BlackBerry UEM

E-Mail, Kalender und Kontakte verwalten

12.20

Inhalt

Einrichten des geschäftlichen E-Mail-Kontos für Geräte

Die folgenden Optionen sind verfügbar, wenn Sie geschäftliche E-Mail-Konten für Geräte einrichten möchten.

Geschäftliche E-Mail-Option	Wichtige Funktionen von
BlackBerry Work	BlackBerry Work synchronisiert sicher geschäftliche E-Mails, Kalender und Kontakte. Sie können auch Online-Präsenz anzeigen und auf geschäftliche Dokumente zugreifen. Im Gegensatz zu integrierten E-Mail-Clients sind bei BlackBerry Work diese Funktionen in einer einzigen, benutzerfreundlichen App integriert. Weitere Informationen zum Verwalten von BlackBerry Work finden Sie unter Verwalten von Apps und im Administratorhandbuch für BlackBerry Work.
E-Mail-Profile	Sie können E-Mail-Profile verwenden, um Geräte mit dem Mailserver Ihres Unternehmens zu verbinden und E-Mail-Nachrichten und Terminplanerdaten mithilfe von Exchange ActiveSync oder IBM Notes Traveler zu synchronisieren. Sie können beispielsweise E-Mail-Profile verwenden, um integrierte E-Mail-Apps einzurichten. E-Mail-Profile sind für BlackBerry Work nicht erforderlich.
IMAP/POP3 E-Mail-Profile	Sie können IMAP- und POP3-E-Mail-Profile verwenden, damit Geräte sich mit IMAP- oder POP3-Mailservern verbinden können, nur um E-Mail-Nachrichten zu synchronisieren.

Steuern, welche Geräte auf Exchange ActiveSync für geschäftliche E-Mail- und Terminplanerdaten zugreifen können

Wenn Ihr Unternehmen Microsoft Exchange ActiveSync verwendet, können Sie den unbefugten Zugriff auf Exchange ActiveSync durch Geräte unterbinden, die nicht explizit auf einer Positivliste aufgeführt sind. Geräte, die nicht auf dieser Liste stehen, können nicht auf geschäftliche E-Mail-Daten und Terminplanerdaten zugreifen.

Mit BlackBerry Gatekeeping Service können Geräte einfach einer Positivliste hinzugefügt werden, indem sie automatisch hinzugefügt werden. Sie können den BlackBerry Gatekeeping Service verwenden, unabhängig davon, ob Sie E-Mail-, Kalender- und Kontaktzugriff auf Benutzergeräten über BlackBerry Dynamics-Apps (wie BlackBerry Work) oder E-Mail-Profile verwalten.

Zum Konfigurieren und Verwenden des BlackBerry Gatekeeping Service gehen Sie wie folgt vor:

1. Erstellen Sie eine Gatekeeping-Konfiguration für Microsoft Exchange Server oder Microsoft 365.
2. Weisen Sie ein Gatekeeping-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.
3. Konfigurieren Sie ein E-Mail-Profil oder BlackBerry Work, um sich auf den automatischen Gatekeeping-Server zu beziehen.

Wenn das Gatekeeping-Profil, E-Mail-Profil oder die E-Mail-App für einen Benutzer entfernt wird, wird das Gerät des Benutzers aus der Positivliste entfernt und kann keine Verbindung zu Microsoft Exchange mehr herstellen, sofern es nicht über andere Methoden zugelassen wurde (z. B. Windows PowerShell).

Bei den meisten Geräten kann nur ein E-Mail-Client zur Positivliste hinzugefügt werden. Bei Android Enterprise- und Samsung Knox-Geräten, die eine App-Konfiguration verwenden, die für Exchange Server zulässige Daten enthält, ist die Priorität für das Zulassen von E-Mail-Anwendungen wie folgt:

1. E-Mail-Anwendungen mit Anwendungskonfigurationen, die die zulässigen Daten vom Exchange Server enthalten
2. BlackBerry Work
3. E-Mail-Client, für den die Exchange ActiveSync-ID während der Registrierung gesendet wird

Wenn Ihr Unternehmen BlackBerry UEM in einer lokalen Umgebung verwendet, können Sie eine oder mehrere Instanzen des BlackBerry Connectivity Node installieren, um weitere Instanzen der Geräteverbindungskomponenten zur Domäne Ihres Unternehmens hinzuzufügen. Jeder BlackBerry Connectivity Node umfasst eine Instanz des BlackBerry Gatekeeping Service. Jede Instanz muss in der Lage sein, auf den Gatekeeping-Server Ihres Unternehmens zuzugreifen. Wenn Gatekeeping-Daten nur von dem BlackBerry Gatekeeping Service verwaltet werden sollen, der mit den primären UEM-Komponenten installiert ist, können Sie die Standardeinstellungen ändern, um BlackBerry Gatekeeping Service in jedem BlackBerry Connectivity Node zu deaktivieren.

Wenn Ihr Unternehmen UEM Cloud verwendet, können Sie eine oder zwei zusätzliche Instanzen von BlackBerry Connectivity Node installieren, um weitere Instanzen der Geräteverbindungskomponenten zur Domäne Ihres Unternehmens hinzuzufügen. Jeder BlackBerry Connectivity Node umfasst eine Instanz des BlackBerry Gatekeeping Service. Jede Instanz muss in der Lage sein, auf den Exchange ActiveSync-Server Ihres Unternehmens zuzugreifen. Wenn die Exchange ActiveSync-Zugriffseinstellungen nur vom BlackBerry Gatekeeping Service verwaltet werden sollen, der mit dem primären BlackBerry Connectivity Node installiert wurde, können Sie die Standardeinstellungen ändern, um den BlackBerry Gatekeeping Service in den weiteren BlackBerry Connectivity Node-Instanzen zu deaktivieren.

Sie können BlackBerry Connectivity Node-Servergruppen einrichten, um den Verbindungsdatenverkehr des Geräts an eine bestimmte regionale Verbindung zur BlackBerry Infrastructure zu richten. Wenn Sie ein Gatekeeping-Profil mit einer Servergruppe verknüpfen, verwendet jeder Benutzer, dem dieses Gatekeeping-Profil zugewiesen wurde, eine aktive Instanz des BlackBerry Gatekeeping Service in dieser Servergruppe. Beim Konfigurieren

einer Servergruppe können Sie festlegen, dass die Instanzen des BlackBerry Gatekeeping Service in der Gruppe deaktiviert werden. Siehe Erstellen einer Servergruppe zum Verwalten regionaler Verbindungen in der Dokumentation zur Konfiguration.

Schritte zum Konfigurieren von Exchange ActiveSync und BlackBerry Gatekeeping Service

Zum Konfigurieren des BlackBerry Gatekeeping Service führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Konfigurieren von Berechtigungen für Gatekeeping.
2	Wenn Ihr Unternehmen Microsoft Exchange Server verwendet, lesen Sie die Informationen unter Konfigurieren von Microsoft Exchange für den ausschließlichen Zugriff autorisierter Geräte auf Exchange ActiveSync. Wenn Ihr Unternehmen Microsoft 365 verwendet, lesen Sie die Informationen unter Konfigurieren der Zugriffsrichtlinie für mobile Geräte in Microsoft 365.
3	Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.
4	Hinzufügen einer Entra-App und Erhalt ihrer Entra-Details für die Konfiguration der modernen Authentifizierung
5	Erstellen einer Gatekeeping-Konfiguration.
6	Erstellen Sie ein Gatekeeping-Profil, und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Konfigurieren von Berechtigungen für Gatekeeping

Zur Verwendung von Exchange ActiveSync Gatekeeping müssen Sie ein Benutzerkonto in Microsoft Exchange Server oder Microsoft 365 erstellen und diesem die erforderlichen Gatekeeping-Berechtigungen zuweisen.

Wenn Sie Microsoft 365 verwenden, erstellen Sie ein Microsoft 365-Benutzerkonto, und ordnen Sie es den E-Mail-Empfänger- und Clientzugriffsrollen des Unternehmens zu.

Wenn Sie Microsoft Exchange Server verwenden, folgen Sie den nachstehenden Anweisungen zum Konfigurieren der Verwaltungsrollen mit den korrekten Berechtigungen zum Verwalten der Postfächer und des Clientzugriffs für Exchange ActiveSync. Für die Durchführung dieses Schritts ist es erforderlich, Microsoft Exchange-Administrator mit den entsprechenden Berechtigungen zum Erstellen und Ändern von Verwaltungsrollen zu sein.

Bevor Sie beginnen:

- Erstellen Sie auf dem Computer, der Microsoft Exchange hostet, ein Konto und ein Postfach für die Verwaltung von Gatekeeping in BlackBerry UEM (z. B. BUEMAdmin). Sie müssen die Anmeldeinformationen für dieses

Konto festlegen, wenn Sie eine Exchange ActiveSync-Konfiguration erstellen. Notieren Sie sich den Namen dieses Kontos, da Sie diesen am Ende der folgenden Aufgabe eingeben müssen.

- WinRM muss mit den Standardeinstellungen auf dem Computer konfiguriert werden, der den Microsoft Exchange Server hostet, den Sie für Gatekeeping festlegen. Sie müssen den Befehl `Winrm quickconfig` von einer Eingabeaufforderung als Administrator ausführen. Wenn das Tool `Make these changes [y/n]` anzeigt, geben Sie y ein. Nach der erfolgreichen Ausführung des Befehls sehen Sie die folgende Meldung.

```
WinRM has been updated for remote management.

WinRM service type changed to delayed auto start.
WinRM service started.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on
 this
 machine.
```

1. Öffnen Sie den Microsoft Exchange Management Shell.
2. Geben Sie `New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"` ein. Drücken Sie die Eingabetaste.
3. Geben Sie `New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"` ein. Drücken Sie die Eingabetaste.
4. Geben Sie `New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"` ein. Drücken Sie die Eingabetaste.
5. Geben Sie `Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry` ein. Drücken Sie die Eingabetaste.
6. Geben Sie `Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry` ein. Drücken Sie die Eingabetaste.
7. Geben Sie `Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry` ein. Drücken Sie die Eingabetaste.
8. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox` ein. Drücken Sie die Eingabetaste.
9. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity` ein. Drücken Sie die Eingabetaste.
10. Geben Sie `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox` ein. Drücken Sie die Eingabetaste.
11. Geben Sie `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox` ein. Drücken Sie die Eingabetaste.
12. Geben Sie `Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs` ein. Drücken Sie die Eingabetaste.
13. Geben Sie `New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"` ein. Drücken Sie die Eingabetaste.
14. Geben Sie `Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"` ein. Drücken Sie die Eingabetaste.
15. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"` ein. Drücken Sie die Eingabetaste.
16. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm` ein. Drücken Sie die Eingabetaste.

17. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm` ein. Drücken Sie die Eingabetaste.

