BlackBerry UEM

E-Mail, Kalender und Kontakte

Verwalten

12.13

Inhalt

Einrichten des geschäftlichen E-Mail-Kontos für Geräte

Mithilfe der folgenden Optionen ermöglichen Sie Benutzern das Lesen und Senden geschäftlicher E-Mails auf Geräten:

- Sie können E-Mail, Kalender und Kontakte für Benutzergeräte mithilfe von BlackBerry Work verwalten. Weitere Informationen zum Verwalten von BlackBerry Work finden Sie unter Verwalten von BlackBerry Dynamics-Apps und im BlackBerry Work-Administratorhandbuch.
- Sie können mit 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.
- 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.

Steuern, welche Geräte Zugriff auf Exchange ActiveSync haben dürfen

Sie können die unbefugte Nutzung von 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.

Für die Verwendung des BlackBerry Gatekeeping Service ist es erforderlich, eine Gatekeeping-Konfiguration für Microsoft Exchange Server oder Microsoft Office 365 zu erstellen, ein Gatekeeping-Profil zuzuweisen und ein E-Mail-Profil oder BlackBerry Work zu konfigurieren, das auf den automatischen Gatekeeping-Server verweist.

Nachdem Sie BlackBerry UEM für die Verwendung von BlackBerry Gatekeeping Service konfiguriert haben, werden die Geräte der Benutzer automatisch der Positivliste hinzugefügt. 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).

Für jedes Gerät kann nur ein E-Mail-Client zur Positivliste hinzugefügt werden. Das gilt allerdings nicht für Android Enterprise- und Samsung Knox-Geräte, die eine App-Konfiguration verwenden, die die Whitelisting-Daten vom Exchange Server enthält. Bei diesen Geräten haben die Whitelists für E-Mail-Anwendungen folgende Priorität:

1. E-Mail-Anwendungen mit Anwendungskonfigurationen, die die Whitelisting-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 BlackBerry UEM-Komponenten installiert ist, können Sie die Standardeinstellungen ändern, um BlackBerry Gatekeeping Service in jedem BlackBerry Connectivity Node zu deaktivieren. Weitere Informationen zum Installieren und Konfigurieren eines BlackBerry Connectivity Node finden Sie in der Dokumentation zur Planung und in der Dokumentation zu Installation und Upgrade.

Wenn Ihr Unternehmen BlackBerry 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. Weitere Informationen zur Installation und Konfiguration eines BlackBerry Connectivity Node finden Sie unter Installation oder Upgrade von BlackBerry Connectivity Node in der Dokumentation zur BlackBerry UEM Cloud-Konfiguration.

Sie können Servergruppen einrichten, um den Verbindungsdatenverkehr des Geräts an eine bestimmte regionale Verbindung zur BlackBerry Infrastructure 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.

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	Zugriff auf Exchange ActiveSync nur über autorisierte Geräte zulassen.
3	Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.
4	Erstellen einer Gatekeeping-Konfiguration.
5	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 Office 365 erstellen und diesem die erforderlichen Gatekeeping-Berechtigungen zuweisen.

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

Wenn Sie Microsoft Exchange Server 2010 oder höher 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` über eine 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. Führen Sie diesen Schritt nur dann durch, wenn Sie Microsoft Exchange 2013 oder höher verwenden. Geben Sie `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox` ein. Drücken Sie die Eingabetaste.
11. Führen Sie diesen Schritt nur dann durch, wenn Sie Microsoft Exchange 2013 oder höher verwenden. 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. Führen Sie diesen Schritt nur dann durch, wenn Sie Microsoft Exchange 2013 oder höher verwenden. Geben Sie `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm` ein. Drücken Sie die Eingabetaste.

Wenn Sie fertig sind: Zugriff auf Exchange ActiveSync nur über autorisierte Geräte zulassen.

Zugriff auf Exchange ActiveSync nur über autorisierte Geräte zulassen

Wenn Ihr Unternehmen Microsoft Exchange Server 2010 oder höher verwendet, lesen Sie die Informationen unter Konfigurieren von Microsoft Exchange für den ausschließlichen Zugriff autorisierter Geräte auf Exchange ActiveSync.

Wenn Ihr Unternehmen Microsoft Office 365 verwendet, lesen Sie die Informationen unter Konfigurieren der Zugriffsrichtlinie für mobile Geräte in Microsoft Office 365.

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

Sie müssen Microsoft Exchange Server 2010 oder höher 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 jedes Gerät kann nur ein E-Mail-Client auf die Whitelist gesetzt werden. Die Whitelists für E-Mail-Anwendungen haben folgende Priorität:

1. E-Mail-Anwendungen mit App-Konfiguration, die die Whitelisting-Daten von Exchange Server enthalten (nur für Android Enterprise oder Samsung KNOX Play for Work)
2. BlackBerry Work
3. E-Mail-Client, über den die EAS-ID während der Registrierung gesendet wird

Für die Durchführung dieses Schritts ist es erforderlich, Microsoft Exchange-Administrator mit den entsprechenden Berechtigungen zum Konfigurieren des Parameters „Set-ActiveSyncOrganizationSettings“ zu sein. Informationen über die ausschließliche Zulassung autorisierter Geräte für den Zugriff auf Exchange ActiveSync finden Sie auf https://technet.microsoft.com in dem Artikel *Aktivieren eines Geräts für Exchange ActiveSync*.

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 Office 365

Zum Verwenden von BlackBerry Gatekeeping Service mit Microsoft Office 365 müssen Sie die Standardzugriffsrichtlinie für mobile Geräte in Microsoft Office 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 Office 365-Verwaltungsportal an.
2. Klicken Sie im Seitenmenü 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. Führen Sie die folgenden Aktionen auf dem Computer aus, der die Microsoft-Client-Zugriffs-Serverrolle hostet.

Bevor Sie beginnen: Zugriff auf Exchange ActiveSync nur über autorisierte Geräte zulassen.

1. Öffnen Sie 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.

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 Office 365 herstellen können.

Bevor Sie beginnen:

- Konfigurieren von Berechtigungen für Gatekeeping.
- Zugriff auf Exchange ActiveSync nur über autorisierte Geräte zulassen.
- Konfigurieren von Microsoft IIS-Berechtigungen für Gatekeeping.

