-E-Mail eingeben**. **b.** Geben Sie in das Feld **Benutzerdefinierte Domäne** die Domäne aus der Aktivierungs-E-Mail ein, die Sie für die CylancePROTECT Mobile-App erhalten haben (Option B). **c.** Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein. **d.** Geben Sie in das Feld **Aktivierungskennwort** das Aktivierungskennwort ein. **e.** Tippen Sie auf **Fortfahren**.

5. Je nach Konfiguration durch Ihren Administrator werden Sie möglicherweise mehrere Aufforderungen zur Aktivierung und zum Zulassen des Zugriffs auf verschiedene Funktionen erhalten. Folgen Sie den Eingabeaufforderungen, lassen die erforderlichen Zugriffsberechtigungen zu und führen Sie alle zusätzlich angezeigten Anweisungen aus.

   Um Netzwerkänderungen für die Wi-Fi-Schutzfunktion zu erkennen, müssen Sie die Standortberechtigungen im Hintergrund jederzeit zulassen.

Wenn Sie fertig sind:

- Sie müssen Hintergrundaktivitäten für die CylancePROTECT Mobile-App zulassen.
- Sie können diese Schritte wiederholen, um die CylancePROTECT Mobile-App auf weiteren Geräten zu installieren und zu aktivieren.
- Die CylancePROTECT Mobile-App für Android benachrichtigt Sie, wenn eine neue Version der App in Google Play verfügbar ist. Nach 30 Tagen lädt die App das Update automatisch herunter und fordert Sie auf, das Update abzuschließen und die App neu zu starten. Nach 60 Tagen können Sie die App erst dann verwenden, wenn Sie auf die Aktualisierungsaufforderung reagiert haben.
- Die CylancePROTECT Mobile-App für iOS unterstützt automatische Updates aus dem App Store.
- Siehe Aktivieren des Arbeitsmodus und Aktivieren der Nachrichtenscanfunktion.

Aktivieren des Arbeitsmodus

Wenn Ihr Administrator die CylanceGATEWAY-Funktion für Sie konfiguriert hat, können Sie den Arbeitsmodus in der CylancePROTECT Mobile-App aktivieren, um sicher auf Netzwerkressourcen zuzugreifen und Ihr Gerät vor verdächtigen und potenziell schädlichen Netzwerkaktivitäten zu schützen. Wenn Sie die Funktion aktivieren, richtet sie einen sicheren Zugriff ein, um die Netzwerkaktivität zu analysieren, und wendet die vom Administrator verwalteten Richtlinien für den Netzwerkzugriff an.

Bevor Sie beginnen: Sie müssen für die CylancePROTECT Mobile-App jederzeit Hintergrundstandortberechtigungen zulassen.

1. Führen Sie in der CylancePROTECT Mobile-App eine der folgenden Aktionen aus:
   - Aktivieren Sie die Einstellung **Arbeitsmodus**.
   - Tippen Sie auf **Aktivieren Sie diese Option, um sicher zu arbeiten** > **Arbeitsmodus aktivieren**.
2. Tippen Sie auf **OK**.
3. Tippen Sie zur Bestätigung im Dialogfeld **Verbindungsanfrage** auf **OK**.

Wenn die Verbindung hergestellt ist, wird der Status „Aktiviert“ angezeigt.

Wenn Sie fertig sind:

- Wenn Ihr Administrator Sie dazu auffordert, TCP-Verbindungen für die CylanceGATEWAY-Funktion zu aktivieren, tippen Sie auf dem CylanceGATEWAY-Bildschirm auf  oder auf  und wählen die Option **TCP verwenden** aus.
- Um Warnungen zu verdächtigen Netzwerkaktivitäten anzuzeigen, tippen Sie auf **Warnungen anzeigen**. Auf dem Bildschirm **Warnungen** können Sie auch Warnmeldungen stummschalten.