Wenn Sie fertig sind:

- Wenn Ihr Unternehmen Microsoft Exchange Server verwendet, lesen Sie die Informationen unter Konfigurieren von Microsoft Exchange für den ausschließlichen Zugriff autorisierter Geräte auf Exchange ActiveSync.
- Wenn Ihr Unternehmen Microsoft 365 verwendet, lesen Sie die Informationen unter Konfigurieren der Zugriffsrichtlinie für mobile Geräte in Microsoft 365.

Konfigurieren von Microsoft Exchange für den ausschließlichen Zugriff autorisierter Geräte auf Exchange ActiveSync

Sie müssen Microsoft Exchange Server so konfigurieren, dass nur autorisierte Geräte Zugriff auf Exchange ActiveSync erhalten. Geräte bestehender Benutzer, die nicht explizit der Liste zulässiger Geräte in Microsoft Exchange hinzugefügt wurden, müssen unter Quarantäne gestellt werden, bis BlackBerry UEM sie zulässt.

Für die Durchführung dieses Schritts ist es erforderlich, Microsoft Exchange-Administrator mit den entsprechenden Berechtigungen für den Befehl „Set-ActiveSyncOrganizationSettings“ zu sein. Unter https://technet.microsoft.com finden Sie weitere Informationen über den Befehl und die Verwaltung von Geräten, die auf Exchange ActiveSync zugreifen.

Bevor Sie beginnen:

- Konfigurieren von Berechtigungen für Gatekeeping.
- Überprüfen Sie zusammen mit dem Microsoft Exchange-Administrator, ob es Benutzer gibt, die Exchange ActiveSync verwenden. Wenn die Standardzugriffsebene für Exchange ActiveSync für Ihr Unternehmen auf „Zulassen“ festgelegt ist und Sie Benutzer eingerichtet haben, die ihre Geräte erfolgreich synchronisieren, müssen Sie sicherstellen, dass den Konten bzw. Geräten dieser Benutzer eine Ausnahme oder Geräterichtlinie zugewiesen ist, bevor Sie die Standardzugriffsebene auf Quarantäne festlegen. Ist dies nicht der Fall, werden sie unter Quarantäne gestellt und ihre Geräte können erst dann synchronisiert werden, wenn sie von BlackBerry UEM zugelassen werden. Weitere Informationen zum Festlegen der Standardzugriffsebene für Exchange ActiveSync auf Quarantäne finden Sie unter support.blackberry.com/community im Artikel 36800.

1. Öffnen Sie auf einem Computer, der die Microsoft Exchange Management Shell hostet, die Microsoft Exchange Management Shell.
2. Geben Sie `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine` ein. Drücken Sie die Eingabetaste.

Wenn Sie fertig sind: Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.

Konfigurieren der Zugriffsrichtlinie für mobile Geräte in Microsoft 365

Zum Verwenden von BlackBerry Gatekeeping Service mit Microsoft 365 müssen Sie die Standardzugriffsrichtlinie für mobile Geräte in Microsoft 365 auf Quarantäne (Isolieren) festlegen.

Bevor Sie beginnen:

- Konfigurieren von Berechtigungen für Gatekeeping.
- Wenn die Standardzugriffsebene für Exchange ActiveSync für Ihr Unternehmen auf „Zulassen“ festgelegt ist und Sie Benutzer eingerichtet haben, die ihre Geräte erfolgreich synchronisieren, müssen Sie sicherstellen, dass den Konten bzw. Geräten dieser Benutzer eine Ausnahme oder Geräterichtlinie zugewiesen ist, bevor

Sie die Standardzugriffsebene auf Quarantäne festlegen. Ist dies nicht der Fall, werden sie unter Quarantäne gestellt und ihre Geräte können erst dann synchronisiert werden, wenn sie von BlackBerry UEM zugelassen werden. Weitere Informationen zum Festlegen der Standardzugriffsebene für Exchange ActiveSync auf Quarantäne finden Sie unter support.blackberry.com/community im Artikel 33531.

1. Melden Sie sich beim Microsoft 365-Verwaltungsportal an.
2. Klicken Sie im Menü auf **Admin**.
3. Klicken Sie auf **Exchange**.
4. Klicken Sie auf im Bereich **Mobil** auf **Zugriff auf mobile Geräte**.
5. Klicken Sie auf **Bearbeiten**.
6. Klicken Sie auf **Isolieren - Selbst entscheiden, ob blockiert oder später zugelassen werden soll**.

Wenn Sie fertig sind: Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.

Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping

Unter BlackBerry UEM werden Windows PowerShell-Befehle für die Verwaltung der Liste zulässiger Geräte verwendet. Um den BlackBerry Gatekeeping Service zu nutzen, müssen Sie Microsoft IIS-Berechtigungen konfigurieren.

Bevor Sie beginnen:

- Wenn Ihr Unternehmen Microsoft Exchange Server verwendet, lesen Sie die Informationen unter Konfigurieren von Microsoft Exchange für den ausschließlichen Zugriff autorisierter Geräte auf Exchange ActiveSync.
- Wenn Ihr Unternehmen Microsoft 365 verwendet, lesen Sie die Informationen unter Konfigurieren der Zugriffsrichtlinie für mobile Geräte in Microsoft 365.

1. Öffnen Sie auf dem Computer, auf dem die Microsoft-Client Access Server-Rolle gehostet wird, den Microsoft Internet Information Services (IIS)-Manager.
2. Erweitern Sie im linken Fensterbereich den Server.
3. Erweitern Sie **Websites** > **Standard-Website**.
4. Klicken Sie mit der rechten Maustaste auf den PowerShell-Ordner. Wählen Sie **Berechtigungen bearbeiten**.
5. Klicken Sie auf die Registerkarte **Sicherheit**. Klicken Sie auf **Bearbeiten**.
6. Klicken Sie auf **Hinzufügen**, und geben Sie die <neue_Gruppe> ein, die bei der Konfiguration der Microsoft Exchange-Berechtigungen für Gatekeeping erstellt wurde.
7. Klicken Sie auf **OK**.
8. Vergewissern Sie sich, dass **Lesen & Ausführen**, **Auflisten von Verzeichnisinhalten** und **Lesen** ausgewählt sind. Klicken Sie auf **OK**.
9. Wählen Sie den **PowerShell**-Ordner aus. Doppelklicken Sie auf das Symbol **Authentifizierung**.
10. Wählen Sie **Windows-Authentifizierung**. Klicken Sie auf **Aktivieren**.
11. Schließen Sie den Microsoft Internet Information Services (IIS) Manager.

Wenn Sie fertig sind: Erstellen einer Gatekeeping-Konfiguration.

Hinzufügen einer Entra-App und Erhalt ihrer Entra-Details für die Konfiguration der modernen Authentifizierung

Falls Sie BlackBerry UEM für die Verbindung zu Microsoft 365 mit der modernen Authentifizierung konfigurieren wollen, müssen Sie zwei App-Details angeben: App-ID und Unternehmen. Wenn Sie diese Schritte ausführen, wird

die Entra-App-ID im Abschnitt „Mitglieder auswählen“ angezeigt. Die Entra-Organisationsinformationen werden auf der Microsoft Entra ID-Seite als Eigenschaft des Verzeichnisses angezeigt. Zeichnen Sie diese beiden Einträge auf, um sie bei der Konfiguration von BlackBerry UEM für die moderne Authentifizierung im Gatekeeping-Profil zu verwenden.

1. Melden Sie sich bei portal.azure.com an.
2. Klicken Sie auf **App registrations**.
3. Klicken Sie auf **Neue Registrierung**.
4. Geben Sie im Feld **Name** einen Namen für die Anwendung ein.
5. Klicken Sie auf **Registrieren**.
6. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
7. Suchen Sie die Berechtigungsgruppe für **Exchange** oder **Office 365 Exchange Online**.
8. Klicken Sie auf **Anwendungsberechtigungen > Exchange.ManageAsApp > Berechtigung hinzufügen**.
9. Wählen Sie **Exchange.ManageAsApp > Administratorzustimmung erteilen** aus, um die Zustimmung des Administrators zu erteilen.
10. Klicken Sie im Abschnitt „Verwalten“ auf **Zertifikate und geheime Schlüssel > Zertifikat hochladen**, und wählen Sie den öffentlichen Schlüssel (cert.pem) aus.
11. Um der App eine Rolle zuzuweisen, klicken Sie auf der Entra-Startseite auf **Microsoft Entra ID**.
12. Klicken Sie auf **Rollen und Administratoren**.
13. Geben Sie im Abschnitt **Administratorrollen** „Exchange“ ein, um die unterstützten Rollen für Microsoft Exchange anzuzeigen.
14. Klicken Sie auf eine Rolle, um die Rollendetails anzuzeigen.
15. Klicken Sie auf **Zuweisungen hinzufügen**.
16. Klicken Sie unter **Mitglied auswählen** auf **Kein Mitglied ausgewählt**.
17. Suchen Sie anhand der App-ID oder des App-Namens nach der Entra-App-ID.
18. Wählen Sie die App aus, um sie in den Abschnitt **Ausgewählte Elemente** zu verschieben.
19. Klicken Sie auf **Select**.
20. Klicken Sie auf **Weiter**.
21. Stellen Sie auf der Seite **Zuweisungen hinzufügen** sicher, dass der **Zuweisungstyp** auf **aktiv** eingestellt ist. Weitere Informationen zu Zuweisungstypen finden Sie in den Informationen von Microsoft.
22. Klicken Sie auf **Zuweisen**.

Wenn Sie fertig sind: Verknüpfen eines Zertifikats mit der Entra-App-ID von UEM für moderne Authentifizierung

Verknüpfen eines Zertifikats mit der Entra-App-ID von UEM für moderne Authentifizierung

Sie können ein neues Client-Zertifikat von Ihrer Zertifizierungsstelle anfordern und exportieren oder ein selbstsigniertes Zertifikat verwenden. Der private Schlüssel muss das PFX-Format aufweisen. Der öffentliche Schlüssel kann als CER- oder PEM-Datei exportiert werden, um ihn in Microsoft Entra ID hochzuladen.

1. Führen Sie eine der folgenden Aufgaben aus:

Zertifikat	Aufgabe
Wenn Sie eine vorhandene Zertifizierungsstelle verwenden	**a.** Fordern Sie das Zertifikat an. Das Zertifikat, das Sie anfordern, muss den App-Namen im Betreff des Zertifikats enthalten. Dabei steht <*app name*> für den Namen, den Sie der App in Schritt 4 von Eine Entra-App hinzufügen und deren Entra-Details für die Konfiguration der modernen Authentifizierung erhalten zugewiesen haben. **b.** Exportieren Sie den öffentlichen Schlüssel des Zertifikats als CER- oder PEM-Datei. Der öffentliche Schlüssel wird für die erstellte Entra-App-ID verwendet. **c.** Exportieren Sie den privaten Schlüssel des Zertifikats als PFX-Datei.