1. Führen Sie eine der folgenden Aktionen 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. Geben Sie im Feld **Servername** den Namen der Microsoft Exchange Server- oder Microsoft Office 365-Umgebung ein, für die der Zugriff verwaltet werden soll.
4. Geben Sie den Benutzernamen und das Kennwort für das Konto ein, das Sie für die Verwaltung von Exchange ActiveSync-Gatekeeping erstellt haben.
5. Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** die unter Microsoft Exchange Server oder Microsoft Office 365 verwendete Authentifizierung aus.
6. Um die SSL-Authentifizierung zwischen BlackBerry UEM und dem Microsoft Exchange Server oder Microsoft Office 365 zu ermöglichen, aktivieren Sie das Kontrollkästchen **SSL verwenden**. Optional können weitere Zertifikatprüfungen ausgewählt werden.
7. 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 Office 365 verwendet wird.
8. Wenn Sie im vorhergehenden Schritt eine Proxy-Konfiguration ausgewählt haben, wählen Sie den Authentifizierungstyp für den Proxy-Server aus.
9. Wählen Sie bei Bedarf **Authentifizierung erforderlich**, und geben Sie den Benutzernamen und das Kennwort ein.
10. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob die Verbindung erfolgreich ist.
11. Klicken Sie auf **Speichern**.
12. Klicken Sie im Abschnitt **E-Mail-Client-Liste für Android for Work** auf +.

Hinweis: BlackBerry Hub +-Dienste werden standardmäßig zur Liste hinzugefügt.

13. Wählen Sie eine E-Mail-App aus, und klicken Sie auf **Weiter**.
14. Wählen Sie in der Dropdown-Liste **Geräte-ID** das Feld der App-Konfiguration aus, die der Geräte-ID zugeordnet ist.
15. Wählen Sie in der Dropdown-Liste **E-Mail-Adresse** das Feld der App-Konfiguration aus, die der E-Mail-Adresse des Benutzers zugeordnet ist.

Wenn Sie fertig sind:

- Erstellen eines Gatekeeping-Profils und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.
- Wenn Sie eine 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

Wenn Sie automatisches Gatekeeping verwenden, erstellen Sie ein Gatekeeping-Profil.

Wenn Sie den BlackBerry Gatekeeping Service konfiguriert haben, müssen Sie ein Gatekeeping-Profil erstellen und dieses Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen. Mit dem Gatekeeping-Profil können Sie die Microsoft Exchange-Server für die automatische Gatekeeping-Funktion auswählen.

1. Klicken Sie in der Menüleiste 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 einen oder mehrere Server aus, und klicken Sie auf →.
7. Klicken Sie auf **Speichern**.

Überprüfen, ob ein Gerät für den Zugriff auf geschäftliche E-Mails und Terminplanerdaten zugelassen ist

Wenn Ihre Organisation BlackBerry Gatekeeping Service verwendet, um zu steuern, welche Geräte von Exchange ActiveSync aus auf geschäftliche E-Mails und Terminplanerdaten zugreifen können, wird mindestens ein Gatekeeping-Server für ein E-Mail-Profil konfiguriert. Wenn das E-Mail-Profil mit konfiguriertem Gatekeeping einem Benutzerkonto zugewiesen wird, können Sie den Verbindungsstatus zwischen einem Gerät und Exchange ActiveSync überprüfen. Sie können den Status suchen, indem Sie sich die Seite mit den Gerätedetails im Abschnitt „IT-Richtlinien und -Profile“ ansehen. Die folgenden Statuswerte werden bei den Gerätedetails neben dem E-Mail-Profil angezeigt.

Status	Beschreibung
Unbekannt	Der Status „Unbekannt“ 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 zugelassenen Liste manuell hinzugefügt werden.
Anstehende Verbindung	Der Status „Anstehende Verbindung“ wird angezeigt, wenn BlackBerry UEM die ID des Geräts kennt und das Gerät in der Warteschlange auf die Hinzufügung zur zugelassenen Liste wartet.
Zugelassene Verbindung	Der Status „Zugelassene Verbindung“ wird angezeigt, wenn BlackBerry UEM die ID des Geräts kennt und das Gerät auf der zugelassenen Liste vorhanden ist.

Überprüfen, ob ein Gerät auf Exchange ActiveSync zugreifen darf

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.

4. Wählen Sie die Registerkarte für das zu überprüfende Gerät aus.
5. Wenn das Gerät zugelassen ist, wird im Abschnitt **IT-Richtlinien und -Profile** neben dem E-Mail-Profil **Verbindung zugelassen** angezeigt.

Ermöglichen des Zugriffs eines Geräts auf Microsoft ActiveSync

Wenn BlackBerry UEM keine Exchange ActiveSync-ID von einem Gerät abrufen kann, wird es nicht der Positivliste für Microsoft Exchange hinzugefügt. Sie können diese Geräte aus der Liste der gesperrten Exchange ActiveSync-Geräte manuell der Positivliste hinzufügen. Wenn ein Android-Gerät beispielsweise mithilfe der MDM-Aktivierungsart aktiviert wird, kann BlackBerry UEM keine Exchange ActiveSync-ID abrufen, und Sie müssen das Gerät aus der Liste der gesperrten Exchange ActiveSync-Geräte manuell zur Positivliste hinzufügen.

1. Klicken Sie in der Menüleiste auf **Benutzer > Exchange Gatekeeping**.
2. Suchen Sie ein Gerät.
3. Klicken Sie in der Spalte **Aktion** auf ✓.

Sperren eines Geräts für den Zugriff auf Microsoft ActiveSync

Sie können ein zuvor zugelassenes Geräte manuell vom Zugriff auf Microsoft ActiveSync ausschließen. Der Ausschluss eines Geräts verhindert, dass Benutzer E-Mail-Nachrichten und andere Informationen vom Microsoft Exchange Server auf dem Gerät abrufen.

1. Klicken Sie in der Menüleiste auf **Benutzer**.
2. Klicken Sie auf **Exchange Gatekeeping**.
3. Suchen Sie ein Gerät.
4. Klicken Sie in der Spalte **Aktion** 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.