Aktivieren der Nachrichtenscanfunktion

Sie können die Nachrichtenscanfunktion in der CylancePROTECT Mobile-App aktivieren, damit eingehende SMS-Nachrichten auf potenziell schädliche URLs gescannt werden können. Es werden nur in den Nachrichten enthaltene URLs ausgewertet.

Bei iOS-Geräten werden nur Nachrichten von unbekannten Absendern (Kontakte, die nicht in der Kontaktliste des Geräts enthalten sind) gescannt. Nachrichten, die potenziell schädliche URLs enthalten, werden in den Spam-Ordner gefiltert.

Bei Android-Geräten werden alle Nachrichten von bekannten Kontakten und unbekannten Absendern gescannt. Nachrichten, die potenziell schädliche URLs enthalten, werden in der CylancePROTECT Mobile-App aufgeführt. Sie müssen diese jedoch in der Standard-Messaging-App manuell löschen.

Führen Sie auf Ihrem Mobilgerät einen der folgenden Schritte aus:

Gerät	Schritte
iOS	**a.** Öffnen Sie die App **Einstellungen**. **b.** Navigieren Sie zu **Nachrichten** > **Nachrichtenfilter** > **Unbekannt und Spam**. **c.** Aktivieren Sie im Abschnitt **Nachrichtenfilter** die Einstellung **Unbekannte Absender filtern**. **d.** Tippen Sie im Abschnitt **SMS-Filter** auf **Schutz**. **e.** Tippen Sie auf **Aktivieren**. Diese Anweisungen finden Sie auch in der CylancePROTECT Mobile-App unter **Gerätezustand** > **Nachrichtenscan**. Wenn Sie die iMessage-App verwenden, aktivieren Sie die Option **Als SMS senden** in der App.
Android	**a.** Tippen Sie in der CylancePROTECT Mobile-App auf **Gerätezustand**. **b.** Tippen Sie zum Erweitern auf **Nachrichtenscan**. **c.** Aktivieren Sie die Nachrichtenscanfunktion. **d.** Tippen Sie auf dem Bildschirm **Nachrichtenscan zulassen** auf **Zulassen**. **e.** Tippen Sie auf **OK**.

In der CylancePROTECT Mobile-App wird die Statusmeldung „Scannen aktiviert“ angezeigt.

Abwehren von mobilen Bedrohungen

Wenn die CylancePROTECT Mobile-App mobile Bedrohungen auf Ihrem Gerät erkennt, erhalten Sie eine Gerätebenachrichtigung. Sie können die CylancePROTECT Mobile-App öffnen, um die Bedrohungen schnell zu identifizieren und abzuwehren.

1. Öffnen Sie die CylancePROTECT Mobile-App.
2. Tippen Sie auf **Gerätezustand**.
3. Erweitern Sie einen der folgenden Abschnitte:
   - App-Sicherheit
   - Gerätesicherheit
   - Netzwerkschutz
4. Verwenden Sie die folgende Tabelle, um Bedrohungen abzuwehren, die auf dem Gerät erkannt worden sind.

Funktion	Plattform	Beschreibung	Auflösung
App-Sicherheit			
Schädliche Apps	Android	Erweitern Sie den Abschnitt, um eine Liste aller schädlichen Apps anzuzeigen, die die App erkannt hat.	Tippen Sie auf **Beheben**, um eine schädliche App vom Betriebssystem des Geräts zu deinstallieren.
Apps mit Seitenladefunktion	Android iOS	Sideloading-Apps sind Apps, die aus unbekannten oder nicht vertrauenswürdigen Quellen installiert wurden. Erweitern Sie auf Android-Geräten den Abschnitt, um eine Liste aller von der App erkannten Sideloading-Apps anzuzeigen. Erweitern Sie auf iOS-Geräten den Abschnitt, um eine Liste der vertrauenswürdigen und auf Ihrem Gerät installierten Anwendungsentwicklerprofile von Drittanbietern anzuzeigen.	Tippen Sie auf **Beheben**, um Anweisungen zum Entfernen der Sideloading-App anzuzeigen. Auf Android-Geräten werden Sie zu den Geräteeinstellungen weitergeleitet, um die App zu deinstallieren. Auf iOS-Geräten werden Sie zur App „Einstellungen“ weitergeleitet, um das Profil der vertrauenswürdigen App von Ihrem Gerät zu entfernen.
Gerätesicherheit			
Entwickleroptionen	Android	Entwickleroptionen gibt an, ob der Entwicklermodus auf dem Gerät aktiviert ist.	Tippen Sie auf **Beheben**, um Anweisungen zum Deaktivieren des Entwicklermodus anzuzeigen. Sie werden zu den Geräteeinstellungen weitergeleitet, um den Entwicklermodus zu deaktivieren.