Zertifikat	Aufgabe
Wenn Sie ein selbstsigniertes Zertifikat verwenden	**a.** Erstellen Sie ein selbstsigniertes Zertifikat mit dem Befehl ‚New-SelfSignedCertificate'. Weitere Informationen finden Sie unter docs.microsoft.com im Abschnitt „Neues selbst signiertes Zertifikat". **1.** Öffnen Sie auf dem Computer, auf dem Microsoft Windows ausgeführt wird, die Windows PowerShell. **2.** Geben Sie den folgenden Befehl ein: `$cert=New-SelfSignedCertificate -Subject "CN=<app name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`. Dabei steht <*app name*> für den Namen, den Sie der App in Schritt 4 von Eine Entra-App hinzufügen und deren Entra-Details für die Konfiguration der modernen Authentifizierung erhalten zugewiesen haben. Das Zertifikat, das Sie anfordern, muss im Feld „Betreff" den Namen der Entra-App enthalten. **3.** Drücken Sie die **Eingabetaste**. **b.** Exportieren Sie den öffentlichen Schlüssel aus der Microsoft Management Console (MMC). Stellen Sie sicher, dass Sie das öffentliche Zertifikat als CER- oder PEM-Datei speichern. Der öffentliche Schlüssel wird für die erstellte Entra-App-ID verwendet. **1.** Öffnen Sie auf dem Computer, auf dem Windows ausgeführt wird, den Zertifikat-Manager für den angemeldeten Benutzer. **2.** Erweitern Sie **Personal**. **3.** Klicken Sie auf **Zertifikate**. **4.** Klicken Sie mit der rechten Maustaste auf <*user*>@<*domain*>, und klicken Sie auf **Alle Aufgaben > Exportieren**. **5.** Klicken Sie im **Assistent zum Exportieren für Zertifikate** auf **Nein, privaten Schlüssel nicht exportieren**. **6.** Klicken Sie auf **Weiter**. **7.** Wählen Sie **Base-64 encoded X.509 (.CER)**. Klicken Sie auf **Weiter**. **8.** Geben Sie einen Namen für das Zertifikat ein und speichern Sie es auf Ihrem Desktop. **9.** Klicken Sie auf **Weiter**. **10.** Klicken Sie auf **Fertigstellen**. **11.** Klicken Sie auf **OK**. **c.** Exportieren Sie den privaten Schlüssel aus der Microsoft Management Console (MMC). Stellen Sie sicher, dass Sie den privaten Schlüssel mit aufnehmen und ihn als PFX-Datei speichern. **1.** Öffnen Sie auf dem Computer, auf dem Windows ausgeführt wird, den Zertifikat-Manager für den angemeldeten Benutzer. **2.** Erweitern Sie **Personal**. **3.** Klicken Sie auf **Zertifikate**. **4.** Klicken Sie mit der rechten Maustaste auf <*user*>@<*domain*>, und klicken Sie auf **Alle Aufgaben > Exportieren**. **5.** Klicken Sie im **Assistent zum Exportieren für Zertifikate** auf **Ja, privaten Schlüssel exportieren**. **6.** Klicken Sie auf **Weiter**. **7.** Wählen Sie **Austausch persönlicher Informationen – PKCS-Nr. 12 (PFX)** aus. Klicken Sie auf **Weiter**. **8.** Wählen Sie die Sicherheitsmethode aus. **9.** Geben Sie einen Namen für das Zertifikat ein und speichern Sie es auf Ihrem Desktop. **10.** Klicken Sie auf **Weiter**. **11.** Klicken Sie auf **Fertigstellen**.

2. Laden Sie das öffentliche Zertifikat (PEM- oder CER-Datei) hoch, das Sie in Schritt 1 exportiert haben, um die Anmeldeinformationen des Zertifikats mit der Entra-App-ID von UEM zu verknüpfen.
   a) Öffnen Sie in portal.azure.com den <*app name*>, den Sie der App in Schritt 4 von Eine Entra-App hinzufügen und deren Entra-Details für die Konfiguration der modernen Authentifizierung erhalten zugewiesen haben.
   b) Klicken Sie auf **Zertifikate und geheime Schlüssel**.
   c) Klicken Sie im Abschnitt **Zertifikate** auf **Zertifikat hochladen**.
   d) Gehen Sie im Suchfeld **Datei auswählen** zu dem Speicherort, an den Sie das Zertifikat exportiert haben.
   e) Klicken Sie auf **Hinzufügen**.

Erstellen einer Gatekeeping-Konfiguration

Sie können eine Gatekeeping-Konfiguration so erstellen, dass die den Sicherheitsrichtlinien Ihres Unternehmens entsprechenden Geräte eine Verbindung zu Microsoft Exchange Server oder Microsoft 365 herstellen können.

Bevor Sie beginnen:

- Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.
- Wenn Sie eine moderne Authentifizierung verwenden möchten, Hinzufügen einer Entra-App und Erhalt ihrer Entra-Details für die Konfiguration der modernen Authentifizierung.

1. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie BlackBerry UEM in einer lokalen Umgebung verwenden, klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Microsoft Exchange Gatekeeping**.
   - Wenn Sie BlackBerry UEM Cloud verwenden, klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > BlackBerry Gatekeeping Service**.
2. Klicken Sie im Abschnitt mit der Microsoft Exchange Server-Liste auf +.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Herstellen einer Verbindung zu Microsoft 365 mit moderner Authentifizierung	Bevor Sie BlackBerry UEM für die Verwendung der modernen Authentifizierung konfigurieren, müssen Sie ein Zertifikat mit öffentlichen und privaten Schlüsseln generieren. Sie können OpenSSL oder PowerShell verwenden, um das Zertifikat zu generieren. Weitere Informationen finden Sie unter Verknüpfen eines Zertifikats mit der Entra-App-ID für moderne Authentifizierung. **a.** Aktivieren Sie das Kontrollkästchen **Moderne Authentifizierung**. **b.** Geben Sie im Feld **Verbindungsname für Exchange Online** einen Namen für die Verbindung ein. **c.** Klicken Sie auf **Durchsuchen** , und wählen Sie das Zertifikat aus, das für die Authentifizierung verwendet werden soll. **d.** Geben Sie im Feld **Zertifikatskennwort** das Kennwort für das Zertifikat ein. **e.** Geben Sie Ihre **Entra-Anwendungs-ID** an. **f.** Geben Sie Ihr **Entra-Unternehmen** an.

Aufgabe	Schritte
Verbindung zu Microsoft Exchange Server oder Microsoft 365 mithilfe der Standardauthentifizierung herstellen	**a.** Geben Sie im Feld **Servername** den Namen der Microsoft Exchange Server- oder Microsoft 365-Umgebung ein, für die der Zugriff verwaltet werden soll. **b.** Geben Sie den Benutzernamen und das Kennwort für das Konto ein, das Sie für die Verwaltung von Exchange ActiveSync-Gatekeeping erstellt haben. **c.** Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** die unter Microsoft Exchange Server oder Microsoft 365 verwendete Authentifizierung aus. **d.** Um die SSL-Authentifizierung zwischen BlackBerry UEM und dem Microsoft Exchange Server oder Microsoft 365 zu ermöglichen, aktivieren Sie das Kontrollkästchen **SSL verwenden**. Optional können weitere Zertifikatprüfungen ausgewählt werden. **e.** Wählen Sie in der Dropdown-Liste **Proxy-Typ** ggf. die Art der Proxy-Konfiguration aus, die zwischen BlackBerry UEM und dem Microsoft Exchange Server oder Microsoft 365 verwendet wird. **f.** Wenn Sie im vorhergehenden Schritt eine Proxy-Konfiguration ausgewählt haben, wählen Sie den Authentifizierungstyp für den Proxy-Server aus. **g.** Wählen Sie bei Bedarf **Authentifizierung erforderlich**, und geben Sie den Benutzernamen und das Kennwort ein.

4. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob die Verbindung erfolgreich ist.
5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Erstellen eines Gatekeeping-Profils und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.
- Wenn Sie eine BlackBerry Connectivity Node-Servergruppe mit einer oder mehreren aktiven Instanzen des BlackBerry Gatekeeping Service konfiguriert haben, ordnen Sie das Gatekeeping-Profil der entsprechenden Servergruppe zu. Jeder Benutzer, dem dieses Gatekeeping-Profil zugewiesen ist, kann jede aktive Instanz des BlackBerry Gatekeeping Service in dieser Servergruppe verwenden.

Erstellen eines Gatekeeping-Profils

Nach dem Konfigurieren des BlackBerry Gatekeeping Service für das automatische Gatekeeping müssen Sie ein Gatekeeping-Profil erstellen und dieses Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen. Mit dem Gatekeeping-Profil können Sie die Microsoft Exchange-Gatekeeping-Server oder BlackBerry Connectivity Node-Servergruppen für das automatische Gatekeeping auswählen.

Wenn Sie BlackBerry Connectivity Node-Servergruppen verwenden, wählen Sie die entsprechende Servergruppe aus, die über eine oder mehrere aktive Instanzen des BlackBerry Gatekeeping Service verfügt. Jeder Benutzer, dem dieses Gatekeeping-Profil zugewiesen ist, kann jede aktive Instanz des BlackBerry Gatekeeping Service in dieser Servergruppe verwenden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **E-Mail, Kalender und Kontakte > Gatekeeping**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.

5. Klicken Sie auf **Server auswählen**.
6. Wählen Sie mindestens einen Server aus, und klicken Sie auf ➔.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie das Gatekeeping-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.
- Damit Benutzer auf geschäftliche E-Mails zugreifen können, müssen Sie ihnen ein E-Mail-Profil oder die BlackBerry Work-App zuweisen. Wenn Sie BlackBerry Work verwalten, müssen Sie den BlackBerry Gatekeeping Service-Dienst in der App-Konfiguration aktivieren.

Überprüfen, ob ein Gerät auf Exchange ActiveSync zugreifen darf

Wenn Ihr Unternehmen BlackBerry Gatekeeping Service verwendet, um zu steuern, welche Geräte Zugriff auf geschäftliche E-Mail- und Terminplanerdaten von Exchange ActiveSync haben, können Sie den Verbindungsstatus zwischen dem Gerät und Exchange ActiveSync überprüfen. Um eine Verbindung herzustellen, wird Benutzern ein E-Mail-Profil zugewiesen, mit dem mindestens ein Gatekeeping-Server verknüpft ist. Der Verbindungsstatus wird auf der Seite „Gerätedetails“ des Benutzerkontos neben dem E-Mail-Profil im Abschnitt „IT-Richtlinien und -Profile“ angezeigt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach dem Namen eines Benutzerkontos, und klicken Sie darauf.
3. Wählen Sie die Registerkarte für das zu überprüfende Gerät aus.
4. Beachten Sie im Abschnitt **IT-Richtlinien und -Profile** die folgenden Status.
   - **Zugelassene Verbindung**: Dieser Status wird angezeigt, wenn BlackBerry UEM die ID des Geräts kennt und das Gerät auf der Positivliste vorhanden ist.
   - **Ausstehende Verbindung**: Dieser Status wird angezeigt, wenn BlackBerry UEM die ID des Geräts kennt und das Gerät darauf wartet, zur Positivliste hinzugefügt zu werden.
   - **Unbekannt**: Dieser Status wird angezeigt, wenn BlackBerry UEM die ID des Geräts nicht bestimmen kann. Das Gerät wird in der Liste der gesperrten Geräten aufgeführt und muss der Positivliste manuell hinzugefügt werden.