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

- Zur Erhöhung der E-Mail-Sicherheit können Sie S/MIME für iOS- und Android-Geräte aktivieren. Sie können S/MIME oder PGP für BlackBerry 10-Geräte aktivieren. PGP wird von BlackBerry 10 OS Version 10.3.1 und höher unterstützt.
- 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 Folgendes beachten:

- Um Notes Traveler mit iOS-Geräten zu nutzen, müssen Sie den BlackBerry Secure Gateway aktivieren.
- Die Synchronisierung von Aufgabendaten wird nur auf BlackBerry 10-Geräten unterstützt. Sie nutzt das SyncML-Kommunikationsprotokoll auf dem Notes Traveler-Server.
- Zur Erhöhung der E-Mail-Sicherheit auf BlackBerry 10-Geräten wird nur die IBM Notes-Verschlüsselung unterstützt (nicht aber S/MIME).
- Wenn Sie Notes Traveler mit der IBM Verse-Client-App verwenden möchten, gehen Sie folgendermaßen vor:
  - Konfigurieren Sie für Samsung Knox-Geräte die Einstellungen für IBM Verse im E-Mail-Profil.
  - Konfigurieren Sie für Android Enterprise-Geräte die Einstellungen für IBM Verse mithilfe der App-Konfiguration.

Sie können auch mit 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.

Sie können BlackBerry Work anstelle eines E-Mail-Profils für die Verwaltung von E-Mail, Kalender und Kontakten für Benutzergeräte verwenden. Weitere Informationen zum Verwalten von BlackBerry Work finden Sie unter Verwalten von BlackBerry Dynamics-Apps und im BlackBerry Work-Administratorhandbuch.

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.
- Damit ein E-Mail-Profil automatisch auf Android-Geräte angewendet werden kann, müssen die Geräte eines der nachfolgend aufgeführten Kriterien erfüllen. Wenn das Gerät keines dieser Kriterien erfüllt, sendet BlackBerry UEM das E-Mail-Profil zwar an Android-Geräte, aber der Benutzer muss die Verbindung zum E-Mailserver manuell konfigurieren:
  - Android Enterprise-Geräte
  - Samsung Knox- und Samsung Knox Workspace-Geräte
  - Motorola-Geräte

1. Klicken Sie in der Menüleiste 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.

   Weitere Informationen über BlackBerry Connectivity Node und Servergruppen finden Sie in der Dokumentation zur Planung von lokalen Umgebungen und in der Dokumentation zu Installation und Upgrade oder in der UEM Cloud Dokumentation zur Konfiguration
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: Legen Sie ggf. eine Rangfolge für die Profile fest.

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
- BlackBerry 10

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.

Allgemein: E-Mail-Profileinstellung	Beschreibung
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.
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. Weitere Informationen zum BlackBerry Connectivity Node und zu den Servergruppen in einer lokalen Umgebung finden Sie in der Dokumentation zur Planung und in der Dokumentation zu Installation und Upgrade. Weitere Informationen über BlackBerry Connectivity Node und Servergruppen in einer Cloud-Umgebung finden Sie in der Dokumentation zur BlackBerry UEM Cloud-Konfiguration.

iOS: E-Mail-Profileinstellungen

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 iOS-Gerät verschieben können.
Zulassen, dass letzte Adressen synchronisiert werden	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes zuletzt verwendete 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.
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.

iOS: E-Mail-Profileinstellung	Beschreibung
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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen 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 iOS-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.
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 gilt nur für Geräte mit iOS 12.0 und höher. 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 gilt nur für Geräte mit iOS 12.0 und höher. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen 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 iOS-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.
Benutzer kann S/MIME-Verschlüsselung überschreiben	Diese Einstellung gibt an, ob ein Benutzer die Verschlüsselungseinstellung ein- oder ausschalten kann. Diese Einstellung gilt nur für Geräte mit iOS 12.0 und höher. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
Benutzer kann S/MIME-Verschlüsselungs-Anmeldeinformationen überschreiben	Diese Einstellung gibt an, ob ein Benutzer S/MIME-Verschlüsselungs-Anmeldeinformationen überschreiben kann. Diese Einstellung gilt nur für Geräte mit iOS 12.0 und höher. 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. Mögliche Werte: • Erforderlich • zulassen Der Standardwert ist „Erforderlich“. 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 iOS-Gerät synchronisiert werden sollen. Mögliche Werte: • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat • Unbegrenzt Der Standardwert ist „7 Tage“. **Hinweis:** Diese Einstellung betrifft nur die Standard-Mail- und Standard-Terminplaner-App auf iOS-Geräten mit der Aktivierungsart „MDM-Steuerelemente“.
Authentifizierung	
BlackBerry Secure Gateway aktivieren	Diese Einstellung legt fest, ob iOS-Geräte mit der Aktivierungsart MDM-Steuerelemente den 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.

iOS: E-Mail-Profileinstellung	Beschreibung
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein iOS-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „BlackBerry Secure Gateway aktivieren“ nicht ausgewählt ist. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Profil für freigegebenes Zertifikat	Diese Einstellung legt für das Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein iOS-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 iOS-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 iOS-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. Diese Einstellung gilt nur für Geräte mit iOS 12.1.1 und höher.
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. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Kontakte	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre Geschäftskontakte zugreifen können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Kalender	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihren Geschäftskalender zugreifen können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Erinnerungen	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre geschäftlichen Erinnerungen zugreifen können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Notizen	Diese Einstellung legt fest, ob Benutzer auf dem Gerät auf ihre Geschäftsnotizen zugreifen können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Änderungen an Konten	
E-Mail	Diese Einstellung legt fest, ob Benutzer den Zugriff auf geschäftliche E-Mails auf dem Gerät aktivieren oder deaktivieren können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.

iOS: E-Mail-Profileinstellung	Beschreibung
Kontakte	Diese Einstellung legt fest, ob Benutzer den Zugriff auf Geschäftskontakte auf dem Gerät aktivieren oder deaktivieren können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Kalender	Diese Einstellung legt fest, ob Benutzer den Zugriff auf den Geschäftskalender auf dem Gerät aktivieren oder deaktivieren können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Erinnerungen	Diese Einstellung legt fest, ob Benutzer den Zugriff auf geschäftliche Erinnerungen auf dem Gerät aktivieren oder deaktivieren können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.
Notizen	Diese Einstellung legt fest, ob Benutzer den Zugriff auf Geschäftsnotizen auf dem Gerät aktivieren oder deaktivieren können. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.