Funktion	Plattform	Beschreibung	Auflösung
Root-Erkennung	Android iOS	Bei der Root-Erkennung wird eine Benachrichtigung angezeigt, wenn die App ein Rooting oder einen Jailbreak des Geräts erkennt.	Die App reagiert nicht. Wenden Sie sich an Ihren Administrator, um das Problem zu lösen.
Verschlüsselung des gesamten Datenträgers	Android	Verschlüsselung des gesamten Datenträgers zeigt an, ob die Datenträgerverschlüsselung auf dem Gerät aktiviert ist.	Tippen Sie auf **Beheben**, um Anweisungen zum Aktivieren der Datenträgerverschlüsselung anzuzeigen. Sie werden zu den Geräteeinstellungen weitergeleitet, um die Datenträgerverschlüsselung zu aktivieren.
Bildschirmsperre	Android iOS	Bildschirmsperre zeigt an, ob derzeit eine Bildschirmsperroption (z. B. ein Kennwort oder ein Fingerabdruck) auf dem Gerät aktiviert ist.	Tippen Sie auf **Beheben**, um Anweisungen zum Aktivieren einer Bildschirmsperre anzuzeigen. Auf Android-Geräten werden Sie aufgefordert, zu den Geräteeinstellungen zu wechseln, um eine Bildschirmsperre zu aktivieren.

Funktion	Plattform	Beschreibung	Auflösung
Integritätsnachweis für Geräte	Android iOS	Auf Android-Geräten wird eine Benachrichtigung angezeigt, wenn die CylancePROTECT Mobile-App einen der folgenden Punkte nicht erfüllt: • SafetyNet-Nachweis • Hardwarezertifikat-Nachweis • Sicherheitsebene des Hardwarenachweises ist niedriger als in der CylancePROTECT Mobile-Richtlinie konfiguriert • Sicherheitspatchebene des Hardwarenachweises ist niedriger als in der CylancePROTECT Mobile-Richtlinie konfiguriert • Bootstatus des Hardwarenachweises ist nicht verifiziert Auf iOS-Geräten wird eine Benachrichtigung angezeigt, wenn die CylancePROTECT Mobile-App eine Integritätsprüfung unter Verwendung des Apple DeviceCheck-Frameworks nicht besteht.	Wenn bei Android-Geräten die Sicherheitspatchebene nicht dem konfigurierten Mindestpatch entspricht, tippen Sie auf **Beheben**, um nach Software-Updates zu suchen. Für weitere Nachweiswarnungen und Integritätsprüfungen gibt es keine Aktion in der App. Wenden Sie sich an Ihren Administrator, um das Problem zu lösen.
Gerätebetriebssystem	Android iOS	Das Gerätebetriebssystem gibt an, ob das Gerätebetriebssystem die Anforderungen der Ihnen zugewiesenen CylancePROTECT-Richtlinie erfüllt.	Tippen Sie auf **Beheben**, um Anweisungen zum Aktualisieren des Betriebssystems anzuzeigen. Auf Android-Geräten werden Sie zu den Geräteeinstellungen weitergeleitet, um das Betriebssystem zu aktualisieren.
Gerätemodell	Android iOS	Das Gerätemodell gibt an, ob das Gerätemodell die Anforderungen der Ihnen zugewiesenen CylancePROTECT-Richtlinie erfüllt.	In der App muss keine Aktion ausgeführt werden. Wenden Sie sich an Ihren Administrator, um das Problem zu lösen.
Netzwerkschutz			