Manuelles Erlauben oder Blockieren des Zugriffs auf Exchange ActiveSync

Wenn ein Gerät nicht automatisch der zulässigen Liste für den Zugriff auf Exchange ActiveSync hinzugefügt wird, können Sie den Zugriff darauf manuell über die BlackBerry UEM-Verwaltungskonsole zulassen. Wenn beispielsweise UEM die Exchange ActiveSync-ID des Geräts nicht abrufen kann, z. B. für ein Android-Gerät, das mit der Aktivierungsart MDM aktiviert wurde, müssen Sie das Gerät manuell zulassen, wenn Sie ihm Zugriff darauf gewähren möchten.

Sie können auch zuvor zugelassene Geräte vom Zugriff auf Exchange ActiveSync ausschließen. Der Ausschluss eines Geräts verhindert, dass es E-Mail-Nachrichten und andere Informationen vom Microsoft Exchange Server abruft.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Exchange Gatekeeping.**.
2. Suchen Sie in der Liste **Eingeschränkte Geräte** nach einem Gerät.
3. Führen Sie in der Spalte **Aktion** eine der folgenden Aktionen aus:
   - Um den Zugriff auf Exchange ActiveSync zu ermöglichen, klicken Sie auf ✓.

- Um den Zugriff auf Exchange ActiveSync zu blockieren, klicken Sie auf ⃠.

Erstellen von E-Mail-Profilen

Sie können E-Mail-Profile verwenden, um festzulegen, wie Geräte eine Verbindung zum Mailserver Ihres Unternehmens herstellen und E-Mail-Nachrichten und Terminplanerdaten mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren.

Sie müssen kein E-Mail-Profil verwenden, wenn Ihr Unternehmen BlackBerry Work für die Verwaltung von E-Mails, Kalender und Kontakte für Benutzergeräte verwendet. Weitere Informationen zum Verwalten von BlackBerry Work finden Sie unter Verwalten von Apps und im Administratorhandbuch für BlackBerry Work.

Wenn Sie Exchange ActiveSync verwenden möchten, sollten Sie beachten, dass:

- Exchange ActiveSync kann so konfiguriert werden, dass gesteuert wird, welche Geräte darauf zugreifen können.
- Zur Erhöhung der E-Mail-Sicherheit können Sie S/MIME für iOS- und Android-Geräte aktivieren.
- Wenn Sie S/MIME aktivieren, können Sie andere Profile verwenden, um S/MIME-Zertifikate automatisch mit den Geräten abzurufen und den Zertifikatstatus zu prüfen.

Wenn Sie Notes Traveler verwenden möchten, sollten Sie beachten, dass Sie für seine Verwendung mit iOS-Geräten das BlackBerry Secure Gateway aktivieren müssen.

Sie können auch mithilfe von IMAP/POP3-E-Mail-Profilen festlegen, wie iOS-, macOS-, Android- und Windows-Geräte eine Verbindung zu IMAP- oder POP3-Mailservern herstellen und E-Mail-Nachrichten synchronisieren. Geräte, die für die Verwendung von Knox MDM aktiviert wurden, unterstützen weder IMAP noch POP3.

Erstellen eines E-Mail-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen von dem in der Umgebung Ihrer Organisation genutzten E-Mail-Server ab.

Bevor Sie beginnen: Wenn Sie die zertifikatbasierte Authentifizierung zwischen Geräten und Ihrem E-Mail-Server verwenden, müssen Sie ein Profil für ein Zertifizierungsstellenzertifikat erstellen und Benutzern zuweisen. Sie müssen außerdem sicherstellen, dass die Geräte über ein vertrauenswürdiges Clientzertifikat verfügen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **E-Mail, Kalender und Kontakte > E-Mail**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie bei Bedarf den Domänennamen des Mailservers an. Wenn das Profil für mehrere Benutzer gilt, die sich in unterschiedlichen Microsoft Active Directory-Domänen befinden können, können Sie die Variable `%UserDomain%` verwenden.
6. Führen Sie im Feld **E-Mail-Adresse** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie die E-Mail-Adresse des Benutzers ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserEmailAddress%` ein.
7. Geben Sie den Hostnamen oder die IP-Adresse Mailservers ein.
8. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserName%` ein.
   - Wenn Sie das Profil für mehrere Benutzer in einer IBM Notes Traveler-Umgebung erstellen, geben Sie `%UserDisplayName%` ein.

9. Wenn Sie Servergruppen für direkten BlackBerry Secure Gateway-Datenverkehr zu einer bestimmten regionalen Verbindung zur BlackBerry Infrastructure konfiguriert haben, wählen Sie in der Dropdown-Liste **Servergruppe für BlackBerry Secure Gateway Service** die entsprechende Servergruppe aus.
10. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für jede Profileinstellung.
11. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
- Bei Android-Geräten mit MDM-Steuerelemente-Aktivierungen sendet BlackBerry UEM das E-Mail-Profil an das Gerät; der Benutzer muss die Verbindung zum Mailserver jedoch manuell konfigurieren.

E-Mail-Profileinstellungen

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. E-Mail-Profile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- macOS
- Android
- Windows

Allgemein: E-Mail-Profileinstellungen

Allgemein: E-Mail-Profileinstellung	Beschreibung
Domänenname	Diese Einstellung legt den Domänenname des Mailservers fest.
E-Mail-Adresse	Diese Einstellung legt die E-Mail-Adresse des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserEmailAddress%-Variable verwenden.
Hostname oder IP-Adresse	Diese Einstellung legt den Hostnamen oder die IP-Adresse Mailservers fest.
Benutzername	Diese Einstellung legt den Benutzernamen des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Wenn Sie das Profil für mehrere Benutzer in einer IBM Notes Traveler-Umgebung erstellen, verwenden Sie %UserDisplayName%.
Automatische Gatekeeping-Server	Wenn Sie Servergruppen für direkten BlackBerry Secure Gateway-Datenverkehr oder BlackBerry Gatekeeping Service-Datenverkehr zu einer bestimmten regionalen Verbindung zur BlackBerry Infrastructure konfiguriert haben, gibt diese Einstellung die entsprechende Servergruppe an.

iOS: E-Mail-Profileinstellungen

Diese Einstellungen gelten auch für iPadOS-Geräte.

iOS: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Verschieben von Nachrichten zulassen	Diese Einstellung legt fest, ob Benutzer E-Mail-Nachrichten von diesem Konto auf ein anderes vorhandenes E-Mail-Konto auf einem Gerät verschieben können.
Zulassen, dass letzte Adressen synchronisiert werden	Diese Einstellung legt fest, ob ein Benutzer zuletzt verwendete Adressen mit anderen Geräten synchronisieren kann.
Nur in Mail verwenden	Diese Einstellung legt fest, ob andere Apps als die Mail-App dieses Konto zum Senden von E-Mail-Nachrichten verwenden können.
S/MIME aktivieren	Diese Einstellung legt fest, ob ein Benutzer S/MIME-geschützte E-Mail-Nachrichten senden kann.
Digital signierte S/MIME-Nachrichten aktivieren	Diese Einstellung legt fest, ob ein Gerät ausgehende Nachrichten mit digitaler Signatur sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Anmeldeinformationen signieren	Diese Einstellung legt fest, wie Geräte die Zertifikate auswählen, die zum Signieren von Nachrichten erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde. Nachdem Sie den gewünschten Profiltyp ausgewählt haben, geben Sie das Profil für ein freigegebenes Zertifikat, das SCEP-Profil oder das Profil für Benutzeranmeldeinformationen an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signieren eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signatur-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signieren von Benutzeranmeldeinformati	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
Benutzer kann Signieren mit S/MIME ein-/ausschalten	Diese Einstellung gibt an, ob ein Benutzer das Signieren mit S/MIME ein- oder ausschalten darf. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Benutzer kann Signatur-Anmeldeinformationen ändern	Diese Einstellung gibt an, ob ein Benutzer Signatur-Anmeldeinformationen überschreiben kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
S/MIME-Nachrichtenverschlüsselung aktivieren	Diese Einstellung legt fest, ob ein Gerät ausgehende E-Mail-Nachrichten mit S/MIME-Verschlüsselung verschlüsselt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselungs-Anmeldeinformationen	Diese Einstellung legt fest, wie Geräte die Zertifikate auswählen, die zum Verschlüsseln von Nachrichten erforderlich sind. Nachdem Sie den Profiltyp ausgewählt haben, wählen Sie das gewünschte Profil für ein freigegebenes Zertifikat, das SCEP-Profil oder das Profil für Benutzeranmeldeinformationen aus. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselung eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät zum Verschlüsseln von E-Mail-Nachrichten verwenden kann. Die Geräte wählen das geeignete Zertifikat für den Empfänger aus, um die Nachrichten mit S/MIME zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselungs-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselung von Benutzeranmeldeinformationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
Benutzer kann S/MIME-Verschlüsselung überschreiben	Diese Einstellung gibt an, ob ein Benutzer die Verschlüsselungseinstellung ein- oder ausschalten kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Benutzer kann S/MIME-Verschlüsselungs-Anmeldeinformationen überschreiben	Diese Einstellung gibt an, ob ein Benutzer S/MIME-Verschlüsselungs-Anmeldeinformationen überschreiben kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Nachrichten verschlüsseln	Diese Einstellung legt fest, ob alle E-Mail-Nachrichten zum Zeitpunkt des Sendens verschlüsselt sein müssen (Erforderlich) oder ob der Benutzer zum Zeitpunkt des Sendens entscheiden kann, welche Nachrichten er verschlüsselt (Erlaubt). Diese Einstellung tritt nur dann in Kraft, wenn die Einstellung „S/MIME aktivieren“ ausgewählt ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Gerät synchronisiert werden sollen. **Hinweis:** Diese Einstellung betrifft nur die Standard-Mail- und Standard-Terminplaner-App auf Geräten mit der Aktivierungsart „MDM-Steuerelemente“.
VPN pro Konto	Diese Einstellung gibt das VPN-Profil an, das für die Netzwerkkommunikation dieses Kontos verwendet wird. Diese Einstellung gilt nur für Geräte mit iOS 14 und höher oder für Geräte mit iPadOS 14 und höher.
Authentifizierung	
Enable BlackBerry Secure Gateway	Diese Einstellung legt fest, ob Geräte mit der Aktivierungsart MDM-Steuerelemente das BlackBerry Secure Gateway verwenden, um eine Verbindung zum Mailserver aufzubauen. Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens. Wenn Sie Servergruppen für die Weiterleitung von BlackBerry Secure Gateway-Datenverkehr an eine bestimmte regionale Verbindung zur BlackBerry Infrastructure konfiguriert haben, verknüpfen Sie das E-Mail-Profil mit der entsprechenden Servergruppe.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist.