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

Hinweis: In einer kommenden Version von BlackBerry UEM werden die für BlackBerry Hub + und Divide Productivity geltenden Einstellungen aus dem E-Mail-Profil entfernt und sind nur in den App-Einstellungen in einer App-Konfiguration verfügbar. Wenn Sie die App-Einstellungen dagegen in dieser Version hier und in einer App-Konfiguration festlegen, hat die App-Konfiguration Vorrang, falls beide Konfigurationen zugewiesen werden.

Android: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll. Mögliche Werte: • Exchange ActiveSync • IBM Notes Traveler Der Standardwert ist „Exchange ActiveSync“.
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. Mögliche Werte: • Unbeschränkt • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat Der Standardwert ist „1 Monat“. 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 der Aktivierungsart „MDM-Steuerelemente“.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Android-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.

Android: E-Mail-Profileinstellung	Beschreibung
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. Mögliche Werte sind 1 bis 365. Die Standardeinstellung ist 25. Diese Einstellung gilt nur für Android Enterprise-Geräte.
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.

Android: E-Mail-Profileinstellung	Beschreibung
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. Für Android Enterprise-Geräte 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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Die Standardeinstellung ist „Freigegebenes Zertifikat“.
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. Für Android Enterprise-Geräte 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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Die Standardeinstellung ist „Freigegebenes Zertifikat“.
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.

Android: E-Mail-Profileinstellung	Beschreibung
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 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.
BlackBerry Productivity Suite Diese Einstellungen gelten nur für Android Enterprise-Geräte.	
OSCP-Prüfung ausführen	Diese Einstellung legt fest, ob Geräte OCSP verwenden können, um den Status von S/MIME-Zertifikaten zu prüfen.
Zulassen, dass Benutzer nicht vertrauenswürdige Zertifikate akzeptieren	Diese Einstellung legt fest, ob Benutzer die Verwendung nicht vertrauenswürdiger Zertifikate auf Geräten akzeptieren können.
Zulassen, dass Telemetrie-Ereignisse von einem geschäftlichen Profil gesendet werden	Diese Einstellung legt fest, ob die BlackBerry Productivity Suite die Erfassung von Nutzungsdaten erlaubt.
Sicherheitstyp	Diese Einstellung gibt den Sicherheitstyp an, der von BlackBerry Productivity Suite verwendet wird. Mögliche Werte: • SSL • SSL: Allen vertrauen Der Standardwert ist „SSL“.

Android: E-Mail-Profileinstellung	Beschreibung
Freigabe von Daten zwischen geschäftlichen und persönlichen Profilen zulassen	Diese Einstellung gibt an, ob das persönliche Profil auf Daten des Arbeitsprofils zugreifen kann. Wählen Sie diese Einstellung und „Einschränken des Zugriffs von persönlichen Apps auf geschäftliche Daten zulassen“ aus, um die folgenden Funktionen zu aktivieren: • Ein einheitlicher BlackBerry Hub, der persönliche und geschäftliche Konten umfasst. Weitere Informationen finden Sie unter Aktivieren eines einheitlichen BlackBerry Hub. • Ein einheitliches Tastaturwörterbuch, mit dem gelernte Wörter in persönlichen und geschäftlichen Profilen freigegeben werden können. Benutzer können auswählen, ob das einheitliche Tastaturwörterbuch für Vorschläge und Korrekturen verwendet werden soll. .
Persönlichen Apps Zugriff auf geschäftliche Daten gewähren	Diese Einstellung legt fest, ob persönliche Apps auf geschäftliche Daten zugreifen können. Wählen Sie diese Einstellung und „Freigabe von Daten zwischen geschäftlichen und persönlichen Profilen zulassen“ aus, um die folgenden Funktionen zu aktivieren: • Ein einheitlicher BlackBerry Hub, der persönliche und geschäftliche Konten umfasst. Weitere Informationen finden Sie unter Aktivieren eines einheitlichen BlackBerry Hub. • Ein einheitliches Tastaturwörterbuch, mit dem gelernte Wörter in persönlichen und geschäftlichen Profilen freigegeben werden können. Benutzer können auswählen, ob das einheitliche Tastaturwörterbuch für Vorschläge und Korrekturen verwendet werden soll.
S/MIME-Einstellungen Diese Einstellungen gelten nur für Android Enterprise-Geräte.	
S/MIME-Unterstützung	Diese Einstellung legt fest, ob ein Android-Gerät, das BlackBerry Productivity Suite nutzt, S/MIME-geschützte E-Mail-Nachrichten senden kann. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.

Android: E-Mail-Profileinstellung	Beschreibung
Digital signierte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein Android-Gerät, das BlackBerry Productivity Suite nutzt, ausgehende E-Mail-Nachrichten mit digitaler Signatur sendet. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.
Verschlüsselte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein Android-Gerät, das BlackBerry Productivity Suite nutzt, ausgehende E-Mail-Nachrichten mit S/MIME-Verschlüsselung verschlüsselt. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.
S/MIME-Verschlüsselungsalgorithm	Diese Einstellung gibt die Verschlüsselungsalgorithmen an, mit denen ein Android-Gerät, das BlackBerry Productivity Suite nutzt, S/MIME-geschützte E-Mail-Nachrichten verschlüsseln kann. Mögliche Werte: • AES (256-Bit) • AES (192-Bit) • AES (128-Bit) • Triple DES • ARC2

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. Mögliche Werte: • Exchange ActiveSync • IBM Notes Traveler Der Standardwert ist „Exchange ActiveSync“.

Windows: E-Mail-Profileinstellung	Beschreibung
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. Mögliche Werte: • Wenn Elemente empfangen werden • Manuell • 15 Minuten • 30 Minuten • 60 Minuten Der Standardwert ist „Wenn Elemente empfangen werden“.
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. Mögliche Werte: • Unbegrenzt • 3 Tage • 7 Tage • 14 Tage • 1 Monat Der Standardwert ist „7 Tage“.
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.
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.