Funktion	Plattform	Beschreibung	Auflösung
Netzwerkverbindung	Android iOS	Die Netzwerkverbindung zeigt an, ob das aktuelle Netzwerk unsicher ist.	Tippen Sie auf **Beheben**, um Anweisungen zum Trennen der Verbindung zu einem unsicheren Netzwerk anzuzeigen. Auf Android-Geräten gibt es eine Option, zu den Geräteeinstellungen zu wechseln, um die Verbindung zum Netzwerk zu trennen.
Wi-Fi-Sicherheit	Android	Wi-Fi-Sicherheit gibt an, ob das aktuelle Wi-Fi-Netzwerk unsicher ist.	Tippen Sie auf **Beheben**, um Anweisungen zum Trennen vom Wi-Fi-Netzwerk anzuzeigen. Auf Android-Geräten gibt es eine Option, zu den Geräteeinstellungen zu wechseln, um die Verbindung zum Wi-Fi-Netzwerk zu trennen.
Nachrichtenscanfunktionen			
Malware-Nachrichten erkannt	Android iOS	Identifizieren von SMS-Textnachrichten mit potenziell schädlichen URLs.	Tippen Sie auf Android-Geräten auf **Beheben**, um zur Standard-Messaging-App zu wechseln und die Textnachrichten zu löschen. Auf iOS-Geräten werden die Textnachrichten automatisch per Filter in den Spam-Ordner verschoben.

Von der CylancePROTECT Mobile-App erkannte mobile Bedrohungen

Die folgenden Bedrohungen können in der CylancePROTECT Mobile-App angezeigt werden:

Mobile Sicherheitsbedrohung	Risikoniveau	Farbe
Schädliche Apps	Hoch	Rot
Apps mit Seitenladefunktion	Hoch	Rot
Gerätesicherheit: Entwickleroptionen	Mittel	Gelb
Gerätesicherheit: Bildschirmsperre	Mittel	Gelb

Mobile Sicherheitsbedrohung	Risikoniveau	Farbe
Gerätesicherheit: gerootete oder kompromittierte Geräte	Hoch	Rot
Gerätesicherheit: Vollständige Festplattenverschlüsselung	Mittel	Gelb
Gerätesicherheit: Nachweis	Hoch	Rot
Gerätesicherheit: Sicherheitspatch-Stufe	Mittel	Gelb
Gerätesicherheit: Gerätebetriebssystem	Mittel	Gelb
Gerätesicherheit: Gerätemodell	Mittel	Gelb
Netzwerkschutz: Netzwerkverbindung	Hoch	Rot
Netzwerkschutz: Wi-Fi-Sicherheit	Mittel	Gelb
Scannen von SMS-Nachrichten (Anzeige nur für Android)	Mittel	Gelb

Deaktivieren der CylancePROTECT Mobile-App

Wenn Sie die App deaktivieren, erhält Ihr Gerät keine Benachrichtigungen mehr mit Warnungen vor Sicherheitsrisiken. Die CylanceGATEWAY-Funktion ist auch nicht für den Zugriff auf Arbeitsressourcen und Anwendungen verfügbar.

Bevor Sie beginnen: Vergewissern Sie sich, dass Ihr Gerät mit dem Wi-Fi-Netzwerk verbunden ist.

Führen Sie auf dem Startbildschirm der CylancePROTECT Mobile-App einen der folgenden Schritte aus:

Gerät	Schritte
iOS	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Deaktivieren**. **c.** Tippen Sie erneut auf **Deaktivieren**.
Android	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Deaktivieren**. **c.** Tippen Sie erneut auf **Deaktivieren**. **d.** Tippen Sie auf **OK**.

Wenn Sie fertig sind: Löschen Sie die CylancePROTECT Mobile-App von Ihrem Gerät.