iOS: E-Mail-Profileinstellung	Beschreibung
Profil für freigegebenes Zertifikat	Diese Einstellung legt für das Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt und die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ festgelegt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver anmeldet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist und die Einstellung „Authentifizierungstyp“ auf „SCEP“ festgelegt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, mit denen der Benutzer eines Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver registriert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist und die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ festgelegt ist.
Anmeldedaten und Zertifikat verwenden	Diese Einstellung legt fest, ob ein Gerät die mit dem verknüpften SCEP-Profil erhaltenen Benutzeranmeldeinformationen und ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist und die Einstellung „Authentifizierungstyp“ auf „SCEP“ festgelegt ist.
Zur Authentifizierung OAuth verwenden	Diese Einstellung gibt an, ob die Verbindung „OAuth“ für die Authentifizierung verwenden soll.
URL für OAuth-Anmeldung	Diese Einstellung gibt die URL an, die dieses Konto für die Anmeldung bei OAuth verwenden soll. Wenn Sie diese URL angeben, müssen Sie einen Host festlegen, da die automatische Ermittlung nicht verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist.
URL für OAuth-Tokenanforderung	Diese Einstellung gibt die URL an, die dieses Konto für Tokenanforderungen mit OAuth verwenden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.

iOS: E-Mail-Profileinstellung	Beschreibung
Alle SSL-Zertifikate annehmen	Diese Einstellung gibt an, ob alle SSL-Zertifikate akzeptiert werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SSL verwenden“ ausgewählt wurde.
Externe E-Mail-Domänen	
Liste der zulässigen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer einen Empfänger, der über eine E-Mail-Adresse in der zugelassenen Domäne verfügt, zu einer E-Mail-Nachricht oder einem Kalendereintrag hinzufügt, wird keine Warnmeldung angezeigt. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.
Liste der verbotenen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer keine E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer versucht, einen Empfänger, der über eine E-Mail-Adresse in der gesperrten Domäne verfügt, zu einer E-Mail-Nachricht oder einer Kalendereinladung hinzuzufügen, verhindert die Work Connect-App, dass der Benutzer die Aufgabe abschließen kann. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.
Aktivierte Services	
E-Mail	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre geschäftliche E-Mail zugreifen können.
Kontakte	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre Geschäftskontakte zugreifen können.
Kalender	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihren Geschäftskalender zugreifen können.
Erinnerungen	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre geschäftlichen Erinnerungen zugreifen können.
Notizen	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre Geschäftsnotizen zugreifen können.
Änderungen an Konten	
E-Mail	Diese Einstellung legt fest, ob Benutzer den Zugriff auf geschäftliche E-Mails auf dem Gerät aktivieren oder deaktivieren können.

iOS: E-Mail-Profileinstellung	Beschreibung
Kontakte	Diese Einstellung legt fest, ob Benutzer den Zugriff auf Geschäftskontakte auf dem Gerät aktivieren oder deaktivieren können.
Kalender	Diese Einstellung legt fest, ob Benutzer den Zugriff auf den Geschäftskalender auf dem Gerät aktivieren oder deaktivieren können.
Erinnerungen	Diese Einstellung legt fest, ob Benutzer den Zugriff auf geschäftliche Erinnerungen auf dem Gerät aktivieren oder deaktivieren können.
Notizen	Diese Einstellung legt fest, ob Benutzer den Zugriff auf Geschäftsnotizen auf dem Gerät aktivieren oder deaktivieren können.

macOS: E-Mail-Profileinstellungen

Bei macOS gelten Profile für Benutzerkonten oder Geräte. E-Mail-Profile gelten für Benutzerkonten.

macOS: E-Mail-Profileinstellung	Beschreibung
Pfad	Diese Einstellung legt den Netzwerkpfad des E-Mail-Servers fest.
Port	Diese Einstellung legt den Port fest, der für die Verbindung zum Mailserver verwendet wird.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Externer Hostname oder IP-Adresse	Diese Einstellung legt den externen Hostnamen oder die IP-Adresse des E-Mail-Servers fest.
Externes SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum externen E-Mail-Server aufzubauen.
Externer Pfad	Diese Einstellung legt den Netzwerkpfad des externen E-Mail-Servers fest.
Externer Serverport	Diese Einstellung legt den Port fest, der für die Verbindung zu dem externen E-Mail-Server verwendet wird.

Android: E-Mail-Profileinstellungen

Android: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll. Der Standardwert ist „Exchange ActiveSync“.

Android: E-Mail-Profileinstellung	Beschreibung
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Android-Gerät mit der Aktivierungsart „MDM-Steuerelemente“ synchronisiert werden sollen. Wenn Sie bei Android-Geräten, die Samsung Knox MDM verwenden, den Wert auf „Unbeschränkt“ setzen, wird nur ein Monat synchronisiert. **Hinweis:** Diese Einstellung betrifft nur die Standard-Mail- und Standard-Terminplaner-App auf Android-Geräten mit Aktivierungstyp „MDM-Steuerelemente“.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem ein Android-Gerät ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server abruft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Anmeldedaten und Zertifikat verwenden	Diese Einstellung legt fest, ob ein Gerät die mit dem verknüpften SCEP-Profil erhaltenen Benutzeranmeldeinformationen und ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Profil für freigegebenes Zertifikat	Diese Einstellung legt für das Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Android-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen für das Client-Zertifikat fest, mit dem ein Android-Gerät eine Verbindung zum Mailserver aufbaut. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Alle SSL-Zertifikate annehmen	Mit dieser Einstellung legen Sie fest, ob ein Gerät automatisch nicht vertrauenswürdige SSL-Zertifikate vom Mailserver akzeptieren soll. Wenn diese Einstellung nicht aktiviert ist, können Geräte nur eine Verbindung zu E-Mailservern herstellen, die ein vertrauenswürdiges SSL-Zertifikat verwenden.
Maximale Größe des E-Mail-Anhangs	Diese Einstellung legt die maximal zulässige Größe für E-Mail-Anhänge (in MB) fest. Diese Einstellung gilt nur für Android Enterprise-Geräte.

Android: E-Mail-Profileinstellung	Beschreibung
Standard-E-Mail-Signatur für neue Nachrichten	Diese Einstellung gibt an, dass neuen E-Mails automatisch eine E-Mail-Signatur angehängt wird. Diese Einstellung gilt nur für Android Enterprise-Geräte.
S/MIME aktivieren	Diese Einstellung legt fest, ob Geräte S/MIME-geschützte E-Mail-Nachrichten senden können. Für Geräte, die die BlackBerry Productivity Suite verwenden, müssen Sie stattdessen einen Wert für die Einstellung „S/MIME-Unterstützung“ festlegen.
Nachrichten signieren	Diese Einstellung legt fest, ob Geräte alle ausgehenden E-Mail-Nachrichten mit digitaler Signatur senden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde. Bei Android Enterprise-Geräten gilt diese Einstellung nur für Geräte, die Divide Productivity verwenden. Für Geräte, die die BlackBerry Productivity Suite verwenden, müssen Sie stattdessen einen Wert für die Einstellung „Digital signierte S/MIME-Nachrichten“ festlegen.
Anmeldeinformationen signieren	Diese Einstellung legt die Anmeldeinformationen fest, die ein Gerät zum Signieren von E-Mail-Nachrichten verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Nachrichten signieren“ ausgewählt wurde.
Signieren eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Signatur-SCEP	Diese Einstellung legt für ein Client-Zertifikat das SCEP-Profil fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „SCEP“ gesetzt ist.
Signieren von Benutzeranmeldeinformati	Diese Einstellung legt für ein Client-Zertifikat das Profil für die Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „Benutzeranmeldeinformationen“ gesetzt ist.

Android: E-Mail-Profileinstellung	Beschreibung
Nachrichten verschlüsseln	Diese Einstellung legt fest, ob Geräte ausgehende E-Mail-Nachrichten mit S/MIME-Verschlüsselung verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde. Bei Android Enterprise-Geräten gilt diese Einstellung nur für Geräte, die Divide Productivity verwenden. Für Geräte, die die BlackBerry Productivity Suite verwenden, müssen Sie stattdessen einen Wert für die Einstellung „Digital signierte S/MIME-Nachrichten“ festlegen.
Verschlüsselungs-Anmeldeinformationen	Diese Einstellung legt die Anmeldeinformationen fest, die ein Gerät zur Verschlüsselung von E-Mail-Nachrichten verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Nachrichten verschlüsseln“ ausgewählt wurde.
Verschlüsselung eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verschlüsselungs-Anmeldeinformationen“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verschlüsselungs-SCEP	Diese Einstellung legt für ein Client-Zertifikat das SCEP-Profil fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „SCEP“ gesetzt ist.
Verschlüsselung von Benutzeranmeldeinformationen	Diese Einstellung legt für ein Client-Zertifikat das Profil für die Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Smartcard-Authentifizierung für E-Mail erforderlich	Diese Einstellung legt fest, ob für Samsung Knox-Geräte zur Authentifizierung beim E-Mail-Server eine Smartcard erforderlich ist.
Bearbeiten von Einstellungen durch Benutzer zulassen	Geben Sie an, ob ein Benutzer Übermittlungseinstellungen ändern kann. Diese Einstellung gilt nur für Samsung Knox-Geräte.
Externe E-Mail-Domänen	

Android: E-Mail-Profileinstellung	Beschreibung
Liste der zulässigen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer einen Empfänger, der über eine E-Mail-Adresse in der zugelassenen Domäne verfügt, zu einer E-Mail-Nachricht oder einem Kalendereintrag hinzufügt, wird keine Warnmeldung angezeigt. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.
Liste der verbotenen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer keine E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer versucht, einen Empfänger, der über eine E-Mail-Adresse in der gesperrten Domäne verfügt, zu einer E-Mail-Nachricht oder einer Kalendereinladung hinzuzufügen, verhindert die E-Mail- oder Kalender-App, dass der Benutzer die Aufgabe abschließen kann. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.

Windows: E-Mail-Profileinstellungen

Windows: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll.
Kontoname	Diese Einstellung legt den Namen des geschäftlichen E-Mail-Kontos fest, der auf dem Windows-Gerät angezeigt wird. Sie können eine Variable wie etwa „%UserEmailAddress%“ verwenden.
Synchronisierungsintervall	Diese Einstellung legt fest, wie häufig ein Windows-Gerät neue E-Mail-Nachrichten vom Mailserver herunterlädt.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Windows-Gerät synchronisiert werden sollen.
SSL verwenden	Diese Einstellung legt fest, ob ein Windows-Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Zu synchronisierender Inhalt	
E-Mail	Diese Einstellung legt fest, ob ein Windows-Gerät E-Mail-Nachrichten mit dem Mailserver synchronisiert.

Windows: E-Mail-Profileinstellung	Beschreibung
Kontakte	Diese Einstellung legt fest, ob ein Windows-Gerät Kontakte mit dem Mailserver synchronisiert.
Kalender	Diese Einstellung legt fest, ob ein Windows-Gerät Kalendereinträge mit dem Mailserver synchronisiert.
Aufgabe	Diese Einstellung legt fest, ob ein Windows-Gerät Aufgabendaten mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.