BlackBerry 10: E-Mail-Profileinstellungen

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Kontoname	Diese Einstellung legt den Namen des geschäftlichen E-Mail-Kontos fest, der in BlackBerry Hub und in den Geräteeinstellungen angezeigt wird. Sie können eine Variable wie etwa „%UserEmailAddress%“ verwenden.
Port	Diese Einstellung legt den Port fest, der für die Verbindung zum Mailserver verwendet wird.
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll. Mögliche Werte: • Exchange ActiveSync • IBM Notes Traveler Der Standardwert ist „Exchange ActiveSync“.
SyncML-Server	Diese Einstellung legt den FQDN des IBM Notes Traveler-Servers fest, den ein BlackBerry 10-Gerät verwenden kann, um Aufgabendaten zu synchronisieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
SyncML-Port	Diese Einstellung legt den Port des Notes Traveler-Servers fest, den ein BlackBerry 10-Gerät verwenden kann, um Aufgabendaten zu synchronisieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
SSL für SyncML verwenden	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät eine SSL-Verbindung zum Notes Traveler-Server aufbauen muss. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
Push aktiviert	Diese Einstellung legt fest, ob der Mailserver E-Mail-Nachrichten mithilfe von Push auf ein BlackBerry 10-Gerät übertragen kann.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Zeitraum zwischen Synchronisierungen	Diese Einstellung legt fest, wie häufig ein BlackBerry 10-Gerät neue E-Mail-Nachrichten vom Mailserver abruft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Push aktiviert“ nicht ausgewählt ist. Mögliche Werte: • Manuell • 5 Minuten • 15 Minuten • 30 Minuten • 1 Stunde • 2 Stunden • 4 Stunden • 24 Stunden Der Standardwert ist „15 Minuten“.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein BlackBerry 10-Gerät synchronisiert werden sollen. Mögliche Werte: • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat • Unbegrenzt Der Standardwert ist „1 Monat“.
Beim Roaming manuelle Synchronisierung initiieren	Diese Einstellung legt fest, ob ein Benutzer beim Roaming eine Synchronisierung zwischen einem BlackBerry 10-Gerät und dem Mailserver starten muss.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Kalendersynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Kalendereinträge mit dem Mailserver synchronisiert.
Kontaktsynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Kontakte mit dem Mailserver synchronisiert.
E-Mail-Synchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät E-Mail-Nachrichten mit dem Mailserver synchronisiert.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Notizensynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Notizen mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.
Aufgabensynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Aufgabendaten mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.
ToDo-Synchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die Aufgabendaten mit Notes Traveler synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
Sichere E-Mail-Einstellungen	
Standardverschlüsselung für ausgehende Nachrichten vorschlagen	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die Standardverschlüsselung (z. B. nur Text, signieren, verschlüsseln oder signieren und verschlüsseln) für alle ausgehenden E-Mail-Nachrichten vorschlägt. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob das Gerät die Standardverschlüsselung oder eine Verschlüsselung basierend auf dem Nachrichtenverlauf vorschlägt. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, schlägt das Gerät die Standardverschlüsselung vor. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, schlägt das Gerät die Verschlüsselung basierend auf dem Nachrichtenverlauf vor. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
S/MIME-Einstellungen	

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
S/MIME-Unterstützung	Diese Einstellung legt fest, ob S/MIME auf einem BlackBerry 10-Gerät aktiviert ist. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob S/MIME-Schutz auf dem Gerät aktiviert oder nicht aktiviert werden soll. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, ist S/MIME-Schutz auf dem Gerät aktiviert, und der Benutzer kann ihn nicht deaktivieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, ist S/MIME-Schutz auf dem Gerät deaktiviert, und der Benutzer kann ihn nicht aktivieren. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät beziehungsweise der Smartcard zur Verfügung haben. Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät beziehungsweise der Smartcard verfügbar sein. Diese Einstellung hat höhere Priorität als die Einstellungen „Digital signierte S/MIME-Nachrichten“ und „Verschlüsselte S/MIME-Nachrichten“. Diese Einstellung betrifft die Einstellung „PGP-Support“. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss die Einstellung „PGP-Support“ auf „Nicht zulassen“ gesetzt werden. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Digital signierte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät ausgehende E-Mail-Nachrichten mit digitaler Signatur sendet. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann der Benutzer entscheiden, ob er ausgehende E-Mail-Nachrichten digital signieren möchte. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss der Benutzer ausgehende E-Mail-Nachrichten digital signieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, kann der Benutzer ausgehende E-Mail-Nachrichten nicht digital signieren. Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät beziehungsweise der Smartcard verfügbar sein. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME-Unterstützung“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ gesetzt ist und sowohl diese Einstellung als auch die Einstellung „Verschlüsselte S/MIME-Nachrichten“ auf „Nicht zulassen“ gesetzt sind, werden die Einstellung „Verschlüsselte S/MIME-Nachrichten“ und diese Einstellung ignoriert, und die Standardeinstellung „Zulassen“ wird für beide Einstellungen verwendet. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Verschlüsselte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät ausgehende E-Mail-Nachrichten mit S/MIME-Verschlüsselung verschlüsselt. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann der Benutzer entscheiden, ob ausgehende E-Mail-Nachrichten verschlüsselt oder nicht verschlüsselt werden sollen. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss der Benutzer ausgehende E-Mail-Nachrichten verschlüsseln. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, kann der Benutzer ausgehende E-Mail-Nachrichten nicht verschlüsseln. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät beziehungsweise der Smartcard zur Verfügung haben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME-Unterstützung“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ gesetzt ist und sowohl diese Einstellung als auch die Einstellung „Digital signierte S/MIME-Nachrichten“ auf „Nicht zulassen“ gesetzt sind, werden die Einstellung „Digital signierte S/MIME-Nachrichten“ und diese Einstellung ignoriert, und die Standardeinstellung „Zulassen“ wird für beide Einstellungen verwendet. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.
Verschlüsselungsalgorithmen	Diese Einstellung gibt die Verschlüsselungsalgorithmen an, mit denen ein BlackBerry 10-Gerät S/MIME-geschützte E-Mail-Nachrichten verschlüsseln kann. Mögliche Werte: • AES (256-Bit) • AES (192-Bit) • AES (128-Bit) • Triple DES • RC2 Der Standardwert ist ein Nullwert.
PGP-Einstellungen	