Melden eines Problems an BlackBerry

1. Tippen Sie auf dem Startbildschirm der CylancePROTECT Mobile-App auf .
2. Tippen Sie auf **Ein Problem melden**.
3. Geben Sie einen Kommentar zu dem Problem ein.
4. Tippen Sie auf **Senden**.

Was sind Cylance Endpoint Security-Agenten?

Die Cylance Endpoint Security-Agenten werden auf Desktop-Computern ausgeführt und in der Regel von einem Administrator bereitgestellt und automatisch auf Geräten installiert. In der folgenden Tabelle werden die Desktop-Agenten und deren Verwendung aufgeführt und beschrieben.

Agent	Aufgaben	Verwendung
CylancePROTECT Desktop	CylancePROTECT Desktop erkennt und blockiert Malware, bevor diese Geräte beeinträchtigen kann.	Ihr Administrator stellt die automatische Installation auf Ihrem Gerät bereit oder gibt Anweisungen zur manuellen Installation. CylancePROTECT Desktop wird nach der Anmeldung auf Ihrem Gerät im Hintergrund ausgeführt.
CylanceOPTICS	CylanceOPTICS ist eine Endpunkterkennungs- und Reaktionslösung, die forensische Daten von Geräten sammelt und analysiert, um Bedrohungen zu identifizieren und zu lösen, bevor sie sich auf die Benutzer und Daten Ihres Unternehmens auswirken.	Ihr Administrator stellt die automatische Installation auf Ihrem Gerät bereit oder gibt Anweisungen zur manuellen Installation. CylanceOPTICS wird nach der Anmeldung auf Ihrem Gerät im Hintergrund ausgeführt.
CylanceGATEWAY (Desktop-Agent)	CylanceGATEWAY bietet sicheren Zugriff auf die lokalen und Cloud-basierten Ressourcen, Dienste und Anwendungen Ihres Unternehmens, ohne dass ein herkömmliches VPN erforderlich ist. Darüber hinaus werden Geräte geschützt, indem es Ihrem Unternehmen ermöglicht wird, Verbindungen zu unsicheren und potenziell schädlichen Internetzielen zu blockieren.	Ihr Administrator stellt die automatische Installation auf Ihrem Gerät bereit oder gibt Anweisungen zur manuellen Installation. Sie müssen die Aktivierung von CylanceGATEWAY mit Ihren Verzeichniszugangsdaten oder BlackBerry Online Account-Zugangsdaten vornehmen. Nach der Aktivierung von CylanceGATEWAY aktivieren Sie den Arbeitsmodus über den Agenten.

Agent	Aufgaben	Verwendung
CylanceAVERT	CylanceAVERT identifiziert und kategorisiert vertrauliche Dateien, die in der Unternehmensumgebung gefunden wurden. Wenn diese vertraulichen Dateien im Zusammenhang mit einem Versuch der Datenexfiltration über verschiedene Quellen (USB- oder Netzlaufwerk, E-Mail-Nachrichten oder Browser-Uploads) stehen, kann CylanceAVERT eine vom Administrator festgelegte Korrekturmaßnahme zum Schutz Ihrer Daten durchführen.	Ihr Administrator stellt die automatische Installation auf Ihrem Gerät bereit oder gibt Anweisungen zur manuellen Installation. CylanceAVERT wird nach der Anmeldung auf Ihrem Gerät im Hintergrund ausgeführt.

Aktivieren des Arbeitsmodus im CylanceGATEWAY-Agenten

Wenn Ihr Administrator CylanceGATEWAY für Sie konfiguriert hat, können Sie den Arbeitsmodus im CylanceGATEWAY-Agenten auf Windows- und macOS-Geräten aktivieren, um sicher auf Netzwerkressourcen zuzugreifen und Ihr Gerät vor verdächtigen und potenziell schädlichen Netzwerkaktivitäten zu schützen. Wenn Sie den Arbeitsmodus aktivieren, stellt CylanceGATEWAY sichere Verbindungen zwischen Ihrem Gerät und dem Netzwerk Ihres Unternehmens her, analysiert Ihre Netzwerkaktivitäten und wendet die vom Administrator verwalteten Richtlinien für den Netzwerkzugriff an.