Schützen von an iOS-Geräte gesendete E-Mail-Daten mithilfe des BlackBerry Secure Gateway

Sie können den BlackBerry Secure Gateway verwenden, um E-Mail-Daten zu schützen und iOS- und iPadOS-Geräten das Senden und Empfangen von geschäftlichen E-Mails zu erlauben. Das Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum Mailserver Ihres Unternehmens, ohne dass Sie Ihren Mailserver außerhalb der Firewall zugänglich machen oder Ihren Mailserver in einer DMZ suchen müssen.

Die Geräte müssen mit der Aktivierungsart MDM-Steuerelemente aktiviert werden.

Schritt	Aktion
1	Wählen Sie im E-Mail-Profil die Einstellung „BlackBerry Secure Gateway aktivieren“ aus.
2	Wenn Ihre Umgebung iOS- oder iPadOS 13.0-Geräte oder höher einschließt und der Mailserver Ihres Unternehmens für die Verwendung der modernen Authentifizierung (OAuth) konfiguriert ist: • Wählen Sie im E-Mail-Profil die Einstellung „Zur Authentifizierung OAuth verwenden“ aus. • Konfigurieren von BlackBerry UEM zum Erkennen des Exchange ActiveSync-Servers oder Zertifikats des Identitätsanbieters als vertrauenswürdig • Konfigurieren von BlackBerry Secure Gateway zur Verwendung von OAuth mit dem Mailserver.
3	Wenn Sie Servergruppen so konfiguriert haben, dass sie regionale Verbindungen zum BlackBerry Infrastructure und direkten BlackBerry Secure Gateway-Datenverkehr unterstützen, wählen Sie die entsprechende Servergruppe für die Einstellung „Servergruppe für BlackBerry Secure Gateway Service“ im E-Mail-Profil aus.

Konfigurieren von BlackBerry UEM zum Erkennen des Exchange ActiveSync-Servers oder Zertifikats des Identitätsanbieters als vertrauenswürdig

Wenn Ihre Umgebung Geräte mit iOS und iPadOS Version 13.0 oder höher enthält und Sie die moderne Authentifizierung (OAuth) für die Verbindung mit Microsoft Exchange Online verwenden, müssen Sie das Zertifikat (oder das Stammzertifikat) des Identitätsanbieters zu BlackBerry UEM hinzufügen. Der BlackBerry Secure Gateway verlangt das Zertifikat, damit der Identitätsanbieter als vertrauenswürdig erkannt wird, wenn die Verbindung eingerichtet wird.

Wenn Ihr Exchange ActiveSync-Server so konfiguriert ist, dass eine TLS-Verbindung erforderlich ist, müssen Sie auch das Zertifikat des Exchange ActiveSync-Servers (oder das Stammzertifikat) zu BlackBerry UEM hinzufügen. Der BlackBerry Secure Gateway verlangt das Zertifikat, damit der Server als vertrauenswürdig erkannt wird, wenn die TLS/SSL-Verbindung eingerichtet wird.

Bevor Sie beginnen: Exportieren Sie die Zertifikate im X.509-Format (*.cer, *.der) von den folgenden Servern, und speichern Sie sie in einem Netzwerkpfad, auf den Sie über die Verwaltungskonsole zugreifen können:

- Active Directory-Identitätsprovider, wenn Ihre Umgebung moderne Authentifizierung unterstützt

- Exchange ActiveSync-Server, wenn Ihr Exchange ActiveSync so konfiguriert ist, dass eine TLS-Verbindung erforderlich ist

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Vertrauenswürdige Zertifikate**.
2. Klicken Sie neben **Exchange ActiveSync-Server-Vertrauenseinstellungen** auf +.
3. Klicken Sie auf **Durchsuchen**.
4. Wählen Sie das zu verwendende E-Mail-Profil aus.
5. Klicken Sie auf **Öffnen**.
6. Geben Sie eine Beschreibung für das Zertifikat ein.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Konfigurieren von BlackBerry Secure Gateway zur Verwendung von OAuth mit unterstützten TLS-Versionen und Ciphern.

Konfigurieren von BlackBerry Secure Gateway zur Verwendung von OAuth mit unterstützten TLS-Versionen und Ciphern

Sie können die Verwendung von OAuth für die moderne Authentifizierung für BlackBerry Secure Gateway konfigurieren. Um OAuth zu verwenden, müssen Sie die URL des Mailservers aus dem E-Mail-Profil und die URL zum Abrufen des Erkennungsdokuments des Identitätsanbieters angeben. Weitere Informationen zum Erkennungsdokument finden Sie in der Microsoft-Dokumentation.

Sie können auch die TLS-Version und die Microsoft Exchange SSL-Verschlüsselungen angeben, die BlackBerry Secure Gateway für Verbindungen zu Exchange ActiveSync verwendet. Möglicherweise müssen Sie diese Liste je nach den Sicherheitsanforderungen Ihres Exchange ActiveSync-Servers aktualisieren.

Bevor Sie beginnen: Konfigurieren von BlackBerry UEM zum Erkennen des Exchange ActiveSync-Servers oder Zertifikats des Identitätsanbieters als vertrauenswürdig

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Secure Gateway**.
2. Um eine TLS-Version oder SSL-Verschlüsselung hinzuzufügen oder zu entfernen, klicken Sie in der entsprechenden Tabelle auf +.
3. Klicken Sie auf die TLS-Version oder den Chiffrierschlüssel, den bzw. die Sie in der Liste **Ausgewählt** hinzufügen oder aus der Liste entfernen möchten.
4. Klicken Sie auf den Pfeil, um das Element in die gewünschte Liste zu verschieben.
5. Klicken Sie auf **Zuweisen**.
6. Um die moderne Authentifizierung zu verwenden, wählen Sie **OAuth für E-Mail-Server-Authentifizierung aktivieren**.
7. Geben Sie im Feld **Erkennungsendpunkt** die URL ein, die BlackBerry Secure Gateway zum Abrufen und Zwischenspeichern des Erkennungsdokuments des Identitätsanbieters verwendet.
   - Format:`https://<identity provider>/.well-known/openid-configuration`
   - Beispiel: `https://login.microsoftonline.com/common/.well-known/openid-configuration`
   - Beispiel: `https://login.windows.net/common/.well-known/openid-configuration`

   BlackBerry Secure Gateway ruft sowohl das Erkennungsdokument ohne Versionsangabe als auch das Erkennungsdokument v2.0 ab und aktualisiert die zwischengespeicherten Dokumente in regelmäßigen Abständen.

8. Geben Sie im Feld **E-Mail-Server-Ressource** die URL für den im E-Mail-Profil angegebenen Mailserver ein, beginnend mit „https://“ (z. B. `https://outlook.office365.com`).
9. Klicken Sie auf **Speichern**.

Aktivieren der BlackBerry Hub-App für Android Enterprise-Geräte

BlackBerry Hub ist eine Android-App, mit der Benutzer an einem zentralen Ort Nachrichten, Benachrichtigungen und Ereignisse anzeigen können.

Damit Benutzer mit Android Enterprise-Geräten sowohl geschäftliche als auch persönliche Nachrichten in BlackBerry Hub anzeigen können, müssen Sie einige Einstellungen in BlackBerry UEM überprüfen.

1. Überprüfen Sie für die Benutzern zugewiesene IT-Richtlinie im Abschnitt BlackBerry Productivity Suite, ob die IT-Richtlinienregel **Einheitliche Kontoanzeige in BlackBerry Hub zulassen** aktiviert ist.
2. Überprüfen Sie in der App-Konfiguration für BlackBerry Hub, ob die folgenden Elemente ausgewählt sind:
   - **IPC für alle Profile**
   - **Zugriff auf geschäftliche Inhalte**

Wenn Sie fertig sind: Informationen zur Verwendung des BlackBerry Hub auf Geräten, z. B. zum Hinzufügen eines E-Mail-Kontos oder Anpassen der BlackBerry Hub-Einstellungen, finden Sie in der Dokumentation zum BlackBerry Hub.

Informationen zur Fehlerbehebung finden Sie in KB 37721.

Erweitern der E-Mail-Sicherheit mithilfe von S/MIME

Im E-Mail-Profil können Sie S/MIME aktivieren, sodass Benutzer von iOS- und Android-Geräten die E-Mail-Sicherheit erhöhen können. Mit S/MIME steht ein Standardverfahren zur Verschlüsselung und zum Signieren von E-Mail-Nachrichten zur Verfügung. Bei Verwendung eines geschäftlichen E-Mail-Kontos, das S/MIME-geschützte Nachrichten unterstützt, können Benutzer angeben, ob S/MIME zum Verschlüsseln, Signieren oder Verschlüsseln und Signieren von geschäftlichen E-Mail-Nachrichten verwendet werden soll. S/MIME kann für persönliche E-Mail-Konten nicht aktiviert werden.

Die S/MIME-Einstellungen haben Vorrang vor den PGP-Einstellungen. Wenn die S/MIME-Unterstützung auf „Erforderlich“ gesetzt wird, werden die PGP-Einstellungen ignoriert.

Abrufen von S/MIME-Zertifikaten

Sie können Zertifikatsabrufprofile verwenden, um es Android- und iOS-Geräten zu ermöglichen, nach S/MIME-Zertifikaten von jedem der angegebenen LDAP-Server zu suchen und diese abzurufen. Wenn sich ein erforderliches S/MIME-Zertifikat nicht bereits im Zertifikatspeicher des Geräts befindet, wird es von dem Gerät automatisch vom Server abgerufen und importiert. Wenn mehr als ein S/MIME-Zertifikat vorliegt und ein Gerät nicht ermitteln kann, welches zu bevorzugen ist, zeigt das Gerät alle S/MIME-Zertifikate an, sodass der Benutzer auswählen kann, welches davon verwendet werden soll.

Sie können festlegen, dass die Geräte entweder die einfache Authentifizierung oder die Kerberos-Authentifizierung verwenden, um sich bei LDAP-Zertifikatservern zu authentifizieren. Sie können die erforderlichen Authentifizierungs-Anmeldeinformationen in die Zertifikatsabrufprofile einbinden, sodass sich die Geräte automatisch bei den LDAP-Zertifikatservern authentifizieren können. Wenn Sie die erforderlichen Anmeldeinformationen nicht angeben, fordert das Gerät bei der ersten Authentifizierung bei einem LDAP-Zertifikatserver den Benutzer zur Eingabe der Anmeldeinformationen für die Authentifizierung auf.

Wenn Sie kein Zertifikatsabrufprofil erstellen und es den Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen, müssen die Benutzer die S/MIME-Zertifikate aus dem Anhang einer geschäftlichen E-Mail oder von einem Computer manuell importieren.