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
PGP-Unterstützung	Diese Einstellung legt fest, ob PGP-Schutz auf einem BlackBerry 10-Gerät aktiviert ist. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob PGP-Schutz auf dem Gerät aktiviert oder nicht aktiviert werden soll. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, ist PGP-Schutz auf dem Gerät aktiviert, und der Benutzer kann ihn nicht deaktivieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, ist PGP-Schutz auf dem Gerät deaktiviert, und der Benutzer kann ihn nicht aktivieren. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät zur Verfügung haben. Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät verfügbar sein. Die Einstellung „S/MIME-Unterstützung“ betrifft diese Einstellung. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ oder „Zulassen“ gesetzt und die Einstellung „Digital signierte S/MIME-Nachrichten“ oder die Einstellung„Verschlüsselte S/MIMW-Nachrichten“ auf „Erforderlich“ gesetzt ist, muss diese Einstellung auf „Nicht zulassen“ gesetzt werden. Mögliche Werte: • zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Symantec Encryption Management Server-Adresse	Diese Einstellung legt den FQDN oder die IP-Adresse für den Symantec Encryption Management Server Ihrer Organisation fest, damit ein BlackBerry 10-Gerät bei diesem Server angemeldet werden muss, um PGP-Nachrichten senden zu können. Die Einstellung „PGP-Support“ betrifft diese Einstellung. Das Gerät verwendet diese Einstellung, wenn die Einstellung „PGP-Support“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Symantec Encryption Management Server-Anmeldemethode	Diese Einstellung legt die Methode fest, mit der sich der Benutzer eines BlackBerry 10-Geräts beim Symantec Encryption Management Server Ihrer Organisation anmelden muss. Wenn diese Einstellung auf „E-Mail-Authentifizierung“ gesetzt ist, wird der Benutzer zur Eingabe einer E-Mail-Adresse aufgefordert. Wenn diese Einstellung auf „Microsoft Active Directory-Authentifizierung“ gesetzt ist, wird der Benutzer aufgefordert, einen Domänen-Benutzernamen und ein Kennwort einzugeben. Die Einstellung „PGP-Support“ betrifft diese Einstellung. Das Gerät verwendet diese Einstellung, wenn die Einstellung „PGP-Support“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Mögliche Werte: • E-Mail-Authentifizierung • Microsoft Active Directory-Authentifizierung Der Standardwert ist „E-Mail-Authentifizierung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Verknüpfte Profile	
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein BlackBerry 10-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Mögliche Werte: • Keine • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver anmeldet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, mit denen der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver erhält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Nachrichtenklassifizierung	

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Nachrichtenklassifizierungsdatei (.json)	Diese Einstellung gibt die Nachrichtenklassifizierungsdatei an, die an Benutzergeräte gesendet werden soll. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

S/MIME-Profil und Geräteeinstellungsabhängigkeiten

Die folgende Tabelle zeigt die Abhängigkeiten zwischen den S/MIME-Einstellungen, die Sie in BlackBerry UEM konfigurieren können, und den S/MIME-Einstellungen, die Benutzer auf BlackBerry 10-Geräten konfigurieren können. Abhängig von den jeweiligen Einstellungen ändern sich die Optionen in der Dropdown-Liste „Verschlüsselung“ auf den Geräten. Geräte ignorieren den Wert einiger Einstellungen, wenn eine höhere Prioritätseinstellung (z. B. die Einstellung „S/MIME-Unterstützung“) mit dem Wert für diese Einstellung in Konflikt steht.

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
Zulässig	Zulässig	Zulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	Nur-Text Signieren (S/MIME) Verschlüsseln (S/MIME) Signieren und verschlüsseln (S/MIME)
	Zulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME) Signieren und verschlüsseln (S/MIME)
	Zulässig	Unzulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	Nur-Text Signieren (S/MIME)
	Erforderlich	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME) Signieren und verschlüsseln (S/MIME)
	Erforderlich	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren und verschlüsseln (S/MIME)

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
	Erforderlich	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Unzulässig	Zulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	Nur-Text Verschlüsseln (S/MIME)
	Unzulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)
	Unzulässig	Unzulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten, aber er kann Nachrichten nicht verschlüsseln oder signieren, da die erforderlichen Profile auf „Unzulässig“ eingestellt sind.	Nur-Text
Erforderlich	Zulässig	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME) Verschlüsseln (S/MIME) Signieren und verschlüsseln (S/MIME)
	Zulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME) Signieren und verschlüsseln (S/MIME)
	Zulässig	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Erforderlich	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME) Signieren und verschlüsseln (S/MIME)
	Erforderlich	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren und verschlüsseln (S/MIME)

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
	Erforderlich	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Unzulässig	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)
	Unzulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)
	Unzulässig (Diese Einstellung wird ignoriert)	Unzulässig (Diese Einstellung wird ignoriert)	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME) Verschlüsseln (S/MIME) Signieren und verschlüsseln (S/MIME)
Unzulässig	Alle Einstellungen werden ignoriert	Alle Einstellungen werden ignoriert	S/MIME-Schutz ist ausgeschaltet. Der Benutzer kann ihn nicht einschalten.	Nur-Text

PGP-Profil und Geräteeinstellungsabhängigkeiten

Die folgende Tabelle zeigt die Abhängigkeiten zwischen der „PGP-Unterstützung“, die Sie in BlackBerry UEM konfigurieren können, und den PGP-Einstellungen, die Benutzer auf BlackBerry 10-Geräten konfigurieren können. Abhängig von der Einstellung der „PGP-Unterstützung“ ändern sich die Optionen in der Dropdown-Liste „Verschlüsselung“ auf den Geräten. Geräte ignorieren den Wert dieser Einstellung, wenn eine höhere Prioritätseinstellung (z. B. die Einstellung „S/MIME-Unterstützung“) mit dem Wert für diese Einstellung in Konflikt steht.

Einstellung „PGP-Unterstützung“	PGP-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
zulassen	Die Benutzer können den PGP-Schutz ein- oder ausschalten.	• Nur-Text • Signieren (PGP) • Verschlüsseln (PGP) • Signieren und verschlüsseln (PGP)

Einstellung „PGP-Unterstützung“	PGP-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
Erforderlich	PGP-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (PGP) • Verschlüsseln (PGP) • Signieren und verschlüsseln (PGP)
Nicht zulassen	PGP-Schutz ist ausgeschaltet. Der Benutzer kann ihn nicht einschalten.	Keine Dropdown-Liste. Nur-Text wird verwendet.