Bevor Sie beginnen:

- Installieren Sie den CylanceGATEWAY-Agent. Um den Agenten herunterzuladen, gehen Sie zur BlackBerry-Website und scrollen Sie nach unten zum Abschnitt „CylanceGATEWAY herunterladen“.
- Aktivieren Sie den Agenten mit Ihrem Verzeichnis oder mit den BlackBerry Online Account-Zugangsdaten. Weitere Informationen zur Aktivierung des Agenten finden Sie in der CylanceGATEWAY-Aktivierungs-E-Mail, die Sie von Ihrem Administrator erhalten haben.

1. Öffnen Sie auf Ihrem Computer den CylanceGATEWAY-Agenten.
2. Klicken Sie auf **Arbeitsmodus aktivieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Wenn die Verbindung hergestellt ist, wird der Status „Arbeitsmodus aktiviert“ angezeigt.

Wenn Sie fertig sind: Sie können die Einstellungen für den CylanceGATEWAY-Agenten konfigurieren.

CylanceGATEWAY-Agent-Einstellungen

Sie können Einstellungen für den CylanceGATEWAY-Agent konfigurieren. Die Einstellungsnamen können je nach Betriebssystem des Geräts unterschiedlich angezeigt werden.

Einstellung	Beschreibung
Deaktivieren	Klicken Sie auf diese Schaltfläche, um den CylanceGATEWAY-Agenten zu deaktivieren. Wenn der Agent deaktiviert ist, kann er keine Richtlinienaktualisierungen von CylanceGATEWAY empfangen.

Einstellung	Beschreibung
Ein Problem melden	Klicken Sie auf diese Schaltfläche, um einen Problembericht an BlackBerry zu senden.
TCP verwenden	Aktivieren Sie diese Option, um TCP für Verbindungen zu CylanceGATEWAY zu verwenden, wenn die Firewall Ihres Unternehmens keine UDP-Verbindungen zulässt.
CylanceGATEWAY automatisch starten, wenn ich mich an diesem Computer anmelde	Aktivieren Sie diese Option, um den CylanceGATEWAY-Agenten zu starten, wenn Sie sich auf Ihrem Windows- oder macOS-Gerät anmelden.
Arbeitsmodus automatisch aktivieren, wenn CylanceGATEWAY gestartet wird	Aktivieren Sie diese Option, um den Arbeitsmodus zu aktivieren, wenn der CylanceGATEWAY-Agent gestartet wird.

Wichtig: Wenn Sie möchten, dass der CylanceGATEWAY-Agent den Arbeitsmodus bei jeder Anmeldung bei Ihrem Windows- oder macOS-Gerät automatisch startet und aktiviert, müssen Sie beide Kontrollkästchen auswählen, **CylanceGATEWAY starten, wenn ich mich an diesem Computer anmelde** und **Arbeitsmodus automatisch aktivieren, wenn CylanceGATEWAY gestartet wird**.

Rechtliche Hinweise

Dieses Dokument und alle Dokumente, die per Verweis in dieses Dokument mit einbezogen werden, z. B. alle über die BlackBerry-Webseite erhältlichen Dokumente, werden ohne Mängelgewähr und je nach Verfügbarkeit bereitgestellt. Die entsprechenden Dokumente werden ohne ausdrückliche Billigung, Gewährleistung oder Garantie seitens BlackBerry Limited und seinen angegliederten Unternehmen („BlackBerry“) bereitgestellt. BlackBerry übernimmt keine Verantwortung für eventuelle typografische, technische oder anderweitige Ungenauigkeiten sowie für Fehler und Auslassungen in den genannten Dokumenten. Die BlackBerry-Technologie ist in dieser Dokumentation teilweise in verallgemeinerter Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von BlackBerry zu schützen. BlackBerry behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. BlackBerry ist jedoch nicht verpflichtet, die Benutzer über diese Änderungen, Updates, Verbesserungen oder Zusätze rechtzeitig bzw. überhaupt in Kenntnis zu setzen.