Erstellen eines Zertifikatsabrufprofils

Bevor Sie beginnen:

- Damit die Geräte den LDAP-Zertifikatservern vertrauen können, wenn sie sichere Verbindungen herstellen, müssen Sie die Zertifizierungsstellenzertifikate ggf. an die Geräte versenden. Falls erforderlich, erstellen Sie Profile für Zertifizierungsstellenzertifikate, und weisen sie den Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Weitere Informationen zu Zertifizierungsstellenzertifikaten finden Sie unter Senden von Zertifizierungsstellenzertifikaten an Geräte und Apps.
- Wenn Sie die Kerberos-Authentifizierung über S/MIME-Zertifikatabruf implementieren, müssen Sie den entsprechenden Benutzern oder Benutzergruppen ein Profil für die einmalige Anmeldung (Single Sign-On) zuweisen. Weitere Informationen zu Single Sign-On-Profilen finden Sie unter Aktivieren der automatischen Authentifizierung für iOS-Geräte.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Zertifikatsabruf**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil des Zertifizierungsstellenzertifikats ein.
5. Klicken Sie in der Tabelle auf +.

6. Geben Sie im Feld **Dienst-URL** den FQDN eines LDAP-Zertifikatservers in folgendem Format ein: ldap://<*fqdn*>:<*port*>. (Beispiel: ldap://server01.beispiel.com:389).
7. Geben Sie im Feld **Basissuche** die Basis-DN ein, die bei der Suche der LDAP-Zertifikatserver der Ausgangspunkt ist.
8. Führen Sie in der Dropdown-Liste **Suchbereich** eine der folgenden Aktionen aus:
   - Um nur das Basisobjekt (Basis-DN) zu suchen, klicken Sie auf **Basis**. Diese Option ist der Standardwert.
   - Um nicht das Basisobjekt, sondern eine Ebene unter dem Basisobjekt zu suchen, klicken Sie auf **Eine Ebene**.
   - Um das Basisobjekt und alle Ebenen darunter zu suchen, klicken Sie auf **Unterstruktur**.
   - Um alle Ebenen unter dem Basisobjekt zu suchen, aber nicht das Basisobjekt selbst, klicken Sie auf **Untergeordnet**.
9. Wenn eine Authentifizierung erforderlich ist, führen Sie die folgenden Aktionen aus:
   a) Klicken Sie in der Dropdown-Liste **Authentifizierungstyp** auf **Einfach** oder **Kerberos**.
   b) Geben Sie im Feld **LDAP-Benutzer-ID** die DN eines Kontos ein, das Suchberechtigungen auf dem LDAP-Zertifikatserver hat (zum Beispiel cn=admin, dc=beispiel, dc=com).
   c) Geben Sie im Feld **LDAP-Kennwort** das Kennwort für das Konto ein, das Suchberechtigungen auf dem LDAP-Zertifikatserver hat.
10. Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**.
11. Geben Sie im Feld **Verbindungs-Timeout** die Zeit in Sekunden ein, die das Gerät auf eine Antwort des LDAP-Zertifikatservers wartet.
12. Klicken Sie auf **Hinzufügen**.
13. Wiederholen Sie die Schritte 5 bis 12 für jeden LDAP-Zertifikatserver.
14. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

Ermitteln des Status von S/MIME-Zertifikaten auf Geräten

Sie können OCSP- und CRL-Profile verwenden, um es iOS- und Android-Geräten zu erlauben, den Status der S/MIME-Zertifikate zu überprüfen, um herauszufinden, ob es sich um ein gültiges Zertifikat handelt. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein OCSP-Profil und ein CRL-Profil zuweisen.

Sie können das OSCP-Profil verwenden, um die OSCP-Responder anzugeben, von denen die Geräte den Status von S/MIME-Zertifikaten abrufen sollen.

Sie können CRL-Profile verwenden, damit Geräte die im S/MIME-Zertifikat festgelegten Responder überprüfen können. Sie können es auch so konfigurieren, dass BlackBerry UEM den Status von S/MIME-Zertifikaten über HTTP, HTTPS oder LDAP anfordert. Wenn Sie Exchange ActiveSync für den Zertifikatabruf verwenden, verwenden Geräte Exchange ActiveSync, um den Status von S/MIME-Zertifikaten zu prüfen. Wenn Sie LDAP zum Abrufen von Zertifikaten verwenden, verwenden Geräte das OCSP (Online Certificate Status Protocol), um den Status von Zertifikaten zu prüfen.

Die Zertifikatsstatusanzeigen können sich von Gerät zu Gerät unterscheiden. Weitere Informationen finden Sie im Benutzerhandbuch des Geräts im Abschnitt zu den Symbolen für sichere E-Mail.

Erstellen eines OCSP-Profils

OCSP-Profile werden für iOS- und Android-Geräte unterstützt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > OCSP**.

3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das OCSP-Profil ein.
5. Führen Sie folgende Aktionen aus:
   a) Klicken Sie in der Tabelle auf +.
   b) Geben Sie im Feld **Dienst-URL** die Webadresse eines OCSP-Responders ein.
   c) Geben Sie im Feld **Verbindungs-Timeout** die Zeit in Sekunden ein, die das Gerät auf eine OCSP-Antwort wartet.
   d) Klicken Sie auf **Hinzufügen**.
6. Wiederholen Sie Schritte 3 bis 5 für jeden OCSP-Responder.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

Erstellen eines CRL-Profils

CRL-Profile werden für iOS- und Android-Geräte unterstützt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > CRL**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das CRL-Profil ein.
5. Damit die Geräte die Responder-URLs verwenden können, die im Zertifikat definiert sind, aktivieren Sie das Kontrollkästchen **Zertifikaterweiterungen des Responders verwenden**.
6. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Verwenden von HTTP oder HTTPS für CRL	**a.** Klicken Sie im Abschnitt **HTTP für CRL** auf +. **b.** Geben Sie einen Namen und eine Beschreibung für die HTTP CRL-Konfiguration ein. **c.** Geben Sie im Feld **Dienst-URL** die Webadresse eines HTTP- oder HTTPS-Servers ein. **d.** Klicken Sie auf **Hinzufügen**. **e.** Wiederholen Sie diese Schritte für jeden HTTP- oder HTTPS-Server.

Aufgabe	Schritte
Verwenden von LDAP für CRL	**a.** Klicken Sie im Abschnitt **LDAP für CRL** auf +. **b.** Geben Sie einen Namen und eine Beschreibung für die LDAP CRL-Konfiguration ein. **c.** Geben Sie im Feld **Dienst-URL** den FQDN eines LDAP-Servers gemäß dem folgenden Format ein: ldap://<*fqdn*>:<*port*> (zum Beispiel ldap://server01.example.com:389). Verwenden Sie für sichere Verbindungen das Format ldaps://<*fqdn*>:<*port*>. **d.** Geben Sie im Feld **Basissuche** die Basis-DN ein, die bei der Suche der LDAP-Server der Ausgangspunkt ist. **e.** Wählen Sie in der Dropdown-Liste **Suchbereich** den entsprechenden Suchbereich für LDAP-Serversuchen aus. **f.** Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**. **g.** Geben Sie im Feld **LDAP-Benutzer-ID** die DN eines Kontos ein, der Suchberechtigungen auf dem LDAP-Server hat (zum Beispiel cn=admin,dc=example,dc=com). **h.** Geben Sie im Feld **LDAP-Kennwort** das Kennwort für das Konto ein, das Suchberechtigungen auf dem LDAP-Server besitzt. **i.** Klicken Sie auf **Hinzufügen**. **j.** Wiederholen Sie diese Schritte für jeden LDAP-Server.

7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

Erweitern der E-Mail-Sicherheit mit PGP

Sie können die E-Mail-Sicherheit für die Benutzer von iOS- und Android-Geräten durch Aktivierung von PGP erhöhen. PGP schützt E-Mail-Nachrichten auf Geräten mit dem OpenPGP-Format. Benutzer können E-Mail-Nachrichten mit dem PGP-Schutz signieren, verschlüsseln oder signieren und verschlüsseln, sofern sie eine geschäftliche E-Mail-Adresse verwenden. PGP kann nicht für persönliche E-Mail-Adressen verwendet werden.

Sie können PGP für Benutzer in einem E-Mail-Profil aktivieren. Sie können die Verwendung von PGP auf iOS- und Android-Geräten erzwingen, die Nutzung von PGP untersagen oder die Nutzung freistellen. Wenn die Nutzung von PGP optional ist (Standardeinstellung), kann ein Benutzer PGP auf dem Gerät aktivieren und angeben, ob E-Mail-Nachrichten verschlüsselt, signiert oder verschlüsselt und signiert werden sollen.

Um E-Mail-Nachrichten zu signieren und zu verschlüsseln, müssen Benutzer PGP-Schlüssel für jeden Empfänger auf ihren Geräten speichern. Benutzer können PGP-Schlüssel speichern, indem sie die Dateien aus einer geschäftlichen E-Mail-Nachricht importieren.

Sie können PGP mit den entsprechenden E-Mail-Profileinstellungen konfigurieren.

Erzwingen von sicherer E-Mail mithilfe der Nachrichtenklassifizierung

Die Nachrichtenklassifizierung ermöglicht es Ihrem Unternehmen, auf iOS- und Android-Geräten sichere E-Mail-Richtlinien festzulegen und durchzusetzen sowie visuelle Markierungen zu E-Mail-Nachrichten hinzuzufügen. Sie können BlackBerry UEM verwenden, um Benutzern von iOS- und Android-Geräten die gleichen Optionen zur Nachrichtenklassifizierung zu bieten, die ihnen auch bei den E-Mail-Anwendungen auf ihrem Computer zur

Verfügung stehen. Sie können die folgenden Regeln für ausgehende Nachrichten definieren, basierend auf den Nachrichtenklassifizierungen:

- Ein Etikett hinzufügen, um die Nachrichtenklassifizierung zu markieren (z. B. vertraulich)
- Eine optische Markierung am Ende der Betreffzeile hinzufügen (z. B. [C])
- Text am Anfang oder am Ende des E-Mail-Textkörpers hinzufügen (z. B. "Diese Nachricht wurde als vertraulich eingestuft")
- S/MIME oder PGP-Optionen einstellen (z. B. signieren und verschlüsseln)
- Eine Standardklassifizierung einstellen

Für iOS- und Android-Geräte können Sie mithilfe der Nachrichtenklassifizierung festlegen, dass Benutzer E-Mail-Nachrichten signieren oder verschlüsseln oder signieren und verschlüsseln müssen oder visuelle Markierungen zu E-Mail-Nachrichten, die sie von ihren Geräten senden, hinzufügen müssen. Mithilfe von E-Mail-Profilen können Sie Konfigurationsdateien zur Nachrichtenklassifizierung (mit der Dateierweiterung .json) angeben, die an die Geräte der Benutzer gesendet werden. Wenn Benutzer E-Mail-Nachrichten beantworten, für die eine Nachrichtenklassifizierung festgelegt wurde, oder sichere E-Mail-Nachrichten erstellen, bestimmt die Konfiguration der Nachrichtenklassifizierung, welche Klassifizierungsregeln von den Geräten bei ausgehenden Nachrichten erzwungen werden müssen.