Schützen von E-Mail-Daten mithilfe von BlackBerry Secure Gateway

Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte mit Aktivierungsart „MDM-Steuerelemente“.

Durch Aktivierung des BlackBerry Secure Gateway können Geräte mit Aktivierungsart „MDM-Steuerelemente“ geschäftliche E-Mails senden und empfangen, ohne dass Sie Ihren E-Mail-Server außerhalb der Firewall oder in einer DMZ bereitstellen müssen.

Wenn Sie den BlackBerry Secure Gateway verwenden möchten, müssen Sie sicherstellen, dass Ihr Unternehmen über die entsprechenden Lizenzen verfügt. Weitere Informationen finden Sie in der Dokumentation zur Lizenzierung.

Um den BlackBerry Secure Gateway zu aktivieren, wählen Sie im E-Mail-Profil die Einstellung „BlackBerry Secure Gateway aktivieren“ aus.

Wenn Sie Servergruppen für regionale Verbindung zur BlackBerry Infrastructure konfiguriert haben, können Sie BlackBerry Secure Gateway-Datenverkehr zu einer spezifischen regionalen Verbindung weiterleiten, indem Sie das E-Mail-Profil mit der entsprechenden Servergruppe verknüpfen.

Konfigurieren von TLS/SSL-Verbindungen mit Exchange ActiveSync bei der Aktivierung von BlackBerry Secure Gateway

Wenn Sie den BlackBerry Secure Gateway aktivieren, um über BlackBerry UEM eine sichere Verbindung zwischen dem E-Mail-Server Ihres Unternehmens und iOS-Geräten mit der Aktivierungsart MDM-Steuerelemente zur Verfügung zu stellen, können Sie BlackBerry UEM so konfigurieren, dass TLS/SSL-Verbindungen zu Exchange ActiveSync hergestellt werden.

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

Je nach den Sicherheitsanforderungen des Exchange ActiveSync-Servers müssen Sie möglicherweise auch die Liste der TLS-Versionen und Chiffrierschlüssel aktualisieren, die der BlackBerry Secure Gateway für die Authentifizierung mit Exchange ActiveSync verwenden kann.

Konfigurieren von BlackBerry UEM, sodass das Exchange ActiveSync-Serverzertifikat als vertrauenswürdig erkannt wird

Bevor Sie beginnen: Exportieren Sie das Zertifikat vom Exchange ActiveSync-Server im X.509-Format (*.cer, *.der), und speichern Sie es in einem Netzwerkpfad, auf den Sie über die Verwaltungskonsole zugreifen können.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Vertrauenswürdige Zertifikate**.
2. Klicken Sie auf + neben **Exchange ActiveSync-Server-Vertrauenswürdigkeiten**.
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**.

Konfigurieren von BlackBerry UEM zur Verwendung der TLS-Versionen und der von Exchange ActiveSync unterstützten Chiffrierschlüssel

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > BlackBerry Secure Gateway**.
2. Klicken Sie in der Tabelle, die Sie ändern möchten, 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**.

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

Sie können die E-Mail-Sicherheit für die Benutzer von BlackBerry 10-, iOS- und Android-Geräten durch Aktivierung von S/MIME erhöhen. Mit S/MIME steht ein Standardverfahren zur Verschlüsselung und zum Signieren von E-Mail-Nachrichten zur Verfügung. Die Benutzer können E-Mail-Nachrichten mit dem S/MIME-Schutz signieren, verschlüsseln oder signieren und verschlüsseln, wenn sie E-Mail-Nachrichten von einem geschäftlichen E-Mail-Konto senden, das S/MIME-geschützte Nachrichten auf Geräten unterstützt. S/MIME kann für persönliche E-Mail-Adressen nicht aktiviert werden.

Die Benutzer können die S/MIME-Zertifikate der Empfänger auf ihren Geräten speichern. Benutzer können ihre privaten Schlüssel auf ihren Geräten oder einer Smartcard speichern.

Sie können S/MIME für Benutzer in einem E-Mail-Profil aktivieren. Sie können den Einsatz von S/MIME auf BlackBerry 10-Geräten erzwingen, aber nicht auf iOS- oder Android-Geräten. Wenn die Nutzung von S/MIME optional ist, kann ein Benutzer S/MIME auf dem Gerät aktivieren und angeben, ob E-Mail-Nachrichten verschlüsselt, signiert oder verschlüsselt und signiert werden sollen.

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 BlackBerry 10-Geräten zu ermöglichen, die S/MIME-Zertifikate von LDAP-Servern zu suchen und 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.

Die BlackBerry 10-Geräte durchsuchen jeden LDAP-Zertifikatserver, den Sie im Profil festlegen, und rufen das S/MIME-Zertifikat ab. 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 verlangen, dass die Geräte entweder die einfache Authentifizierung oder Kerberos-Authentifizierung verwenden, um sich bei LDAP-Zertifikatservern zu authentifizieren. Wenn Sie verlangen, dass die Geräte eine einfache Authentifizierung verwenden, können Sie die erforderlichen Authentifizierungs-Anmeldeinformationen in die Zertifikatsabrufprofile einbinden, sodass sich die Geräte automatisch bei den LDAP-Zertifikatservern authentifizieren können. Wenn Sie verlangen, dass die Geräte eine Kerberos-Authentifizierung verwenden, können Sie die erforderlichen Authentifizierungs-Anmeldeinformationen in die Zertifikatsabrufprofile einbinden, sodass sich die Geräte, auf denen BlackBerry 10 OS ab Version 10.3.1 ausgeführt wird, automatisch bei den LDAP-Zertifikatservern authentifizieren können. Andernfalls fordert das Gerät bei der ersten Authentifizierung bei einem LDAP-Zertifikatserver den Benutzer zur Eingabe der erforderlichen Anmeldedaten für die Authentifizierung auf. Bei Geräten, auf denen BlackBerry 10 OS Version 10.2.1 bis 10.3 ausgeführt wird, fordert das Gerät bei der ersten Authentifizierung bei einem LDAP-Zertifikatserver den Benutzer zur Eingabe der erforderlichen Anmeldedaten für die Authentifizierung auf.

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 zum Erstellen und Zuweisen eines Profils für die einmalige Anmeldung finden Sie unter Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte.