Diese Dokumentation enthält möglicherweise Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Dienste, einschließlich Komponenten und Inhalte wie urheberrechtlich geschützte Inhalte und/oder Websites von Drittanbietern (nachfolgend „Drittprodukte und -dienste“ genannt). BlackBerry hat keinen Einfluss auf und übernimmt keine Haftung für Drittprodukte und -dienste, dies gilt u. a. für Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Kompatibilität, Leistung, Zuverlässigkeit, Rechtmäßigkeit, Angemessenheit, Links oder andere Aspekte der Drittprodukte und -dienste. Der Einschluss eines Verweises auf Drittprodukte und -dienste in dieser Dokumentation impliziert in keiner Weise eine besondere Empfehlung der Drittprodukte und -dienste oder des Drittanbieters durch BlackBerry.

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE,

STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUST GESCHÄFTLICHER DATEN, ENTGANGENE GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUST VON DATEN, DAS UNVERMÖGEN, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEME IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON MOBILFUNKDIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS ÜBERNIMMT BLACKBERRY KEINERLEI VERANTWORTUNG, VERPFLICHTUNG ODER HAFTUNG, SEI SIE VERTRAGLICHER, DELIKTRECHTLICHER ODER ANDERWEITIGER NATUR, EINSCHLIESSLICH DER HAFTUNG FÜR FAHRLÄSSIGKEIT UND DER DELIKTSHAFTUNG.

DIE IN DIESEM DOKUMENT GENANNTEN EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTEN KLAGEGRÜNDE, FORDERUNGEN ODER KLAGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, FAHRLÄSSIGKEIT, ZIVILRECHTLICHER DELIKTE, DELIKTSHAFTUNG ODER SONSTIGE RECHTSTHEORIE UND SIND AUCH NACH EINEM WESENTLICHEN VERSTOSS BZW. EINEM FEHLENDEN GRUNDLEGENDEN ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTEN, VERTRETER, LIEFERANTEN (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTEN UND UNABHÄNGIGEN AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTEN EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTEN, VERTRETER, DISTRIBUTOREN, LIEFERANTEN, UNABHÄNGIGEN AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDEN UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Mobilfunktarifen und Funktionen. Für die Installation oder Verwendung von Drittprodukten und -diensten mit den Produkten und Diensten von BlackBerry sind u. U. Patent-, Marken-, Urheberrechts- oder sonstige Lizenzen erforderlich, damit die Rechte Dritter nicht verletzt werden. Es liegt in Ihrer Verantwortung, zu entscheiden, ob Sie Drittprodukte und -dienste verwenden möchten, und festzustellen, ob hierfür Lizenzen erforderlich sind. Für den Erwerb etwaiger Lizenzen sind Sie verantwortlich. Installieren oder verwenden Sie Drittprodukte und -dienste erst nach dem Erwerb aller erforderlichen Lizenzen. Alle Drittprodukte und -dienste, die Sie mit Produkten und Diensten von BlackBerry erhalten, werden lediglich zu Ihrem Vorteil, OHNE MÄNGELGEWÄHR und ohne ausdrückliche oder stillschweigende Bedingung, Billigung, Garantie, Zusicherung oder Gewährleistung jedweder Art von BlackBerry bereitgestellt. BlackBerry übernimmt in diesem Zusammenhang keinerlei Haftung. Die Verwendung von Drittprodukten und -diensten unterliegt Ihrer Zustimmung zu den Bedingungen separater Lizenzen und anderer geltender Vereinbarungen mit Dritten, sofern sie nicht ausdrücklich von einer Lizenz oder anderen Vereinbarung mit BlackBerry abgedeckt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIEN, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

BlackBerry Enterprise Software enthält bestimmte Softwarekomponenten von Drittanbietern. Die mit der Software verbundenen Lizenz- und Copyright-Informationen finden Sie unter: http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Kanada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
Großbritannien

Veröffentlicht in Kanada