Die Nachrichtenschutzoptionen auf einem Gerät sind auf die Arten der Verschlüsselung und digitalen Signatur beschränkt, die auf dem Gerät zugelassen sind. Wenn ein Benutzer eine Nachrichtenklassifizierung für eine E-Mail-Nachricht auf einem Gerät anwendet, muss der Benutzer eine Nachrichtenschutzart auswählen, die die betreffende Nachrichtenklassifizierung zulässt, oder den Standardschutz akzeptieren. Wenn ein Benutzer eine Nachrichtenklassifizierung auswählt, die eine Signatur und/oder Verschlüsselung der E-Mail-Nachricht erfordert, und auf dem Gerät S/MIME oder PGP nicht konfiguriert ist, kann der Benutzer die E-Mail-Nachricht nicht senden.

Die S/MIME- und PGP-Einstellungen haben Vorrang vor der Nachrichtenklassifizierung. Benutzer können die Stufe der Nachrichtenklassifizierung auf ihren Geräten anheben, aber nicht absenken. Die Stufen der Nachrichtenklassifizierung werden von Regeln für sichere E-Mails in jeder Klassifizierung festgelegt.

Wenn die Nachrichtenklassifizierung aktiviert ist, können Benutzer keine E-Mail-Nachrichten mithilfe von BlackBerry Assistant von ihren Geräten senden.

Sie können die Nachrichtenklassifizierung mit den entsprechenden E-Mail-Profileinstellungen konfigurieren.

Weitere Informationen über das Erstellen von Konfigurationsdateien zur Nachrichtenklassifizierung finden Sie unter KB 36736 im Artikel 36736.

Erstellen eines IMAP/POP3-E-Mail-Profils

IMAP/POP3-E-Mail-Profile legen fest, wie iOS-, iPadOS-, macOS-, Android- und Windows-Geräte eine Verbindung zu einem IMAP- bzw. POP3-Mailserver aufbauen und E-Mail-Nachrichten synchronisieren.

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen von den Einstellungen ab, die Sie ausgewählt haben.

Hinweis: BlackBerry UEM sendet das E-Mail-Profil an Android-Geräte, aber der Benutzer muss die Verbindung zum Mailserver manuell konfigurieren.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **E-Mail, Kalender und Kontakte > IMAP/POP3-E-Mail**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie im Feld **E-Mail-Typ** den Typ des E-Mail-Protokolls ein.
6. Führen Sie im Feld **E-Mail-Adresse** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie die E-Mail-Adresse des Benutzers ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserEmailAddress%` ein.
7. Geben Sie im Abschnitt **Einstellungen für eingehende E-Mail-Nachrichten** den Hostnamen oder die IP-Adresse des Mailservers ein, um E-Mail-Nachrichten zu empfangen.
8. Geben Sie ggf. den Port für den Empfang von E-Mail-Nachrichten ein.
9. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserName%` ein.
10. Geben Sie im Abschnitt **Einstellungen für ausgehende E-Mail-Nachrichten** den Hostnamen oder die IP-Adresse des Mailservers ein, um E-Mail-Nachrichten zu senden.
11. Geben Sie ggf. den Port zum Senden von E-Mail-Nachrichten ein.
12. Wählen Sie ggf. die Option **Authentifizierung für ausgehende E-Mail-Nachrichten erforderlich** aus, und geben Sie die Anmeldeinformationen zum Senden von E-Mail-Nachrichten ein.
13. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für jede Profileinstellung. Siehe:
    - iOS und macOS: IMAP/POP3-E-Mail-Profileinstellungen
    - Android: IMAP/POP3-E-Mail-Profileinstellungen
    - Windows: IMAP/POP3-E-Mail-Profileinstellungen
14. Klicken Sie auf **Hinzufügen**.

iOS und macOS: IMAP/POP3-E-Mail-Profileinstellungen

Diese Einstellungen gelten auch für iPadOS-Geräte.

Bei macOS gelten Profile für Benutzerkonten oder Geräte. IMAP/POP3-Profile gelten für Benutzerkonten.

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
Präfix für IMAP-Pfad	Diese Einstellung legt das Präfix zum IMAP-Pfad fest (falls erforderlich). Kontaktieren Sie ggf. Ihren Internetdienstanbieter, um weitere Informationen zu erhalten. Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „IMAP“ gesetzt ist.
Verschieben von Nachrichten zulassen	Diese Einstellung legt fest, ob Benutzer E-Mail-Nachrichten von diesem Konto auf ein anderes E-Mail-Konto auf einem iOS-Gerät verschieben können.
Zulassen, dass letzte Adressen synchronisiert werden	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes zuletzt verwendete E-Mail-Adressen mit anderen Geräten synchronisieren kann.
Nur in Mail verwenden	Diese Einstellung legt fest, ob andere Apps als die Mail-App auf einem iOS-Gerät dieses Konto zum Senden von E-Mail-Nachrichten verwenden können.
S/MIME aktivieren	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes S/MIME-geschützte E-Mail-Nachrichten senden kann. S/MIME wird nur auf Geräten unterstützt, die mit MDM-Steuerungen aktiviert werden.
Anmeldeinformationen signieren	Diese Einstellung legt die Anmeldeinformationen fest, die ein Gerät zum Signieren von E-Mail-Nachrichten verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signieren eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Signatur-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „SCEP“ gesetzt ist.
Signieren von Benutzeranmeldeinformationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Anmeldeinformationen signieren“ auf „Benutzeranmeldeinformationen“ gesetzt ist.

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
Verschlüsselungs-Anmeldeinformationen	Diese Einstellung legt fest, wie Geräte die Zertifikate auswählen, die zum Verschlüsseln von Nachrichten erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde. Nachdem Sie den Profiltyp ausgewählt haben, wählen Sie das gewünschte Profil für ein freigegebenes Zertifikat, das SCEP-Profil oder das Profil für Benutzeranmeldeinformationen aus.
Verschlüsselung eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Gerät verwendet, um E-Mail-Nachrichten zu verschlüsseln. Die Geräte wählen das geeignete Zertifikat für den Empfänger aus, um die Nachrichten mit S/MIME zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verschlüsselungs-Anmeldeinformationen“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verschlüsselungs-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verschlüsselungsanmeldedaten“ auf „SCEP“ gesetzt ist.
Verschlüsselung von Benutzeranmeldeinformationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verschlüsselungsanmeldedaten“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Nachrichten verschlüsseln	Diese Einstellung legt fest, ob alle E-Mail-Nachrichten zum Zeitpunkt des Sendens verschlüsselt sein müssen (Erforderlich) oder ob der Benutzer zum Zeitpunkt des Sendens entscheiden kann, welche Nachrichten er verschlüsselt (Erlaubt). Diese Einstellung tritt nur dann in Kraft, wenn die Einstellung „S/MIME aktivieren“ ausgewählt ist.
Mail Drop zulassen	Diese Einstellung legt fest, ob Benutzer Dateien von diesem Konto mithilfe von Mail Drop senden können.
VPN pro Konto	Diese Einstellung gibt das VPN-Profil an, das für die Netzwerkkommunikation dieses Kontos verwendet wird.

Android: IMAP/POP3-E-Mail-Profileinstellungen

Android: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
Präfix für IMAP-Pfad	Diese Einstellung legt das Präfix zum IMAP-Pfad fest (falls erforderlich). Kontaktieren Sie ggf. Ihren Internetdienstanbieter, um weitere Informationen zu erhalten. Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „IMAP“ gesetzt ist.
Löschen von E-Mail-Nachrichten vom Server	Diese Einstellung legt fest, wann eine E-Mail vom Mailserver gelöscht wird. Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „POP3“ gesetzt ist.

Windows: IMAP/POP3-E-Mail-Profileinstellungen

Windows: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
Löschen von E-Mail-Nachrichten vom Server	Diese Einstellung legt fest, wie E-Mail-Nachrichten behandelt werden, wenn ein Benutzer sie löscht. E-Mail-Nachrichten können vom Server gelöscht (unwiederbringlich löschen) oder aus dem Posteingang entfernt, aber im Ordner „Papierkorb“ beibehalten werden (temporär löschen). Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „IMAP“ gesetzt ist.
Domäne	Diese Einstellung legt die Domäne des E-Mail-Servers fest.
Synchronisierungsintervall	Diese Einstellung legt fest, wie häufig ein Windows-Gerät neue Inhalte vom Mailserver herunterlädt.
Ursprüngliche Abrufmenge	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Windows-Gerät synchronisiert werden sollen.
Ausschließlich Mobilfunknetz verwenden, kein Wi-Fi	Diese Einstellung gibt an, ob E-Mail-Nachrichten nur über das drahtlose Netzwerk gesendet und empfangen werden.

Einrichten von CardDAV- und CalDAV-Profilen für iOS - und macOS-Geräte

Sie können CardDAV- und CalDAV-Profile verwenden, um iOS-, iPadOS- und macOS-Geräten den Zugriff auf Kontakte und Kalender auf einem Remote-Server zu erlauben. Sie können Benutzerkonten, Benutzergruppen oder Gerätegruppen CardDAV- und CalDAV-Profile zuweisen. Mehrere Geräte können auf dieselben Informationen zugreifen.

CardDAV- und CalDAV-Profile gelten für Benutzerkonten.

Erstellen eines CardDAV-Profils

Bevor Sie beginnen: Stellen Sie sicher, dass das Gerät auf einen aktiven CardDAV-Server zugreifen kann.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **E-Mail, Kalender und Kontakte > CardDAV**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie die Serveradresse für das Profil ein. Hierbei handelt es sich um den FQDN des Computers, der die Kalenderanwendung hostet.
6. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserName%` ein.
7. Falls erforderlich, geben Sie den Port für den CardDAV-Server an.
8. Falls erforderlich, wählen Sie das Kontrollkästchen **SSL verwenden** aus und geben die URL für den SSL-Server ein.
9. Wählen Sie bei Bedarf im Feld **VPN pro Konto** das VPN-Profil aus, das Sie für die Netzwerkkommunikation dieses Kontos verwenden möchten.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Profil Benutzern, Benutzergruppen oder Gerätegruppen zu.

Erstellen eines CalDAV-Profils

Bevor Sie beginnen: Stellen Sie sicher, dass das Gerät auf einen aktiven CalDAV-Server zugreifen kann.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **E-Mail, Kalender und Kontakte > CalDAV**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie die Serveradresse für das Profil ein. Hierbei handelt es sich um den FQDN des Computers, der die Kalenderanwendung hostet.
6. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie `%UserName%` ein.

7. Falls erforderlich, geben Sie den Port für den CalDAV-Server an.
8. Falls erforderlich, wählen Sie das Kontrollkästchen **SSL verwenden** aus und geben die URL für den SSL-Server ein.
9. Wählen Sie bei Bedarf im Feld **VPN pro Konto** das VPN-Profil aus, das Sie für die Netzwerkkommunikation dieses Kontos verwenden möchten.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Profil Benutzern, Benutzergruppen oder Gerätegruppen zu.

Rechtliche Hinweise

Patente, sofern zutreffend, zu finden unter: www.blackberry.com/patents.

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