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 Profilen für die einmalige Anmeldung finden Sie unter Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Zertifikatabruf**.
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 im Format ldap://<*fqdn*>:<*port*> ein. (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 11 für jeden LDAP-Zertifikatserver.
14. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um BlackBerry 10-Geräten zu erlauben, den Zertifikatstatus zu überprüfen, erstellen Sie ein OCSP- oder CRL-Profil.
- Legen Sie ggf. eine Rangfolge für die Profile fest.

Ermitteln des Status von S/MIME-Zertifikaten auf Geräten

Sie können OCSP- und CRL-Profile verwenden, um den BlackBerry 10-Geräten zu erlauben, den Status der S/MIME-Zertifikate zu überprüfen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein OCSP-Profil und ein CRL-Profil zuweisen.

BlackBerry 10-Geräte durchsuchen jeden OCSP-Responder, den Sie im OCSP-Profil vorgeben, und rufen den Status des S/MIME-Zertifikats ab. Geräte, auf denen BlackBerry 10 OS ab Version 10.3.1 ausgeführt wird, können Zertifikat-Statusabfragen an BlackBerry UEM senden, und Sie können CRL-Profile zur Konfiguration von BlackBerry UEM verwenden, um den Status der S/MIME-Zertifikate mit HTTP, HTTPS oder LDAP zu suchen.

Wenn Sie Exchange ActiveSync für den Zertifikatabruf verwenden, überprüfen iOS- und Android-Geräte den Status von S/MIME-Zertifikaten mithilfe von Exchange ActiveSync. Wenn Sie LDAP für den Zertifikatabruf verwenden, überprüfen iOS- und Android-Geräte den Status von Zertifikaten mithilfe von OCSP. iOS- und Android-Geräte verwenden keine OCSP-Profile. Die Geräte prüfen den OCSP-Responder innerhalb des Zertifikats.

Weitere Informationen zu Zertifikatstatusanzeigen finden Sie im Benutzerhandbuch im Abschnitt zu den Symbolen für sichere E-Mail.

Erstellen eines OCSP-Profils

OCSP-Profile werden auf BlackBerry 10-Geräten unterstützt.

1. Klicken Sie in der Menüleiste 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 Schritt 4 für jeden OCSP-Responder.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Legen Sie ggf. eine Rangfolge für die Profile fest.

Erstellen eines CRL-Profils

CRL-Profile werden für BlackBerry 10- und BlackBerry-Geräte mit Android unterstützt.

1. Klicken Sie in der Menüleiste 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
Festlegen einer HTTP CRL-Konfiguration	**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 die Schritte 1 bis 4 für jeden HTTP- oder HTTPS-Server.
Festlegen einer LDAP CRL-Konfiguration	**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** den Basis-DN ein, der bei der Suche der LDAP-Server der Ausgangspunkt ist. **e.** Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**. **f.** Geben Sie im Feld **LDAP-Benutzer-ID** den DN eines Kontos ein, der Suchberechtigungen auf dem LDAP-Server hat (zum Beispiel cn=admin,dc=example,dc=com). **g.** Geben Sie im Feld **LDAP-Kennwort** das Kennwort für das Konto ein, das Suchberechtigungen auf dem LDAP-Server besitzt. **h.** Klicken Sie auf **Hinzufügen**. **i.** Wiederholen Sie die Schritte 1 bis 8 für jeden LDAP-Server.

7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Legen Sie ggf. eine Rangfolge für die Profile fest.

Erweitern der E-Mail-Sicherheit mit PGP

Bei Geräten mit einer BlackBerry 10 OS Version ab 10.3.1 können Sie die E-Mail-Sicherheit für Gerätebenutzer erweitern, indem Sie PGP aktivieren. 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 BlackBerry 10-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 BlackBerry 10-Geräten sichere E-Mail-Richtlinien festzulegen und durchzusetzen sowie visuelle Markierungen zu E-Mail-Nachrichten hinzuzufügen. Sie können BlackBerry UEM verwenden, um Benutzern von BlackBerry 10-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

Auf Geräten, auf denen BlackBerry 10 OS-Version 10.3.1 und höher ausgeführt wird, können Sie mithilfe der Nachrichtenklassifizierung festlegen, dass Benutzer E-Mail-Nachrichten signieren, verschlüsseln oder signieren und verschlüsseln müssen oder E-Mail-Nachrichten, die sie von ihren Geräten senden, visuelle Markierungen hinzufügen. 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 support.blackberry.com/community im Artikel 36736.

Erstellen eines IMAP/POP3-E-Mail-Profils

IMAP/POP3-E-Mail-Profile legen fest, wie -iOS, -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; der Benutzer muss die Verbindung zum Mailserver jedoch manuell konfigurieren.

1. Klicken Sie in der Menüleiste 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.
14. Klicken Sie auf **Hinzufügen**.

IMAP/POP3-E-Mail-Profileinstellungen

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BlackBerry UEM unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. IMAP/POP3-E-Mail-Profile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- macOS
- Android
- Windows

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BlackBerry UEM unterstützt. Weitere Informationen zu den unterstützten Versionen finden Sie in der Kompatibilitätsmatrix.

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

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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Die Standardeinstellung ist „Freigegebenes Zertifikat“.
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.

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
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.
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. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen 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.

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
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. Mögliche Werte: • Erforderlich • zulassen Der Standardwert ist „Erforderlich“.
Mail Drop zulassen	Diese Einstellung legt fest, ob Benutzer Dateien von diesem Konto mithilfe von Mail Drop senden können.

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. Mögliche Werte: • Nie • Wenn aus Posteingang gelöscht Der Standardwert ist „Nie“. 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). Mögliche Werte: • Unwiederbringlich löschen • Temporär löschen Der Standardwert ist „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. Mögliche Werte: • Manuell • 15 Minuten • 30 Minuten • 60 Minuten • 2 Stunden Der Standardwert ist „15 Minuten“.
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. Mögliche Werte: • Alle • 7 Tage • 14 Tage • 30 Tage Der Standardwert ist „7 Tage“.
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- 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.

Bei macOS gelten Profile für Benutzerkonten oder Geräte. 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 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 Sie die URL für den SSL-Server ein.
9. 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 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 Sie die URL für den SSL-Server ein.
9. Klicken Sie auf **Hinzufügen**.

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

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada