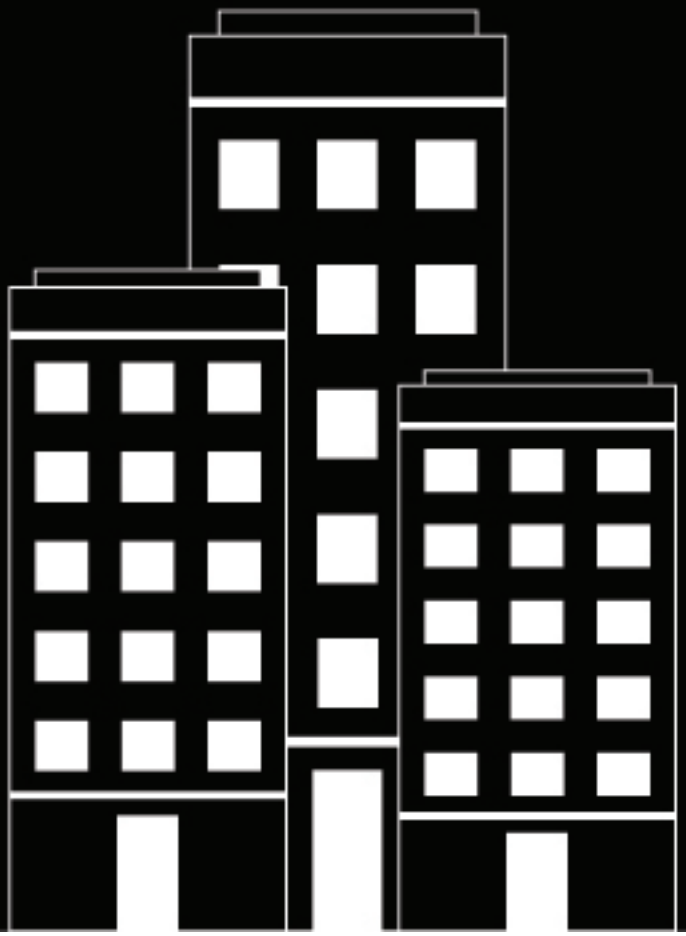

BlackBerry UEM

メール、カレンダー、および連絡先

管理

12.12

目次

デバイスの仕事用メールの設定 5

Exchange ActiveSync にアクセス可能なデバイスの制御 6

Exchange ActiveSync および BlackBerry Gatekeeping Service を設定する手順 7
ゲートキーピングのための権限の設定 7
承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可 9
Microsoft Exchange を設定して承認されているデバイスに対する Exchange ActiveSync へのアクセス許可 9
Microsoft Office 365 でのモバイルデバイスアクセスポリシーの設定 10
ゲートキーピングのための Microsoft IIS 権限を設定する 10
ゲートキーピング設定の作成 11
ゲートキーピングプロファイルの作成 12
デバイスに、仕事用メールおよびオーガナイザーデータへのアクセスが許可されていることの確認 12
Exchange ActiveSync へのアクセスをデバイスが許可されていることの確認 12
デバイスによる Microsoft ActiveSync へのアクセスの許可 13
デバイスによる Microsoft ActiveSync へのアクセスのブロック 13

メールプロファイルの作成 14

メールプロファイルの作成 14
メールプロファイル設定 15
共通：メールプロファイル設定 15
iOS ：メールプロファイル設定 16
macOS ：メールプロファイル設定 22
Android ：メールプロファイル設定 23
Windows ：メールプロファイル設定 29
BlackBerry 10 ：メールプロファイル設定 31

BlackBerry Secure Gateway によるメールデータの保護 41

BlackBerry Secure Gateway を有効にする場合の Exchange ActiveSync への TLS/SSL 接続の設定 41
Exchange ActiveSync サーバー証明書を信頼するように BlackBerry UEM を設定する 41
Exchange ActiveSync がサポートする TLS バージョンと暗号を使用するように BlackBerry UEM を設定します。 42

S/MIME を使用したメールセキュリティの強化 43

S/MIME 証明書の取得 43
証明書の取得プロファイルの作成 43
デバイスでの S/MIME 証明書のステータスの判別 45
OCSP プロファイルの作成 45
CRL プロファイルの作成 45

PGP を使用したメールセキュリティの強化 46
メッセージ分類を使用したセキュリティ保護されたメールの強制 47

IMAP/POP3 メールプロファイルを作成 48
IMAP/POP3 メールプロファイルの設定 48
iOSおよび macOS：IMAP/POP3 メールプロファイルの設定 49
Android ：IMAP/POP3 メールプロファイルの設定 51
Windows ：IMAP/POP3 メールプロファイルの設定 52

iOS および macOS デバイス用 CardDAV プロファイルおよび CalDAV プロファイルの設定 53
CardDAV プロファイルの作成 53
CalDAV プロファイルの作成 53

商標などに関する情報 55

デバイスの仕事用メールの設定

次のいずれかのオプションを使用して、ユーザーがデバイスで仕事用メールを読んだり送信したりできるようにします。

- BlackBerry Work を使用して、ユーザーデバイスのメール、カレンダー、および連絡先を管理できます。BlackBerry Work の管理の詳細については、「BlackBerry Dynamics アプリの管理」および『BlackBerry Work 管理ガイド』を参照してください。
- IMAP/POP3 メールプロファイルを使用して iOS、macOS、Android、および Windows デバイスが IMAP または POP3 メールサーバーに接続して、メールメッセージを同期する方法を指定できます。Knox MDM を使用するようにアクティベーションを行ったデバイスは、IMAP または POP3 をサポートしません。
- メールプロファイルを使用すると、デバイスが組織のメールサーバーに接続し、Exchange ActiveSync または IBM Notes Traveler を使用してメール、カレンダーエントリ、およびオーガナイザーデータを同期する方法を指定できます。

Exchange ActiveSync にアクセス可能なデバイスの制御

デバイスが明示的に許可リストに追加される場合を除き、未許可のデバイスによる Exchange ActiveSync の使用をブロックできます。許可リストにないデバイスは、仕事用メールやオーガナイザーデータにアクセスできません。BlackBerry Gatekeeping Service を使用すると、デバイスを許可リストに簡単に追加できます。

BlackBerry Gatekeeping Service を使用するには、Microsoft Exchange Server または Microsoft Office 365 のゲートキーピング設定を作成して、ゲートキーピングプロファイルを割り当て、自動ゲートキーピングサーバーを参照するメールプロファイルまたは BlackBerry Work を設定する必要があります。

BlackBerry Gatekeeping Service を使用するように BlackBerry UEM を設定すると、ユーザーのデバイスは自動的に許可リストに追加されます。ゲートキーピングプロファイル、メールプロファイル、またはメールアプリがユーザーから削除される場合、ユーザーのデバイスは許可リストから削除され、他の手段（Windows PowerShell など）を使用して許可されないかぎり、Microsoft Exchange に接続できなくなります。

許可リストに追加できる E メールクライアントはデバイスごとに 1 つだけです。ただし、Exchange Server のホワイトリストデータが含まれるアプリ設定を使用する Android Enterprise および Samsung Knox デバイスは例外となります。これらのデバイスでは、メールアプリケーションのホワイトリストの優先度は次のようになります。

1. Exchange Server のホワイトリストデータを含むアプリケーション設定が割り当てられたメールアプリケーション
2. BlackBerry Work
3. 加入時に Exchange ActiveSync ID が送信されるメールクライアント

組織がオンプレミス環境で BlackBerry UEM を使用している場合、BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。各 BlackBerry Connectivity Node には、BlackBerry Gatekeeping Service のインスタンスが含まれています。各インスタンスは、組織のゲートキーピングサーバーにアクセスできる必要があります。プライマリ BlackBerry UEM コンポーネントとともにインストールされる BlackBerry Gatekeeping Service によってのみ、ゲートキーピングデータを管理する場合、それぞれの BlackBerry Connectivity Node で BlackBerry Gatekeeping Service を無効にするようにデフォルト設定を変更できます。BlackBerry Connectivity Node のインストールと設定の詳細については、計画関連の資料およびインストールおよびアップグレード関連の資料を参照してください。

組織で BlackBerry UEM Cloud を使用している場合、BlackBerry Connectivity Node の 1 つまたは 2 つの追加インスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。各 BlackBerry Connectivity Node には、BlackBerry Gatekeeping Service のインスタンスが含まれています。各インスタンスは、組織の Exchange ActiveSync サーバーにアクセスできる必要があります。メイン BlackBerry Connectivity Node とともにインストールされた BlackBerry Gatekeeping Service によってのみ、Exchange ActiveSync アクセス設定を管理する場合、追加 BlackBerry Connectivity Node インスタンスにおいて BlackBerry Gatekeeping Service を無効にするようにデフォルト設定を変更できます。BlackBerry Connectivity Node のインストールおよび設定の詳細については、BlackBerry UEM Cloud の設定関連の資料の「BlackBerry Connectivity Node のインストールまたはアップグレード」を参照してください。

デバイス接続トラフィックを、BlackBerry Infrastructure への特定の地域接続に向けるように、サーバーグループを設定できます。ゲートキーピングプロファイルをサーバーグループに関連付けると、そのゲートキーピングプロファイルが割り当てられているすべてのユーザーは、そのサーバーグループの BlackBerry Gatekeeping Service のアクティブなインスタンスを使用します。サーバーグループを設定する場合、グループ内の BlackBerry Gatekeeping Service のインスタンスを無効にすることができます。

Exchange ActiveSync および BlackBerry Gatekeeping Service を設定する手順

BlackBerry Gatekeeping Service を設定するには、次の操作を実行します。

手順	アクション
1	ゲートキーピングのための権限の設定.
2	承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可.
3	ゲートキーピングのための Microsoft IIS 権限を設定する.
4	ゲートキーピング設定の作成.
5	ゲートキーピングプロファイルを作成し、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。

ゲートキーピングのための権限の設定

Exchange ActiveSync ゲートキーピングを使用するには、Microsoft Exchange Server または Microsoft Office 365 でユーザーアカウントを作成し、ゲートキーピングに必要な権限を与える必要があります。

Microsoft Office 365 を使用している場合は、Microsoft Office 365 ユーザーアカウントを作成し、メール受信者と組織のクライアントアクセスのロールを割り当てます。

Microsoft Exchange Server 2010 以降を使用している場合は、次の手順に従って、Exchange ActiveSync のメールボックスとクライアントアクセスを管理するための適切な権限を持つ管理ロールを設定します。このタスクを実行するには、適切な権限を保持する Microsoft Exchange 管理者として、管理ロールを作成および変更する必要があります。

作業を始める前に：

- Microsoft Exchange をホストするコンピューターで、BlackBerry UEM のゲートキーピングを管理するアカウントとメールボックスを作成します（例：BUEMAdmin）。Exchange ActiveSync を作成するときに、このアカウントのログイン情報を指定する必要があります。このアカウントの名前をメモして、以下のタスクの最後に指定します。
- WinRM は、ゲートキーピングのために設定した Microsoft Exchange Server をホストするコンピューターで、デフォルト設定で構成されている必要があります。管理者として、コマンドプロンプトから「`Winrm quickconfig`」コマンドを実行する必要があります。ツールで「変更しますか `[y/n]`」と表示されたら「`y`」と入力します。コマンドが成功すると、次のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。
```

```
WinRM サービスの種類が遅延自動開始に変更されました。

WinRM サービスが開始されました。

このコンピュータ上のあらゆる IP への WS-Man 要求を受け付けるため、HTTP://* 上に WinRM リス

ナー

 を作成しました。
```

1. Microsoft Exchange Management Shell を開きます。
2. 「`New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`」と入力します。Enter キーを押します。
3. 「`New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`」と入力します。Enter キーを押します。
4. 「`New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`」と入力します。Enter キーを押します。
5. 「`Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`」と入力します。Enter キーを押します。
6. 「`Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`」と入力します。Enter キーを押します。
7. 「`Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`」と入力します。Enter キーを押します。
8. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`」と入力します。Enter キーを押します。
9. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`」と入力します。Enter キーを押します。
10. Microsoft Exchange 2013 以降を使用している場合にのみ、この手順を実行します。「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-MobileDeviceStatistics" -Parameters Mailbox`」と入力します。Enter キーを押します。
11. Microsoft Exchange 2013 以降を使用している場合にのみ、この手順を実行します。「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-MobileDevice" -Parameters Mailbox`」と入力します。Enter キーを押します。
12. 「`Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`」と入力します。Enter キーを押します。
13. 「`New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"`」と入力します。Enter キーを押します。
14. 「`Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`」と入力します。Enter キーを押します。
15. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"`」と入力します。Enter キーを押します。
16. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`」と入力します。Enter キーを押します。
17. Microsoft Exchange 2013 以降を使用している場合にのみ、この手順を実行します。「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`」と入力します。Enter キーを押します。

終了したら： 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可.

承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可

所属組織が Microsoft Exchange Server 2010 以降を使用している場合は、「Microsoft Exchange を設定して承認されているデバイスに対する Exchange ActiveSync へのアクセス許可」を参照してください。

所属組織が Microsoft Office 365 を使用している場合は、「Microsoft Office 365 でのモバイルデバイスアクセスポリシーの設定」を参照してください。

Microsoft Exchange を設定して承認されているデバイスに対する Exchange ActiveSync へのアクセス許可

承認されているデバイスにのみ Microsoft Exchange Server へのアクセスを許可するには、Exchange ActiveSync 2010 以降を設定する必要があります。Microsoft Exchange で許可リストに明示的に追加されていない既存ユーザーのデバイスは、BlackBerry UEM による許可が得られるまで検疫されます。

ホワイトリスト設定できるメールクライアントは、デバイスごとに 1 つだけです。メールアプリケーションのホワイトリストの優先度は次のとおりです。

1. Exchange Server のホワイトリストデータを含むアプリ設定を使用したメールアプリケーション（Android Enterprise または Samsung KNOX Play for Work のみ）
2. BlackBerry Work
3. 加入時に EAS ID が送信されるメールクライアント

このタスクを実行するには、適切な権限を保有する Microsoft Exchange 管理者として、Set-ActiveSyncOrganizationSettings を設定する必要があります。承認されているデバイスにのみ Exchange ActiveSync へのアクセスを許可する方法の詳細については、https://technet.microsoft.com にアクセスし、「*Exchange ActiveSync* のデバイスを有効にする」を参照してください。

作業を始める前に：

- ゲートキーピングのための権限の設定.
- 現在 Microsoft Exchange を使用しているユーザーがいるかどうかを Exchange ActiveSync 管理者に確認してください。
- Exchange ActiveSync に対する組織のデフォルトアクセスレベルが［許可］に設定されていて、かつユーザーがデバイスを正常にセットアップおよび同期している場合は、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーのアカウントまたはデバイスに関連付けられた、個人的例外またはデバイスルールがあることを確認します。持っていない場合、これらのユーザーは検疫され、BlackBerry UEM により許可されるまでデバイスは同期されません。Exchange ActiveSync のデフォルトアクセスレベルを設定して検疫する方法の詳細については、support.blackberry.com/community にアクセスし、記事「36800」を参照してください。

1. Microsoft Exchange Management Shell をホストするコンピューターで、Microsoft Exchange Management Shell を開きます。
2. 「`Set-ActiveSyncOrganizationSettings -DefaultAccessLevel Quarantine`」と入力します。Enter キーを押します。

終了したら： ゲートキーピングのための Microsoft IIS 権限を設定する.

Microsoft Office 365 でのモバイルデバイスアクセスポリシーの設定

Microsoft Office 365 で BlackBerry Gatekeeping Service を使用するには、Microsoft Office 365 でモバイルデバイスアクセスポリシーを設定して、デフォルトでデバイスを検疫する必要があります。

作業を始める前に：

- ゲートキーピングのための権限の設定.
- Exchange ActiveSync に対する組織のデフォルトアクセスレベルが［許可］に設定されていて、かつユーザーがデバイスを正常にセットアップおよび同期している場合は、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーのアカウントまたはデバイスに関連付けられた、個人的例外またはデバイスルールがあることを確認します。関連付けられていないと、これらのユーザーは検疫され、BlackBerry UEM で許可されるまでデバイスは同期されません。Exchange ActiveSync のデフォルトアクセスレベルを設定して検疫する方法の詳細については、support.blackberry.com/community にアクセスし、記事 33531 を参照してください。

1. Microsoft Office 365 管理ポータルにログインします。
2. サイドメニューで、［管理者］をクリックします。
3. ［**Exchange**］をクリックします。
4. ［モバイル］セクションで、［モバイルデバイスアクセス］をクリックします。
5. ［編集］をクリックします。
6. ［検疫 - ブロックまたは許可の判断を後で行う］をクリックします。

終了したら： ゲートキーピングのための Microsoft IIS 権限を設定する.

ゲートキーピングのための Microsoft IIS 権限を設定する

BlackBerry UEM は Windows PowerShell コマンドを使用して、許可されたデバイスのリストを管理します。BlackBerry Gatekeeping Service を使用するには、Microsoft IIS 権限を設定する必要があります。Microsoft クライアントアクセスサーバーロールをホストするコンピューターで、次の操作を実行します。

作業を始める前に： 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可.

1. Microsoft Internet Information Services （IIS）マネージャーを開きます。
2. 左ペインで、サーバーを展開します。
3. ［サイト］ > ［デフォルトの **Web** サイト］を展開します。
4. ［PowerShell］フォルダーを右クリックします。［権限を編集］を選択します。
5. ［セキュリティ］タブをクリックします。［編集］をクリックします。
6. ［追加］をクリックし、ゲートキーピングのための Microsoft Exchange 権限を設定したときに作成された <new_group> を入力します。
7. ［**OK**］をクリックします。
8. ［読み込んで実行］、［フォルダーの内容を一覧表示］、および［読み込み］が選択されていることを確認します。［**OK**］をクリックします。
9. ［**PowerShell**］フォルダーを選択します。認証アイコンをダブルクリックします。
10. ［**Windows** 認証］を選択します。［有効］をクリックします。
11. Microsoft Internet Information Services （IIS）マネージャーを閉じます。

終了したら： ゲートキーピング設定の作成.

ゲートキーピング設定の作成

ゲートキーピング設定を作成し、組織のセキュリティポリシーに準拠するデバイスが Microsoft Exchange Server または Microsoft Office 365 に接続できるようにできます。

作業を始める前に：

- ゲートキーピングのための権限の設定.
- 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可.
- ゲートキーピングのための Microsoft IIS 権限を設定する.

1. 次の操作のいずれかを実行します。
   - オンプレミス環境に BlackBerry UEM がある場合は、メニューバーで、［設定］ > ［外部統合］ > ［**Microsoft Exchange** ゲートキーピング］をクリックします。
   - BlackBerry UEM Cloud がある場合は、BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［一般設定］ > ［**BlackBerry Gatekeeping Service**］をクリックします。
2. Microsoft Exchange Server リストセクションで、＋をクリックします。
3. ［サーバー名］フィールドに、アクセスを管理する Microsoft Exchange Server または Microsoft Office 365 環境の名前を入力します。
4. Exchange ActiveSync ゲートキーピングを管理するために作成したアカウントのユーザー名とパスワードを入力します。
5. ［認証の種類］ドロップダウンリストで、Microsoft Exchange Server または Microsoft Office 365 で使用する認証の種類を選択します。
6. BlackBerry UEM と Microsoft Exchange Server または Microsoft Office 365 の間で SSL 認証を有効にするには、［**SSL** を使用］チェックボックスをオンにします。オプションで、追加の証明書確認を選択します。
7. ［プロキシのタイプ］ドロップダウンリストで、BlackBerry UEM と Microsoft Exchange Server または Microsoft Office 365 の間で使用するプロキシ設定の種類を選択します（存在する場合）。
8. 以前の手順でプロキシ設定を選択した場合は、プロキシサーバーで使用される認証の種類を選択します。
9. 必要に応じて［認証が必須］を選択し、ユーザー名とパスワードを入力します。
10. ［テスト接続］をクリックし、接続が成功していることを確認します。
11. ［保存］をクリックします。
12. ［**Android for Work** メールクライアントリスト］セクションで、＋をクリックします。

メモ： BlackBerry Hub + サービスはデフォルトでリストに追加されます。

13. メールアプリを選択し、［次へ］をクリックします。
14. ［デバイス **ID**］ドロップダウンリストで、デバイス ID にマップするアプリ設定からのフィールドを選択します。
15. ［メールアドレス］ドロップダウンリストで、ユーザーのメールアドレスにマップするアプリ設定からのフィールドを選択します。

終了したら：

- ゲートキーピングプロファイルの作成 を行い、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。
- 1 つまたは複数の BlackBerry Gatekeeping Service のアクティブなインスタンスを持つサーバーグループを設定した場合は、ゲートキーピングプロファイルを適切なサーバーグループに関連付けます。そのゲート

キーピングプロファイルを割り当てられているすべてのユーザーは、そのサーバーグループの BlackBerry Gatekeeping Service の任意のアクティブなインスタンスを使用できます。

ゲートキーピングプロファイルの作成

自動ゲートキーパーを使用する場合は、ゲートキーパープロファイルを作成します。

BlackBerry Gatekeeping Service を設定した場合は、ゲートキーピングプロファイルを作成し、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てる必要があります。ゲートキーピングプロファイルでは、自動ゲートキーピングのために Microsoft Exchange サーバーを選択できます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［メール、カレンダー、連絡先］ > ［ゲートキーピング］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. ［サーバーを選択］をクリックします。
6. 1 つ以上のサーバーを選択し、➡ をクリックします。
7. ［保存］をクリックします。

デバイスに、仕事用メールおよびオーガナイザーデータへのアクセスが許可されていることの確認

組織が BlackBerry Gatekeeping Service を使用して、どのデバイスが Exchange ActiveSync から仕事用メールとオーガナイザーデータにアクセスできるか制御している場合は、少なくとも 1 台のゲートキーピングサーバーがメールプロファイルに設定されています。ゲートキーピングが設定されたメールプロファイルをユーザーアカウントに割り当てると、デバイスと Exchange ActiveSync 間の接続のステータスを確認できます。デバイスの詳細ページの［IT ポリシーおよびプロファイル］セクションでステータスを確認できます。メールプロファイルの横のデバイスの詳細に次のステータスが表示されます。

ステータス	説明
不明	BlackBerry UEM がデバイスの ID を判別できない場合は、［不明］ステータスが表示されます。デバイスは、［制限されたデバイス］リストに一覧表示され、手動で許可リストに追加する必要があります。
接続を保留中	BlackBerry UEM がデバイスの ID を認識しており、デバイスがキュー内で許可リストへの追加を待機中の場合は、［接続を保留中］ステータスが表示されます。
接続が許可されています	BlackBerry UEM がデバイスの ID を認識しており、デバイスが許可リストに入っている場合は、［接続が許可されています］ステータスが表示されます。

Exchange ActiveSync へのアクセスをデバイスが許可されていることの確認

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。

3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. 確認するデバイスのタブを選択します。
5. デバイスが許可されている場合は、［**IT** ポリシーおよびプロファイル］セクションのメールプロファイルの横に、［接続が許可されています］と表示されます。

デバイスによる **Microsoft ActiveSync** へのアクセスの許可

BlackBerry UEM がデバイスから Exchange ActiveSync ID を取得できない場合、デバイスは Microsoft Exchange の許可リストには追加されません。これらのデバイスは、制限された Exchange ActiveSync デバイスリストから許可リストに手動で追加できます。たとえば、Android デバイスが MDM アクティベーションタイプを使用してアクティブ化された場合、BlackBerry UEM は Exchange ActiveSync ID を取得できないため、制限された Exchange ActiveSync デバイスリスト内のデバイスは手動でホワイトリストに移動する必要があります。

1. メニューバーで、［ユーザー］ **>** ［**Exchange** ゲートキーピング］をクリックします。
2. デバイスを検索します。
3. ［アクション］列で、✓ をクリックします。

デバイスによる **Microsoft ActiveSync** へのアクセスのブロック

以前に許可したデバイスが Microsoft ActiveSync にアクセスするのを手動でブロックできます。デバイスをブロックすると、ユーザーは Microsoft Exchange Server からのメールとその他の情報をデバイスで取得できなくなります。

1. メニューバーで［ユーザー］をクリックします。
2. ［**Exchange** ゲートキーピング］をクリックします。
3. デバイスを検索します。
4. ［アクション］列で、⊘ をクリックします。

メールプロファイルの作成

メールプロファイルを使用すると、デバイスが組織のメールサーバーに接続し、Exchange ActiveSync または IBM Notes Traveler を使用してメール、カレンダーエントリ、およびオーガナイザーデータを同期する方法を指定できます。

Exchange ActiveSync を使用する場合は、次の点に注意する必要があります。

- 拡張メールセキュリティの場合は、iOS デバイスおよび Android デバイスの S/MIME を有効にすることができます。PGP デバイスに対して S/MIME または BlackBerry 10 を有効にできます。PGP は、BlackBerry 10 OS バージョン 10.3.1 以降でサポートされています。
- S/MIME を有効にすると、他のプロファイルを使用して、デバイスが自動的に S/MIME 証明書を取得して、証明書のステータスをチェックできるように指定できます。

Notes Traveler を使用する場合は、次の点に注意する必要があります。

- iOS デバイスで Notes Traveler を使用するには、BlackBerry Secure Gateway を有効にする必要があります。
- To Do データの同期は BlackBerry 10 デバイスでのみサポートされています。それは、Notes Traveler サーバーで SyncML 通信プロトコルを使用します。
- BlackBerry 10 デバイスで強化されたメールセキュリティの場合は、IBM Notes 暗号化のみがサポートされます（S/MIME はサポートされません）。
- Notes Traveler クライアントアプリで IBM Verse を使用するには：
  - Samsung Knox デバイスの場合、メールプロファイルで IBM Verse の設定を行います。
  - Android Enterprise デバイスの場合、アプリ設定を使用して IBM Verse の設定を行います。

また IMAP/POP3 メールプロファイルを使用して iOS、macOS、Android、および Windows デバイスが IMAP または POP3 メールサーバーに接続して、メールメッセージを同期する方法を指定できます。Knox MDM を使用するようにアクティベーションを行ったデバイスは、IMAP または POP3 をサポートしません。

メールプロファイルではなく、BlackBerry Work を使用して、ユーザーデバイスのメール、カレンダー、および連絡先を管理できます。BlackBerry Work の管理の詳細については、「BlackBerry Dynamics アプリの管理」および『BlackBerry Work 管理ガイド』を参照してください。

メールプロファイルの作成

必要となるプロファイルの設定は、各デバイスタイプと組織の環境で使用されるメールサーバーに応じて異なります。

作業を始める前に：

- デバイスとメールサーバーの間で証明書ベースの認証を使用する場合、CA 証明書プロファイルを作成して、ユーザーに割り当てる必要があります。また、デバイスに信頼済みクライアント証明書があることを確認してください。
- メールプロファイルを Android デバイスに自動的に適用するには、デバイスが以下の条件のいずれかに適合している必要があります。デバイスがこれらのいずれかの条件に適合していない場合、BlackBerry UEM は引き続きメールプロファイルを Android デバイスに送信しますが、ユーザーは手動でメールサーバーへの接続を設定する必要があります。
  - Android Enterprise デバイス
  - Samsung Knox デバイスおよび Samsung Knox Workspace デバイス

- Motorola デバイス

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［メール、カレンダー、連絡先］ > ［メール］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. 必要に応じて、メールサーバーのドメイン名を入力します。プロファイルが、異なる Microsoft Active Directory ドメインに属する複数のユーザーに対応している場合は、`%UserDomain%` 変数を使用できます。
6. ［メールアドレス］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合は、ユーザーのメールアドレスを入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserEmailAddress%` と入力します。
7. メールサーバーのホスト名または IP アドレスを入力します。
8. ［ユーザー名］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合、ユーザー名を入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserName%` と入力します。
   - プロファイルが IBM Notes Traveler 環境の複数のユーザーに対応している場合は、`%UserDisplayName%` と入力します。
9. BlackBerry Infrastructure への特定の地域接続に BlackBerry Secure Gateway トラフィックを転送するようにサーバーグループを設定した場合、［**BlackBerry Secure Gateway Service** サーバーグループ］ドロップダウンリストで適切なサーバーグループをクリックします。

   BlackBerry Connectivity Node およびサーバーグループの詳細については、「オンプレミス計画関連の資料」、「インストールおよびアップグレード関連の資料」または「UEM Cloud 設定関連の資料」を参照してください。
10. 組織内の各デバイスタイプのタブをクリックして、各プロファイル設定に適切な値を設定します。
11. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

メールプロファイル設定

実際の値を指定するのではなく、値を参照するためにテキストフィールドになっているプロファイル設定では、変数を使用できます。メールプロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- macOS
- Android
- Windows
- BlackBerry 10

共通：メールプロファイル設定

共通：メールプロファイル設定	説明
ドメイン名	この設定では、メールサーバーのドメイン名を指定します。

共通：メールプロファイル設定	説明
メールアドレス	この設定では、ユーザーのメールアドレスを指定します。プロファイルが複数のユーザーに対応している場合は、%UserEmailAddress% 変数を使用できます。
ホスト名または IP アドレス	この設定では、メールサーバーのホスト名または IP アドレスを指定します。
ユーザー名	この設定では、ユーザーのユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を使用できます。
自動ゲートキーピングサーバー	サーバーグループを設定し、BlackBerry Secure Gateway トラフィックまたは BlackBerry Gatekeeping Service トラフィックを、BlackBerry Infrastructure に至る特定の地域接続に転送する場合に、この設定で適切なサーバーグループを指定します。 オンプレミス環境での BlackBerry Connectivity Node およびサーバーグループの詳細については、「計画関連の資料」、「インストールおよびアップグレード関連の資料」を参照してください。クラウド環境での BlackBerry Connectivity Node およびサーバーグループの詳細については、「BlackBerry UEM Cloud 設定関連の資料」を参照してください。

iOS ：メールプロファイル設定

iOS ：メールプロファイル設定	説明
配信の設定	
メッセージの移動を許可する	この設定では、ユーザーがこのアカウントから iOS デバイスに既存の別のメールアカウントにメールを移動できるかどうかを指定します。
最近のアドレスの同期を許可する	この設定では、iOS デバイスユーザーが最近使用したアドレスをデバイス間で同期できるかどうかを指定します。
メール内でのみ使用する	この設定では、iOS デバイス上のメールアプリ以外のアプリが、このアカウントを使用してメールを送信できるかどうかを指定します。
S/MIME を有効にする	この設定では、iOS デバイスユーザーが S/MIME で保護されたメールを送信できるかどうかを指定します。
デジタル署名済み S/MIME メッセージを有効にする	この設定では、デバイスが送信メッセージをデジタル署名付きで送信するかどうかを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。

iOS ：メールプロファイル設定	説明
署名資格情報	この設定では、デバイスがメッセージに署名するために必要な証明書を検索する方法を指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 使用するプロファイルの種類の選択後、共有証明書、SCEP、またはユーザー資格情報プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
署名共有証明書	この設定では、iOS デバイスがメールに署名するために使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
SCEP に署名する	この設定では、デバイスが、S/MIME を使用してメールに署名するために必要な証明書を取得するために使用できる SCEP プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
署名ユーザー資格情報	この設定では、デバイスが、S/MIME を使用してメールに署名するために必要なクライアント証明書を取得するために、ユーザーが使用できる資格情報プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
ユーザーは S/MIME 署名を有効または無効にできます。	この設定では、ユーザーが S/MIME 署名を有効または無効にできるかどうかを指定します。この設定は、iOS 12.0 以降のデバイスにのみ適用されます。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
ユーザーは署名の資格情報を変更できます	この設定では、ユーザーが署名の資格情報を上書きできるかどうかを指定します。この設定は、iOS 12.0 以降のデバイスにのみ適用されます。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。

iOS ：メールプロファイル設定	説明
S/MIME メッセージの暗号化を有効にする	この設定では、デバイスが送信メールを S/MIME 暗号化で暗号化するかどうかを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
暗号化資格情報	この設定では、デバイスがメッセージを暗号化するために必要な証明書を検索する方法を指定します。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 プロファイルの種類の選択後、使用する共有証明書、SCEP、または資格情報プロファイルを選択します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
暗号化共有証明書	この設定では、iOS デバイスがメールを暗号化するために使用するクライアント証明書の共有の証明書プロファイルを指定します。 デバイスは、S/MIME を使用してメッセージを暗号化するために、受信者に適した証明書を選択します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
暗号化 SCEP	この設定では、デバイスが、S/MIME を使用してメールを暗号化するために必要な証明書を取得するために使用できる SCEP プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
暗号化ユーザー資格情報	この設定では、デバイスが、S/MIME を使用してメールを暗号化するために必要なクライアント証明書を取得するために、デバイスが使用できるユーザー資格情報プロファイルを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
ユーザーは S/MIME 暗号化を上書きできます。	この設定では、ユーザーが暗号化設定を有効または無効にできるかどうかを指定します。この設定は、iOS 12.0 以降のデバイスにのみ適用されます。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。

iOS ：メールプロファイル設定	説明
ユーザーは S/MIME 暗号化の資格情報を上書きできます。	この設定では、ユーザーが S/MIME 暗号化の資格情報を上書きできるかどうかを指定します。この設定は、iOS 12.0 以降のデバイスにのみ適用されます。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
メッセージを暗号化	この設定では、ユーザーが送信するときにすべてのメールメッセージを暗号化する必要があるか（［必須］）、または送信する時点で暗号化するメッセージをユーザーが選択できるようにするか（［許可］）を指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効になります。 使用できる値： • 必須 • を許可する デフォルト値は［必須］です。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。
同期日数	この設定では、過去何日まで遡って、メールとオーガナイザーデータを iOS デバイスに同期するかを指定します。 使用できる値： • 1 日 • 3 日 • 7 日 • 14 日 • 1 ヶ月 • 無期限 デフォルト値は［7 日］です。 メモ： この設定は、アクティベーションタイプが iOS の MDM 制御 デバイス上のデフォルトのメールアプリとオーガナイザーアプリにのみ適用されます。
認証	
BlackBerry Secure Gateway を有効化する	この設定では、MDM 制御 アクティベーションタイプの iOS デバイスで、メールサーバーへの接続に BlackBerry Secure Gateway を使用するかどうかを指定します。BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry UEM 経由で、組織のメールサーバーにセキュリティ保護された接続を提供します。 サーバーグループを設定し、BlackBerry Secure Gateway トラフィックを、BlackBerry Infrastructure に至る特定の地域接続に転送する場合、メールプロファイルと適切なサーバーグループを関連付ける必要があります。

iOS ：メールプロファイル設定	説明
認証の種類	この設定では、iOS デバイスがメールサーバーに接続するために使用する認証タイプを指定します。 この設定は、［BlackBerry Secure Gateway を有効化］設定が選択されていない場合のみ有効です。 使用できる値： • None • 共有証明書 • SCEP • ユーザー資格情報 デフォルト値は［なし］です。
共有証明書プロファイル	この設定では、iOS デバイスがメールサーバーに接続するために使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［BlackBerry Secure Gateway を有効化］設定が選択されていない場合で、なおかつ、［認証の種類］設定が［共有証明書］に設定されている場合にのみ有効です。
関連付けられた SCEP プロファイル	この設定では、iOS デバイスがメールサーバー認証に使用するクライアント証明書を登録するために使用する、関連付けられた SCEP プロファイルを指定します。 この設定は、［BlackBerry Secure Gateway を有効化］設定が選択されていない場合で、なおかつ、［認証の種類］設定が［SCEP］に設定されている場合にのみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、iOS デバイスがメールサーバー認証に使用するクライアント証明書を登録するために使用する、関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［BlackBerry Secure Gateway を有効化］設定が選択されていない場合で、なおかつ、［認証の種類］設定が［ユーザー資格情報］に設定されている場合にのみ有効です。
資格情報と証明書を使用する	この設定では、デバイスがメールサーバーで認証するために、関連付けられた SCEP プロファイルを使用して取得した、資格情報とクライアント証明書を使用するかどうかを指定します。 この設定は、［BlackBerry Secure Gateway を有効化］設定が選択されていない場合で、なおかつ、［認証の種類］設定が［SCEP］に設定されている場合にのみ有効です。
認証に OAuth を使用する	この設定は、接続が認証に OAuth を使用するかどうかを指定します。この設定は、iOS 12.1.1 以降のデバイスにのみ適用されます。

iOS ：メールプロファイル設定	説明
SSL を使用	この設定では、デバイスがメールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
すべての SSL 証明書を受け入れる	この設定では、すべての SSL 証明書を受け入れるかどうかを指定します。 この設定は、［SSL を使用］設定が選択されている場合のみ有効です。
外部メールドメイン	
外部メールドメイン許可リスト	この設定では、ユーザーが仕事用メールまたはカレンダーエントリを送信できるドメインのリストを指定します。たとえば、許可されたドメインに含まれるメールアドレスを持つ受信者をユーザーがメールまたはカレンダーエントリに追加した場合、警告メッセージは表示されません。この設定は、仕事用領域のみに適用されます。 複数のドメイン名をリストする場合は、ドメイン名をカンマ（,）、セミコロン（;）、またはスペースで区切ります。
外部メールドメイン制限リスト	この設定では、ユーザーが仕事用メールまたはカレンダーエントリを送信できないドメインのリストを指定します。たとえば、制限されたドメインに含まれるメールアドレスを持つ受信者をユーザーがメールまたはカレンダーの会議出席依頼に追加しようとした場合、Work Connect アプリはユーザーがこのタスクを完了することを禁止します。この設定は、仕事用領域のみに適用されます。 複数のドメイン名をリストする場合は、ドメイン名をカンマ（,）、セミコロン（;）、またはスペースで区切ります。
有効にされたサービス	
メール	この設定では、ユーザーがデバイス上の仕事用メールにアクセスできるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
連絡先	この設定では、ユーザーがデバイス上の仕事用連絡先にアクセスできるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
カレンダー	この設定では、ユーザーがデバイス上の仕事用カレンダーにアクセスできるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
リマインダー	この設定では、ユーザーがデバイス上の仕事用リマインダーにアクセスできるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
Notes	この設定では、ユーザーがデバイス上の仕事用メモにアクセスできるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
アカウントの変更	

iOS ：メールプロファイル設定	説明
メール	この設定では、ユーザーがデバイス上の仕事用メールへのアクセスを有効にするか無効にするかを変更できるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
連絡先	この設定では、ユーザーがデバイス上の仕事用連絡先へのアクセスを有効にするか無効にするかを変更できるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
カレンダー	この設定では、ユーザーがデバイス上の仕事用カレンダーへのアクセスを有効にするか無効にするかを変更できるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
リマインダー	この設定では、ユーザーがデバイス上の仕事用リマインダーへのアクセスを有効にするか無効にするかを変更できるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
Notes	この設定では、ユーザーがデバイス上の仕事用メモへのアクセスを有効にするか無効にするかを変更できるかどうかを指定します。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。

macOS ：メールプロファイル設定

macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。メールプロファイルはユーザーアカウントに適用されます。

macOS ：メールプロファイル設定	説明
パス	この設定では、メールサーバーのネットワークパスを指定します。
ポート	この設定では、メールサーバーに接続するために使用されるポートを指定します。
SSL を使用	この設定では、デバイスがメールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
外部のホスト名または IP アドレス	この設定では、メールサーバーの外部ホスト名または IP アドレスを指定します。
外部の SSL を使用	この設定では、デバイスが外部メールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
外部パス	この設定では、外部メールサーバーのネットワークパスを指定します。
外部サーバーポート	この設定では、外部メールサーバーに接続するために使用されるポートを指定します。

Android ：メールプロファイル設定

メモ： 今後の BlackBerry UEM のリリースでは、BlackBerry Hub + に適用される設定と Divide Productivity はメールプロファイルから削除され、アプリ設定ページのアプリ構成のみで利用可能になります。このリリースで、アプリの設定とアプリの構成を行い、両方が割り当てられる場合、アプリの構成が優先されます。

Android ：メールプロファイル設定	説明
配信の設定	
プロファイルの種類	この設定では、このプロファイルで Exchange ActiveSync または IBM Notes Traveler をサポートするかどうかを指定します。 使用できる値： • Exchange ActiveSync • IBM Notes Traveler デフォルト値は［Exchange ActiveSync ］です。
同期日数	この設定では、MDM 制御 アクティベーションタイプを使用して過去何日まで遡って、メールとオーガナイザーデータを Android デバイスに同期するかを指定します。 使用できる値： • 無制限 • 1 日 • 3 日 • 7 日 • 14 日 • 1 ヶ月 デフォルト値は［1 ヶ月］です。 Samsung Knox MDM を使用する Android デバイスでは、この値を［無制限］に設定した場合、1 ヶ月のみが同期されます。 メモ： この設定は、アクティベーションタイプが Android の MDM 制御 デバイス上のデフォルトのメールアプリとオーガナイザーアプリにのみ適用されます。
認証の種類	この設定では、Android デバイスがメールサーバーに接続するために使用する認証タイプを指定します。 使用できる値： • None • 共有証明書 • SCEP • ユーザー資格情報 デフォルト値は［なし］です。

Android ：メールプロファイル設定	説明
関連付けられた SCEP プロファイル	この設定では、Android デバイスがメールサーバー認証のためのクライアント証明書を取得するために使用する、関連付けられた SCEP プロファイルを指定します。 この設定は、［認証の種類］が［SCEP］に設定されている場合のみ有効です。
資格情報と証明書を使用する	この設定では、デバイスがメールサーバーで認証するために、関連付けられた SCEP プロファイルを使用して取得した、資格情報とクライアント証明書を使用するかどうかを指定します。 この設定は、［認証の種類］が［SCEP］に設定されている場合のみ有効です。
共有証明書プロファイル	この設定では、Android デバイスがメールサーバーに接続するために使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［認証の種類］が［共有証明書］に設定されている場合のみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、Android デバイスがメールサーバーに接続するために使用するクライアント証明書のユーザー資格情報プロファイルを指定します。 この設定は、［認証の種類］が［ユーザー資格情報］に設定されている場合のみ有効です。
SSL を使用	この設定では、デバイスがメールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
すべての SSL 証明書を受け入れる	この設定は、デバイスがメールサーバーからの信頼されない SSL 証明書を自動的に受け入れるかどうかを指定します。この設定が選択されていない場合、デバイスは、信頼済み SSL 証明書を使用するメールサーバーにのみ接続できます。
メールの添付ファイルの最大サイズ	この設定では、メールの添付ファイルの最大サイズを MB 単位で指定します。 使用できる値は 1～365 です。デフォルト設定は 25 です。 この設定は Android Enterprise デバイスにのみ適用されます。
新しいメッセージのデフォルトのメールの署名	この設定では、新しいメールに自動的に付加されるメールの署名を指定します。 この設定は Android Enterprise デバイスにのみ適用されます。
S/MIME を有効にする	この設定では、デバイスから S/MIME で保護されたメールを送信できるかどうかを指定します。 BlackBerry Productivity Suite を使用するデバイスでは、代わりに［S/MIME サポート］設定の値を設定する必要があります。

Android ：メールプロファイル設定	説明
メッセージに署名	この設定では、デバイスがすべての送信メールをデジタル署名付きで送信するかどうかを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。 Android Enterprise デバイスの場合、この設定は、Divide Productivity を使用するデバイスにのみ適用されます。 BlackBerry Productivity Suite を使用するデバイスでは、代わりに［デジタル署名付き S/MIME メッセージ］設定の値を設定する必要があります。
署名資格情報	この設定では、デバイスがメールの署名に使用する資格情報を指定します。 この設定は、［メッセージに署名］設定が選択されている場合のみ有効です。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 デフォルト設定は［共有証明書］です。
署名共有証明書	この設定では、デバイスがメールの署名に使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［署名資格情報］設定が［共有証明書］に設定されている場合のみ有効です。
SCEP に署名する	この設定では、デバイスがメールの署名に使用するクライアント証明書の SCEP プロファイルを指定します。 この設定は、［署名資格情報］設定が［SCEP］に設定されている場合のみ有効です。
署名ユーザー資格情報	この設定では、デバイスがメールの署名に使用するクライアント証明書のユーザー資格情報プロファイルを指定します。 この設定は、［署名資格情報］設定が［ユーザー資格情報］に設定されている場合のみ有効です。

Android ：メールプロファイル設定	説明
メッセージを暗号化	この設定では、デバイスが S/MIME 暗号化を使用して送信メールを暗号化するかどうかを指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。 Android Enterprise デバイスの場合、この設定は、Divide Productivity を使用するデバイスにのみ適用されます。 BlackBerry Productivity Suite を使用するデバイスでは、代わりに［デジタル署名付き S/MIME メッセージ］設定の値を設定する必要があります。
暗号化資格情報	この設定では、デバイスがメールの暗号化に使用する資格情報を指定します。 この設定は、［メッセージを暗号化］設定が選択されている場合のみ有効です。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 デフォルト設定は［共有証明書］です。
暗号化共有証明書	この設定では、デバイスがメールの暗号化に使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［暗号化資格情報］設定が［共有証明書］に設定されている場合のみ有効です。
暗号化 SCEP	この設定では、デバイスがメールの暗号化に使用するクライアント証明書の SCEP プロファイルを指定します。 この設定は、［署名資格情報］設定が［SCEP］に設定されている場合のみ有効です。
暗号化ユーザー資格情報	この設定では、デバイスがメールの暗号化に使用するクライアント証明書のユーザー資格情報プロファイルを指定します。 この設定は、［署名資格情報］設定が［ユーザー資格情報］に設定されている場合のみ有効です。
メールのスマートカード認証を要求する	この設定では、Samsung Knox デバイスがメールサーバーの認証を行うために、スマートカードが必須であるかどうかを指定します。
設定の編集をユーザーに許可する	ユーザーによる配信設定の変更を許可するかどうかを指定します。 この設定は Samsung Knox デバイスにのみ適用されます。
外部メールドメイン	

Android ：メールプロファイル設定	説明
外部メールドメイン許可リスト	この設定では、ユーザーが仕事用メールまたはカレンダーエントリを送信できるドメインのリストを指定します。たとえば、許可されたドメインに含まれるメールアドレスを持つ受信者をユーザーがメールまたはカレンダーエントリに追加した場合、警告メッセージは表示されません。この設定は、仕事用領域のみに適用されます。 複数のドメイン名をリストする場合は、ドメイン名をカンマ（,）、セミコロン（;）、またはスペースで区切ります。
外部メールドメイン制限リスト	この設定では、ユーザーが仕事用メールまたはカレンダーエントリを送信できないドメインのリストを指定します。たとえば、制限されたドメインに含まれるメールアドレスを持つ受信者をユーザーがメールまたはカレンダーの会議出席依頼に追加しようとした場合、メールアプリまたはカレンダーアプリはユーザーがこのタスクを完了することを禁止します。この設定は、仕事用領域のみに適用されます。 複数のドメイン名をリストする場合は、ドメイン名をカンマ（,）、セミコロン（;）、またはスペースで区切ります。
BlackBerry Productivity Suite これらの設定は Android Enterprise デバイスにのみ適用されます。	
OCSP 確認の実行	この設定では、デバイスで OCSP を使用して、S/MIME 証明書のステータスを確認するかどうかを指定します。
信頼されない証明書の承諾をユーザーに許可する	この設定では、ユーザーが、信頼されない証明書の承諾をデバイスに許可できるようにするかどうかを指定します。
テレメトリイベントの仕事用プロファイルからの送信を許可する	この設定では、BlackBerry Productivity Suite で利用データの収集を許可するかどうかを指定します。
セキュリティの種類	この設定では、BlackBerry Productivity Suite が使用するセキュリティタイプを指定します。 使用できる値： • SSL • SSL - すべて信頼 デフォルト値は［SSL］です。

Android ：メールプロファイル設定	説明
仕事用プロファイルと個人用プロファイル間でデータの共有を許可する	この設定では、個人用プロファイルで仕事用プロファイルのデータにアクセスできるようにするかどうかを指定します。 この設定と［個人用アプリによる仕事用データへのアクセスを許可する］設定を選択すると、次の機能が有効になります。 • 仕事用と個人用の両方のアカウントを含む統合 BlackBerry Hub。詳細については、「統合 BlackBerry Hub を有効する」を参照してください。 • 学習した単語を、仕事用と個人用のプロファイルで共有できるようにする統合キーボード辞書。ユーザーは、予測と修正に統合キーボード辞書を使用するかどうかを決定できます。 .
個人用アプリによる仕事用データへのアクセスを制限する	この設定では、個人用アプリで仕事用データにアクセスできるようにするかどうかを指定します。 この設定と［仕事用プロファイルと個人用プロファイル間でデータの共有を許可する］設定を選択すると、次の機能が有効になります。 • 仕事用と個人用の両方のアカウントを含む統合 BlackBerry Hub。詳細については、「統合 BlackBerry Hub を有効する」を参照してください。 • 学習した単語を、仕事用と個人用のプロファイルで共有できるようにする統合キーボード辞書。ユーザーは、予測と修正に統合キーボード辞書を使用するかどうかを決定できます。
S/MIME 設定 これらの設定は Android Enterprise デバイスにのみ適用されます。	
S/MIME サポート	この設定では、BlackBerry Productivity Suite を使用する Android デバイスから S/MIME で保護されたメールを送信できるようにするかどうかを指定します。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。
デジタル署名済み S/MIME メッセージ	この設定では、BlackBerry Productivity Suite を使用する Android デバイスが送信メールをデジタル署名付きで送信するかどうかを指定します。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。

Android ：メールプロファイル設定	説明
暗号化された S/MIME メッセージ	この設定では、BlackBerry Productivity Suite を使用する Android デバイスが送信メールを S/MIME 暗号化を使用して暗号化するかどうかを指定します。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。
S/MIME 暗号化アルゴリズム	この設定では、BlackBerry Productivity Suite を使用する Android デバイスで、S/MIME で保護されたメールの暗号化に使用できる暗号化アルゴリズムを指定します。 使用できる値： • AES（256 ビット） • AES（192 ビット） • AES（128 ビット） • 3DES • ARC2

Windows ：メールプロファイル設定

Windows ：メールプロファイル設定	説明
配信の設定	
プロファイルの種類	この設定では、このプロファイルで Exchange ActiveSync または IBM Notes Traveler をサポートするかどうかを指定します。 使用できる値： • Exchange ActiveSync • IBM Notes Traveler デフォルト値は［Exchange ActiveSync ］です。
アカウント名	この設定では、Windows デバイスに表示される仕事用メールアカウント名を指定します。%UserEmailAddress% などの変数を使用できます。

Windows ：メールプロファイル設定	説明
同期間隔	この設定では、Windows デバイスがメールサーバーから新しいメールをダウンロードする頻度を指定します。 使用できる値： • アイテムの受信時 • 手動 • 15 分 • 30 分 • 60 分 デフォルト値は、［アイテムの受信時］です。
同期日数	この設定では、過去何日まで遡って、メールとオーガナイザーデータを Windows デバイスに同期するかを指定します。 使用できる値： • 無期限 • 3 日 • 7 日 • 14 日 • 1 ヶ月 デフォルト値は［7 日］です。
SSL を使用	この設定では、Windows デバイスがメールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
同期するコンテンツ	
メール	この設定では、Windows デバイスがメールとメールサーバーを同期するかどうかを指定します。
連絡先	この設定では、Windows デバイスが連絡先とメールサーバーを同期するかどうかを指定します。
カレンダー	この設定では、Windows デバイスがカレンダーエントリとメールサーバーを同期するかどうかを指定します。
タスク	この設定では、Windows デバイスがタスクデータとメールサーバーを同期するかどうかを指定します。 この設定は、［プロファイルの種類］が［Exchange ActiveSync ］に設定されている場合のみ有効です。

BlackBerry 10 ：メールプロファイル設定

BlackBerry 10 ：メールプロファイル設定	説明
アカウント名	この設定では、BlackBerry Hub およびデバイス設定に表示される仕事用メールアカウント名を指定します。%UserEmailAddress% などの変数を使用できます。
ポート	この設定では、メールサーバーに接続するために使用されるポートを指定します。
配信の設定	
プロファイルの種類	この設定では、このプロファイルで Exchange ActiveSync または IBM Notes Traveler をサポートするかどうかを指定します。 使用できる値： • Exchange ActiveSync • IBM Notes Traveler デフォルト値は［Exchange ActiveSync ］です。
SyncML サーバー	この設定では、BlackBerry 10 デバイスが To Do データを同期するために使用できる IBM Notes Traveler サーバーの FQDN を指定します。 この設定は、［プロファイルの種類］が［IBM Notes Traveler ］に設定されている場合のみ有効です。
SyncML ポート	この設定では、BlackBerry 10 デバイスが To Do データを同期するために使用できる Notes Traveler サーバーのポートを指定します。 この設定は、［プロファイルの種類］が［IBM Notes Traveler ］に設定されている場合のみ有効です。
SyncML に SSL を使用	この設定では、BlackBerry 10 デバイスが Notes Traveler サーバーへの SSL 接続を確立する必要があるかどうかを指定します。 この設定は、［プロファイルの種類］が［IBM Notes Traveler ］に設定されている場合のみ有効です。
プッシュ有効化	この設定では、メールサーバーがメールを BlackBerry 10 デバイスにプッシュできるかどうかを指定します。

BlackBerry 10 ：メールプロファイル設定	説明
同期間隔	この設定では、BlackBerry 10 デバイスがメールサーバーで新しいメールを確認する頻度を指定します。 この設定は、［プッシュ有効化］設定が選択されていない場合のみ有効です。 使用できる値： • 手動 • 5 分 • 15 分 • 30 分 • 1 時間 • 2 時間 • 4 時間 • 24 時間 デフォルト値は［15 分］です。
同期日数	この設定では、過去何日まで遡って、メールとオーガナイザーデータを BlackBerry 10 デバイスに同期するかを指定します。 使用できる値： • 1 日 • 3 日 • 7 日 • 14 日 • 1 ヶ月 • 無期限 デフォルト値は［1 ヶ月］です。
ローミング時に手動同期が必要	この設定では、ローミング時に、BlackBerry 10 デバイスとメールサーバーの同期をユーザーが開始する必要があるかどうかを指定します。
SSL を使用	この設定では、デバイスがメールサーバーに接続するために SSL を使用する必要があるかどうかを指定します。
カレンダー同期	この設定では、BlackBerry 10 デバイスがカレンダーエントリとメールサーバーを同期するかどうかを指定します。
連絡先同期	この設定では、BlackBerry 10 デバイスが連絡先とメールサーバーを同期するかどうかを指定します。
メール同期	この設定では、BlackBerry 10 デバイスがメールとメールサーバーを同期するかどうかを指定します。

BlackBerry 10 ：メールプロファイル設定	説明
メモの同期	この設定では、BlackBerry 10 デバイスがメモデータとメールサーバーを同期するかどうかを指定します。 この設定は、［プロファイルの種類］が［Exchange ActiveSync ］に設定されている場合のみ有効です。
タスクの同期	この設定では、BlackBerry 10 デバイスがタスクデータとメールサーバーを同期するかどうかを指定します。 この設定は、［プロファイルの種類］が［Exchange ActiveSync ］に設定されている場合のみ有効です。
ToDo の同期	この設定では、BlackBerry 10 デバイスが Notes Traveler を使用して To Do データを同期するかどうかを指定します。 この設定は、［プロファイルの種類］が［IBM Notes Traveler ］に設定されている場合のみ有効です。
セキュリティ保護されたメールの設定	
送信メッセージのデフォルトエンコーディングの候補を表示する	この設定では、BlackBerry 10 デバイスがすべての送信メールに対してデフォルトエンコーディングの候補を表示するかどうかを指定します（たとえば、プレーンテキスト、署名、暗号化、または署名と暗号化）。これが［許可］に設定されている場合は、デバイスがデフォルトエンコーディングの候補を表示するか、またはメッセージ履歴に基づいたエンコーディングを候補として表示するかどうかをユーザーが選択できます。これを［必須］に設定すると、デバイスはデフォルトエンコーディングの候補を表示します。これを［許可しない］に設定すると、デバイスはメッセージ履歴に基づいたエンコーディングを候補として表示します。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
S/MIME 設定	

BlackBerry 10 ：メールプロファイル設定	説明
S/MIME サポート	この設定では、S/MIME を BlackBerry 10 デバイスで有効にするかどうかを指定します。これが［許可］に設定されている場合、デバイスの S/MIME 保護を有効にするかどうかをユーザーが選択できます。これが［必須］に設定されている場合、デバイスの S/MIME 保護は有効になり、ユーザーはそれを無効にできません。これが［許可しない］に設定されている場合、デバイスの S/MIME 保護は無効になり、ユーザーはそれを有効にできません。 暗号化されたメールを送信するには、デバイスまたはスマートカードに受信者の公開鍵が存在している必要があります。デジタル署名されたメールを送信するには、デバイスまたはスマートカードにユーザーの秘密鍵が存在している必要があります。 この設定は、［デジタル署名済み S/MIME メッセージ］および［暗号化された S/MIME メッセージ］の設定より優先されます。 この設定は、［PGP サポート］の設定に影響します。これが［必須］に設定されている場合は、［PGP サポート］を［許可しない］に設定する必要があります。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。
デジタル署名済み S/MIME メッセージ	この設定では、BlackBerry 10 デバイスが送信メールをデジタル署名付きで送信するかどうかを指定します。これが［許可］に設定されている場合、送信メールにデジタル署名するかどうかは、ユーザーが選択できます。これが［必須］に設定されている場合、ユーザーは送信メールにデジタル署名する必要があります。これが［許可しない］に設定されている場合、ユーザーは送信メールにデジタル署名できません。 デジタル署名されたメールを送信するには、デバイスまたはスマートカードにユーザーの秘密鍵が存在している必要があります。 この設定は、［S/MIME サポート］が［許可］または［必須］に設定されている場合のみ有効です。 ［S/MIME サポート］が［必須］に設定されており、この設定と［暗号化された S/MIME メッセージ］の両方が［許可しない］に設定されている場合、［暗号化された S/MIME メッセージ］とこの設定の値は無視され、どちらもデフォルト設定の［許可］が使用されます。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。

BlackBerry 10 ：メールプロファイル設定	説明
暗号化された S/MIME メッセージ	この設定では、BlackBerry 10 デバイスが送信メールを S/MIME 暗号化を使用して暗号化するかどうかを指定します。これが［許可］に設定されている場合、送信メールを暗号化するかどうかは、ユーザーが選択できます。これが［必須］に設定されている場合、ユーザーは送信メールを暗号化する必要があります。これが［許可しない］に設定されている場合、ユーザーは送信メールを暗号化できません。 暗号化されたメールを送信するには、デバイスまたはスマートカードに受信者の公開鍵が存在している必要があります。 この設定は、［S/MIME サポート］が［許可］または［必須］に設定されている場合のみ有効です。 ［S/MIME サポート］が［必須］に設定されており、この設定と［デジタル署名済み S/MIME メッセージ］の両方が［許可しない］に設定されている場合、［デジタル署名済み S/MIME メッセージ］とこの設定の値は無視され、どちらもデフォルト設定の［許可］が使用されます。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。
暗号化アルゴリズム	この設定では、BlackBerry 10 デバイスで S/MIME で保護されたメールの暗号化に使用できる暗号化アルゴリズムを指定します。 使用できる値： • AES（256 ビット） • AES（192 ビット） • AES（128 ビット） • 3DES • RC2 デフォルト値は NULL 値です。
PGP 設定	

BlackBerry 10 ：メールプロファイル設定	説明
PGP サポート	この設定では、PGP 保護を BlackBerry 10 デバイスで有効にするかどうかを指定します。これが［許可］に設定されている場合、デバイスの PGP 保護を有効にするかどうかをユーザーが選択できます。これが［必須］に設定されている場合、デバイスの PGP 保護は有効になり、ユーザーはそれを無効にできません。これが［許可しない］に設定されている場合、デバイスの PGP 保護は無効になり、ユーザーはそれを有効にできません。 暗号化されたメールを送信するには、デバイスに受信者の公開鍵が存在している必要があります。デジタル署名されたメールを送信するには、デバイスユーザーの秘密鍵が存在している必要があります。 ［S/MIME サポート］の値がこの設定に影響します。［S/MIME サポート］が［必須］に設定されているか、または［S/MIME サポート］が［許可］に設定されており、［デジタル署名済み S/MIME メッセージ］または［暗号化された S/MIME メッセージ］が［必須］に設定されている場合、この設定は［許可しない］にする必要があります。 使用できる値： • を許可する • 必須 • 許可しない デフォルト値は［許可］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
Symantec Encryption Management Server アドレス	この設定では、BlackBerry 10 デバイスユーザーがこのサーバーにデバイスを登録して PGP メッセージを送信するために必要となる、組織の Symantec Encryption Management Server の FQDN または IP アドレスを指定します。 ［PGP サポート］の値がこの設定に影響します。［PGP サポート］が［許可］または［必須］に設定されている場合に、デバイスはこの設定を使用できます。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。

BlackBerry 10 ：メールプロファイル設定	説明
Symantec Encryption Management Server 登録方法	この設定では、BlackBerry 10 デバイスユーザーがデバイスを組織の Symantec Encryption Management Server に登録するために使用する必要のある方法を指定します。これが［メール認証］に設定されている場合、デバイスはユーザーにメールアドレスの入力を要求します。これが［Microsoft Active Directory 認証］に設定されている場合、デバイスはユーザーにドメインユーザー名とパスワードの入力を要求します。 ［PGP サポート］の値がこの設定に影響します。［PGP サポート］が［許可］または［必須］に設定されている場合に、デバイスはこの設定を使用できます。 使用できる値： • メール認証 • Microsoft Active Directory 認証 デフォルト値は［メール認証］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
関連付けられたプロファイル	
認証の種類	この設定では、BlackBerry 10 デバイスがメールサーバーに接続するために使用する認証タイプを指定します。 使用できる値： • None • SCEP • ユーザー資格情報 デフォルト値は［なし］です。
関連付けられた SCEP プロファイル	この設定では、BlackBerry 10 デバイスがメールサーバー認証に使用するクライアント証明書を登録するために使用する、関連付けられた SCEP プロファイルを指定します。 この設定は、［認証の種類］が［SCEP］に設定されている場合のみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、BlackBerry 10 デバイスがメールサーバー認証に使用するクライアント証明書を取得するために使用する、関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［認証の種類］が［ユーザー資格情報］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
メッセージの分類	
メッセージ分類ファイル（.json）	この設定では、ユーザーのデバイスに送信するメッセージの分類を指定します。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。

S/MIME プロファイルとデバイス設定の依存関係

次の表は、管理者が BlackBerry UEM で設定できる S/MIME 設定と、ユーザーが BlackBerry 10 デバイスで設定できる S/MIME 設定との依存関係を示しています。これらが何に設定されているかに応じて、デバイスの［エンコーディング］ドロップダウンリスト内のオプションが変わります。デバイスは、優先度の高い設定（たとえば、［S/MIME サポート］設定）が一部の設定の値と競合する場合は、その設定の値を無視します。

［**S/MIME** サポート］設定	［デジタル署名済み **S/MIME** メッセージ］設定	［暗号化された **S/MIME** メッセージ］設定	デバイスの **S/MIME** 設定	デバイスの［エンコーディング］ドロップダウン
許可する	許可する	許可する	ユーザーは S/MIME 保護の有効/無効を切り替えることができます。	プレーンテキスト 署名（S/MIME） 暗号化（S/MIME） 署名および暗号化（S/MIME）
	許可する	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	暗号化（S/MIME） 署名および暗号化（S/MIME）
	許可する	許可しない	ユーザーは S/MIME 保護の有効/無効を切り替えることができます。	プレーンテキスト 署名（S/MIME）
	必須	許可する	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME） 署名および暗号化（S/MIME）
	必須	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名および暗号化（S/MIME）
	必須	許可しない	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME）
	許可しない	許可する	ユーザーは S/MIME 保護の有効/無効を切り替えることができます。	プレーンテキスト 暗号化（S/MIME）
	許可しない	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	暗号化（S/MIME）

［**S/MIME** サポート］設定	［デジタル署名済み **S/MIME** メッセージ］設定	［暗号化された **S/MIME** メッセージ］設定	デバイスの **S/MIME** 設定	デバイスの［エンコーディング］ドロップダウン
	許可しない	許可しない	ユーザーは S/MIME 保護の有効/無効を切り替えることができますが、必要なプロファイルが［許可しない］に設定されているため、メッセージに対して暗号化または署名できません。	プレーンテキスト
必須	許可する	許可する	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME） 暗号化（S/MIME） 署名および暗号化（S/MIME）
	許可する	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	暗号化（S/MIME） 署名および暗号化（S/MIME）
	許可する	許可しない	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME）
	必須	許可する	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME） 署名および暗号化（S/MIME）
	必須	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名および暗号化（S/MIME）
	必須	許可しない	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME）
	許可しない	許可する	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	暗号化（S/MIME）
	許可しない	必須	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	暗号化（S/MIME）

［**S/MIME** サポート］設定	［デジタル署名済み **S/MIME** メッセージ］設定	［暗号化された **S/MIME** メッセージ］設定	デバイスの **S/MIME** 設定	デバイスの［エンコーディング］ドロップダウン
	許可しない （この設定は無視されます）	許可しない （この設定は無視されます）	S/MIME 保護は有効です。ユーザーが無効にすることはできません。	署名（S/MIME） 暗号化（S/MIME） 署名および暗号化（S/MIME）
許可しない	すべての設定が無視されます	すべての設定が無視されます	S/MIME 保護は無効です。ユーザーが有効にすることはできません。	プレーンテキスト

PGP プロファイルとデバイス設定の依存関係

次の表は、管理者が BlackBerry UEM で設定できる［PGP サポート］設定と、ユーザーが BlackBerry 10 デバイスで設定できる PGP 設定との依存関係を示しています。［PGP サポート］設定が何に設定されているかに応じて、デバイスの［エンコーディング］ドロップダウンリスト内のオプションが変わります。デバイスは、優先度の高い設定（たとえば、［S/MIME サポート］設定）がこの設定の値と競合する場合は、この設定の値を無視します。

［**PGP** サポート］設定	デバイスの **PGP** 設定	デバイスの［エンコーディング］ドロップダウン
を許可する	ユーザーは PGP 保護の有効/無効を切り替えることができます。	• プレーンテキスト • 署名（PGP） • 暗号化（PGP） • 署名および暗号化（PGP）
必須	PGP 保護は有効です。ユーザーが無効にすることはできません。	• 署名（PGP） • 暗号化（PGP） • 署名および暗号化（PGP）
許可しない	PGP 保護は無効です。ユーザーが有効にすることはできません。	ドロップダウンなし。プレーンテキストが使用されます。

BlackBerry Secure Gateway によるメールデータの保護

BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry UEM を介して、MDM 制御 でアクティベーションされた iOS デバイスに対し、組織のメールサーバーへのセキュリティ保護された接続を提供します。

BlackBerry Secure Gateway を有効にすると、MDM 制御 でアクティベーションされたデバイスは、メールサーバーをファイアウォールの外部に公開したり、DMZ 内のメールサーバーを検索したりすることなく、仕事用メールを送受信できるようになります。

BlackBerry Secure Gateway を使用する場合は、組織に適切なライセンスがあることを確認する必要があります。詳細については、ライセンス関連の資料を参照してください。

BlackBerry Secure Gateway を有効にするには、メールプロファイルで［BlackBerry Secure Gateway を有効にする］設定を選択します。

BlackBerry Infrastructure への地域接続をサポートするようにサーバーグループを設定した場合、メールプロファイルと適切なサーバーグループを関連付けることで、特定の地域接続に BlackBerry Secure Gateway トラフィックを転送できます。

BlackBerry Secure Gateway を有効にする場合の Exchange ActiveSync への TLS/SSL 接続の設定

BlackBerry Secure Gateway を有効にして、BlackBerry UEM を介した、組織のメールサーバーと MDM 制御 アクティベーションタイプの iOS デバイスの間のセキュリティで保護された接続を提供する場合は、BlackBerry UEM を設定して、Exchange ActiveSync への TLS/SSL 接続を作成する必要がある場合があります。

Exchange ActiveSync サーバーが TLS 接続を必要とするように構成されている場合、Exchange ActiveSync サーバー証明書（またはそのルート証明書）を BlackBerry UEM に追加する必要があります。BlackBerry Secure Gateway は、TLS/SSL 接続を確立するときに、Exchange ActiveSync サーバーを信頼するための証明書を必要とします。

Exchange ActiveSync サーバーのセキュリティ要件に応じて、BlackBerry Secure Gateway が Exchange ActiveSync との認証に使用できる TLS バージョンと暗号のリストを更新する必要があります。

Exchange ActiveSync サーバー証明書を信頼するように BlackBerry UEM を設定する

作業を始める前に： Exchange ActiveSync サーバーから X.509 形式（*.cer、*.der）で証明書をエクスポートし、管理コンソールからアクセスできるネットワークの場所に保存します。

1. メニューバーで、［設定］ > ［外部統合］ > ［信頼済み証明書］をクリックします。
2. ［**Exchange ActiveSync** サーバー信頼］の横にある＋をクリックします。
3. ［参照］をクリックします。
4. 使用する証明書ファイルを選択します。

5. ［開く］をクリックします。
6. 証明書の説明を入力します。
7. ［追加］をクリックします。

Exchange ActiveSync がサポートする TLS バージョンと暗号を使用するように BlackBerry UEM を設定します。

1. メニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Secure Gateway**］をクリックします。
2. 変更するテーブルの＋をクリックします。
3. ［選択］リストで追加または削除する TLS バージョンまたは暗号をクリックします。
4. 矢印をクリックして、目的のリストに項目を移動します。
5. ［割り当て］をクリックします。

S/MIME を使用したメールセキュリティの強化

S/MIME を有効にすることで、BlackBerry 10、iOS、および Android デバイスユーザーのメールセキュリティを強化できます。S/MIME は、メールを暗号化し署名する標準的な方法を提供します。ユーザーは、デバイス上の S/MIME で保護されたメッセージをサポートする仕事用メールアカウントを使用している場合に、S/MIME 保護を使用して、メールの暗号化、署名、暗号化、または暗号化と署名の両方を実行できます。S/MIME は、個人用メールアドレスに対しては有効化できません。

ユーザーは、受信者の S/MIME 証明書をデバイスに保存できます。ユーザーは自身の秘密鍵をデバイスまたはスマートカードに保存できます。

ユーザー向けの S/MIME はメールプロファイルで有効にします。BlackBerry 10 デバイスユーザーには S/MIME の使用を強制できますが、iOS または Android デバイスユーザーには強制できません。S/MIME の使用がオプションの場合、ユーザーはデバイスで S/MIME を有効にし、メールの暗号化、署名、または暗号化と署名の両方のいずれを使用するかを指定できます。

S/MIME 設定は、PGP 設定より優先されます。S/MIME のサポートが［必須］に設定されている場合、PGP 設定は無視されます。

S/MIME 証明書の取得

証明書の取得プロファイルを使用して、BlackBerry 10 デバイスに対し、LDAP 証明書サーバーでの受信者 S/MIME 証明書の検索および取得を許可できます。必要な S/MIME 証明書がデバイスの証明書ストアにまだない場合は、デバイスは自動的にサーバーからそれを取得し、証明書ストアにインポートします。

BlackBerry 10 デバイスは、プロファイルに指定された各 LDAP 証明書サーバーを検索し、S/MIME 証明書を取得します。複数の S/MIME 証明書があり、デバイスが優先される証明書を判別できない場合は、ユーザーが使用する証明書を選択できるように、すべての S/MIME 証明書が表示されます。

管理者はデバイスに対し、単純な認証または Kerberos 認証のどちらかを使用して LDAP 証明書サーバーで認証を実行するよう要求できます。デバイスが単純な認証を使用するように要求する場合は、デバイスが自動的に LDAP 証明書サーバーでの認証を実行できるように、必要な認証資格情報を証明書の取得プロファイルに含めることができます。デバイスに対し Kerberos 認証の使用を要求する場合は、バージョン 10.3.1 以降の BlackBerry 10 OS を実行しているデバイスが LDAP 証明書サーバーで自動的に認証できるように、必要な認証資格情報を証明書取得プロファイルに含めることができます。それ以外の場合は、デバイスが LDAP 証明書サーバーでの認証を初めて試行する際に、ユーザーが必要な認証資格情報を入力するように求められます。バージョン 10.2.1～10.3 の BlackBerry 10 OS を実行しているデバイスでは、LDAP 証明書サーバーでの認証を初めて試行する際に、必要な認証資格情報を入力するように求められます。

S/MIME 証明書の取得のために Kerberos 認証を実装する場合は、該当するユーザーまたはユーザーグループにシングルサインオンプロファイルを割り当てる必要があります。シングルサインオンプロファイルの作成と割り当ての詳細については、「デバイスのシングルサインオン認証を設定」を参照してください。

管理者が証明書の取得プロファイルを作成して、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てない場合は、ユーザーが手動で仕事用メールの添付ファイルまたはコンピューターから S/MIME 証明書をインポートする必要があります。

証明書の取得プロファイルの作成

作業を始める前に：

- デバイスがセキュリティ保護された接続を確立する際に LDAP 証明書サーバーを信頼できるようにするために、CA 証明書をデバイスに配布しなければならない場合があります。必要に応じて、CA 証明書プロファイルを作成し、それらをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。CA 証明書の詳細については、「デバイスおよびアプリへの CA 証明書の送信」を参照してください。
- S/MIME 証明書の取得のために Kerberos 認証を実装する場合は、該当するユーザーまたはユーザーグループにシングルサインオンプロファイルを割り当てる必要があります。シングルサインオンプロファイルの詳細については、「デバイスでシングルサインオン認証を設定」を参照してください。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［証明書］ > ［証明書の取得］をクリックします。
3. ＋ をクリックします。
4. 証明書の取得プロファイルの名前と説明を入力します。
5. 表で、＋ をクリックします。
6. ［サービス **URL**］フィールドに、ldap://<*FQDN*>:<ポート> 形式を使用して、LDAP 証明書サーバーの FQDN を入力します。（ldap://server01.example.com:389 など）。
7. ［検索ベース］フィールドに、LDAP 証明書サーバー検索の起点となるベース DN を入力します。
8. ［検索範囲］ドロップダウンリストで、次の操作のいずれかを実行します。
   - ベースオブジェクトのみ（ベース DN）を検索するには、［ベース］をクリックします。このオプションは、デフォルト値です。
   - ベースオブジェクトの 1 レベル下を検索するが、ベースオブジェクト自体は検索しない場合は、［**1** レベル］をクリックします。
   - ベースオブジェクトとその下のすべてのレベルを検索するには、［サブツリー］をクリックします。
   - ベースオブジェクトの下のすべてのレベルを検索するが、ベースオブジェクト自体は検索しない場合は、［子］をクリックします。
9. 認証が必要な場合は、次の操作を実行します。
   a) ［認証の種類］ドロップダウンリストで、［単純］または［**Kerberos**］をクリックします。
   b) ［**LDAP** ユーザー **ID**］フィールドに、LDAP 証明書サーバーの検索権限を持つアカウントの DN を入力します（cn=admin、dc=example、dc=com など）。
   c) ［**LDAP** パスワード］フィールドに、LDAP 証明書サーバーの検索権限を持つアカウントのパスワードを入力します。
10. 必要に応じて、［セキュリティ保護された接続を使用する］チェックボックスをオンにします。
11. ［接続のタイムアウト］フィールドに、デバイスが LDAP 証明書サーバーの応答を待機する時間（秒単位）を入力します。
12. ［追加］をクリックします。
13. LDAP 証明書サーバーごとに手順 5〜11 を繰り返します。
14. ［追加］をクリックします。

終了したら：

- BlackBerry 10 デバイスが証明書ステータスをチェックできるようにするには、OCSP または CRL プロファイルを作成します。
- 必要に応じて、プロファイルをランク付けします。

デバイスでの S/MIME 証明書のステータスの判別

OCSP プロファイルおよび CRL プロファイルを使用して、BlackBerry 10 デバイスに S/MIME 証明書のステータスの確認を許可できます。OCSP プロファイルと CRL プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

BlackBerry 10 デバイスは、OCSP プロファイルに指定された各 OCSP レスポンダーを検索し、S/MIME 証明書のステータスを取得します。10.3.1 より後のバージョンの BlackBerry 10 OS を実行するデバイスは、証明書ステータス要求を BlackBerry UEM に送信できます。管理者は CRL プロファイルで、BlackBerry UEM が HTTP、HTTPS、または LDAP を使用して S/MIME 証明書のステータスを検索するように設定できます。

証明書の取得に Exchange ActiveSync を使用する場合、iOS および Android デバイスは Exchange ActiveSync を使用して、S/MIME 証明書のステータスをチェックします。証明書の取得に LDAP を使用する場合、iOS および Android デバイスは OCSP を使用して、証明書のステータスをチェックします。iOS および Android デバイスは、OCSP プロファイルを使用しません。デバイスは証明書内の OCSP レスポンダーをチェックします。

証明書ステータス表示の詳細については、デバイスのユーザーガイドのセキュリティ保護されたメールアイコンに関する説明を参照してください。

OCSP プロファイルの作成

OCSP プロファイルは BlackBerry 10 デバイスでサポートされます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［証明書］ > ［**OCSP**］をクリックします。
3. ＋ をクリックします。
4. OCSP プロファイルの名前と説明を入力します。
5. 次の操作を実行します。
   a) 表で、＋ をクリックします。
   b) ［サービス **URL**］フィールドに、OCSP レスポンダーの Web アドレスを入力します。
   c) ［接続タイムアウト］フィールドに、デバイスが OCSP の応答を待機する時間（秒単位）を入力します。
   d) ［追加］をクリックします。
6. OCSP レスポンダーごとに手順 4 を繰り返します。
7. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

CRL プロファイルの作成

CRL プロファイルは、BlackBerry 10 デバイスおよび Android を搭載した BlackBerry デバイスでサポートされています。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［証明書］ > ［**CRL**］をクリックします。
3. ＋ をクリックします。
4. CRL プロファイルの名前と説明を入力します。
5. デバイスに証明書に定義されたレスポンダー URL の使用を許可するには、［証明書拡張レスポンダーを使用する］チェックボックスをオンにします。
6. 次のタスクを実行します。

タスク	手順
HTTP CRL 設定を指定する	**a.** ［**HTTP for CRL**］セクションで ＋ をクリックします。 **b.** HTTP CRL 設定の名前と説明を入力します。 **c.** ［サービス **URL**］フィールドに、HTTP サーバーまたは HTTPS サーバーの Web アドレスを入力します。 **d.** ［追加］をクリックします。 **e.** HTTP サーバーまたは HTTPS サーバーごとに手順 1～4 を繰り返します。
LDAP CRL 設定を指定する	**a.** ［**LDAP for CRL**］セクションで ＋ をクリックします。 **b.** LDAP CRL 設定の名前と説明を入力します。 **c.** ［サービス **URL**］フィールドに、ldap://<*FQDN*>:<ポート> 形式を使用して、LDAP サーバーの FQDN を入力します（たとえば、ldap://server01.example.com:389）。セキュリティ保護された接続の場合は、ldaps://<*FQDN*>:<ポート> 形式を使用します。 **d.** ［検索ベース］フィールドに、LDAP サーバー検索の起点となるベース DN を入力します。 **e.** 必要に応じて、［セキュリティ保護された接続を使用する］チェックボックスをオンにします。 **f.** ［**LDAP** ユーザー **ID**］フィールドに、LDAP サーバーの検索権限を持つアカウントの DN を入力します（たとえば、cn=admin、dc=example、dc=com）。 **g.** ［**LDAP** パスワード］フィールドに、LDAP サーバーの検索権限を持つアカウントのパスワードを入力します。 **h.** ［追加］をクリックします。 **i.** LDAP サーバーごとに手順 1～8 を繰り返します。

7. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

PGP を使用したメールセキュリティの強化

BlackBerry 10 OS のバージョン 10.3.1 以降を実行しているデバイスでは、PGP を有効にすることで、デバイスユーザーのメールセキュリティを強化できます。PGP は、OpenPGP 形式を使用してデバイスのメールを保護します。ユーザーは、仕事用メールアドレスの使用時に、PGP 保護を使用して署名、暗号化、または署名と暗号化の両方でメールを保護できます。PGP は、個人用メールアドレスに対しては有効化できません。

ユーザー向けの PGP はメールプロファイルで有効にします。BlackBerry 10 デバイスユーザーに PGP の使用を強制することもできれば、PGP の使用を許可しないことも、またはそれをオプションにすることもできます。PGP の使用がオプションの場合（デフォルト設定）、ユーザーはデバイスで PGP を有効にし、メールで暗号化、署名、または暗号化と署名の両方のいずれを使用するかを指定できます。

メールに署名して暗号化するには、受信者ごとの PGP キーをデバイスに保存しておく必要があります。ユーザーは、仕事用メールからファイルをインポートすることで PGP キーを保存できます。

適切なメールプロファイル設定を使用して PGP を設定できます。

メッセージ分類を使用したセキュリティ保護されたメールの強制

メッセージを分類すると、BlackBerry 10 デバイスのメールを対象に、セキュリティ保護メールポリシーを指定して適用し、メールに視覚的なマークを追加できます。BlackBerry UEM を使用して、BlackBerry 10 デバイスのユーザーに、コンピューターのメールアプリケーションと同様のメッセージ分類オプションを提供できます。メッセージの分類に基づいて、送信メッセージに適用する次のルールを定義できます。

- メッセージの分類を示すラベルを追加する（「機密情報」など）
- 件名の末尾に視覚的なマーカーを追加する（[C] など）
- メール本文の先頭または末尾にテキストを追加する（「このメッセージは機密情報として分類されました」など）
- S/MIME または PGP のオプションを設定する（署名や暗号化など）
- デフォルトの分類を設定する

BlackBerry 10 OS バージョン 10.3.1 以降を実行するデバイスでは、メッセージの分類を使用して、ユーザーにメールの署名、暗号化、またはその両方を求めたり、ユーザーがデバイスから送信するメールに視覚的なマークを追加したりできます。ユーザーのデバイスに送信するメッセージ分類設定ファイル（拡張子 .json）の指定には、メールプロファイルを使用します。ユーザーがメッセージ分類の設定されているメールに返信、またはセキュリティで保護されたメールを作成すると、メッセージ分類の設定に基づいて、デバイスにより送信メッセージに強制される分類ルールが決められます。

デバイスのメッセージ保護オプションは、デバイスで許可されている種類の暗号化およびデジタル署名に制限されます。ユーザーがデバイス上のメールにメッセージ分類を適用する場合は、メッセージ分類により許可されている 1 つの種類のメッセージ保護を選択するか、またはデフォルトのメッセージ保護を承諾する必要があります。ユーザーが、署名、暗号化、またはその両方を要求するメッセージ分類を選択したが、デバイスで S/MIME または PGP が設定されていない場合、そのユーザーはメールを送信できません。

S/MIME および PGP 設定は、メッセージ分類より優先されます。ユーザーは、各自のデバイスでメッセージの分類を上げることはできても、下げることはできません。メッセージ分類レベルは、各分類のセキュリティ保護メールのルールで決まります。

メッセージ分類が有効化されている場合、ユーザーはデバイスからメールを送信するときに BlackBerry Assistant を使用できません。

適切なメールプロファイル設定を使用して、メッセージ分類を設定できます。

メッセージ分類設定ファイルの作成方法の詳細については、support.blackberry.com/community にアクセスして、記事 36736 を参照してください。

IMAP/POP3 メールプロファイルを作成

IMAP/POP3 メールプロファイルは、iOS、macOS、Android、および Windows デバイスが IMAP または POP3 メールサーバーに接続して、メールメッセージを同期する方法を指定するために使用します。

必要となるプロファイルの設定は、各デバイスタイプと選択する設定に応じて異なります。

メモ： BlackBerry UEM はメールプロファイルを Android デバイスに送信しますが、ユーザーは手動でメールサーバーへの接続を設定する必要があります。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［メール、カレンダー、および連絡先］ > ［**IMAP/POP3** メール］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. ［メールの種類］フィールドで、メールプロトコルの種類を選択します。
6. ［メールアドレス］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合は、ユーザーのメールアドレスを入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserEmailAddress%` と入力します。
7. ［受信メール設定］セクションには、受信メール用メールサーバーのホスト名または IP アドレスを入力します。
8. 必要に応じて、受信メールのポートを入力します。
9. ［ユーザー名］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合、ユーザー名を入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserName%` と入力します。
10. ［送信メール設定］セクションには、送信メール用メールサーバーのホスト名または IP アドレスを入力します。
11. 必要に応じて、送信メールのポートを入力します。
12. 必要に応じて、［送信メールに必要な認証］を選択し、送信メールに使用する資格情報を指定します。
13. 組織内の各デバイスタイプのタブをクリックして、各プロファイル設定に適切な値を設定します。
14. ［追加］をクリックします。

IMAP/POP3 メールプロファイルの設定

実際の値を指定するのではなく、値を参照するためにテキストフィールドになっているプロファイル設定では、変数を使用できます。BlackBerry UEM は、事前定義されたデフォルトの変数と定義されたカスタム変数をサポートしています。IMAP/POP3 メールプロファイルは、次の種類のデバイスでサポートされています。

- iOS
- macOS
- Android
- Windows

ときには、設定をサポートするためのデバイス OS の必要最小バージョンが、BlackBerry UEM によってサポートされていないバージョンである場合があります。サポートされるバージョンの詳細については、「互換性一覧表」を参照してください。

iOSおよび macOS：IMAP/POP3 メールプロファイルの設定

macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。IMAP/POP3 プロファイルはユーザーアカウントに適用されます。

iOS ：IMAP/POP3 メールプロファイルの設定	説明
IMAP パスのプレフィックス	ここには必要に応じて、IMAP パスプレフィックスを指定します。 詳細については、必要に応じて、ISP へお問い合わせください。 この設定は、［メールの種類］の値が［IMAP］に設定されている場合のみ有効です。
メッセージの移動を許可する	この設定では、ユーザーがこのアカウントから iOS デバイスにある別のメールアカウントへメールを移動できるかどうかを指定します。
最近のアドレスの同期を許可する	この設定では、iOS デバイスユーザーが最近使用したメールアドレスをデバイス間で同期できるかどうかを指定します。
メール内でのみ使用する	この設定では、iOS デバイス上のメールアプリ以外のアプリが、このアカウントを使用してメールを送信できるかどうかを指定します。
S/MIME を有効にする	この設定では、iOS デバイスユーザーが S/MIME で保護されたメールを送信できるかどうかを指定します。 S/MIME は、MDM コントロールでアクティベーションされたデバイスでのみサポートされます。
署名資格情報	この設定では、デバイスがメールの署名に使用する資格情報を指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 デフォルト設定は［共有証明書］です。
署名共有証明書	この設定では、デバイスがメールの署名に使用するクライアント証明書の共有の証明書プロファイルを指定します。 この設定は、［署名資格情報］設定が［共有証明書］に設定されている場合のみ有効です。

iOS ：IMAP/POP3 メールプロファイルの設定	説明
SCEP に署名する	この設定では、デバイスが、S/MIME を使用してメールに署名するために必要な証明書を取得するために使用できる SCEP プロファイルを指定します。 この設定は、［署名資格情報］設定が［SCEP］に設定されている場合のみ有効です。
署名ユーザー資格情報	この設定では、デバイスが、S/MIME を使用してメールに署名するために必要なクライアント証明書を取得するために、ユーザーが使用できる資格情報プロファイルを指定します。 この設定は、［署名資格情報］設定が［ユーザー資格情報］に設定されている場合のみ有効です。
暗号化資格情報	この設定では、デバイスがメッセージを暗号化するために必要な証明書を検索する方法を指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効です。 使用できる値： • 共有証明書 • SCEP • ユーザー資格情報 プロファイルの種類の選択後、使用する共有証明書、SCEP、または資格情報プロファイルを選択します。
暗号化共有証明書	この設定では、デバイスがメールの暗号化に使用するクライアント証明書の共有の証明書プロファイルを指定します。 デバイスは、S/MIME を使用してメッセージを暗号化するために、受信者に適した証明書を選択します。 この設定は、［暗号化資格情報］設定が［共有証明書］に設定されている場合のみ有効です。
暗号化 SCEP	この設定では、デバイスが、S/MIME を使用してメールを暗号化するために必要な証明書を取得するために使用できる SCEP プロファイルを指定します。 この設定は、［暗号化資格情報］設定が［SCEP］に設定されている場合のみ有効です。
暗号化ユーザー資格情報	この設定では、デバイスが、S/MIME を使用してメールを暗号化するために必要なクライアント証明書を取得するために、デバイスが使用できるユーザー資格情報プロファイルを指定します。 この設定は、［暗号化資格情報］設定が［ユーザー資格情報］に設定されている場合のみ有効です。

iOS ：IMAP/POP3 メールプロファイルの設定	説明
メッセージを暗号化	この設定では、ユーザーが送信するときにすべてのメールメッセージを暗号化する必要があるか（［必須］）、または送信する時点で暗号化するメッセージをユーザーが選択できるようにするか（［許可］）を指定します。 この設定は、［S/MIME を有効にする］設定が選択されている場合のみ有効になります。 使用できる値： • 必須 • を許可する デフォルト値は［必須］です。
Mail Drop を許可する	この設定では、ユーザーが Mail Drop を使用して、このアカウントからファイルを送信できるようにするどうかを指定します。

Android ：IMAP/POP3 メールプロファイルの設定

Android ：IMAP/POP3 メールプロファイルの設定	説明
IMAP パスのプレフィックス	ここには必要に応じて、IMAP パスプレフィックスを指定します。 詳細については、必要に応じて、ISP へお問い合わせください。 この設定は、［メールの種類］の値が［IMAP］に設定されている場合のみ有効です。
サーバーからメールを削除	この設定では、メールサーバーからメールを削除する時期を指定します。 使用できる値： • 許可しない • 受信トレイから削除されたとき デフォルト値は［なし］です。 この設定は、［メールの種類］の値が［POP3］に設定されている場合のみ有効です。

Windows ：IMAP/POP3 メールプロファイルの設定

Windows ：IMAP/POP3 メールプロファイルの設定	説明
サーバーからメールを削除	この設定は、ユーザーがメールメッセージを削除したときに、削除したメッセージを処理する方法を指定します。メールメッセージは、サーバーから削除するか（ハードの削除）、受信トレイから削除してもごみ箱フォルダーに置いておくことができます（ソフトの削除）。 使用できる値： • ハードの削除 • ソフトの削除 デフォルト値は、［ソフトの削除］です。 この設定は、［メールの種類］の値が［IMAP］に設定されている場合のみ有効です。
ドメイン	この設定では、メールサーバーのドメインを指定します。
同期間隔	この設定では、Windows デバイスがメールサーバーから新しいコンテンツをダウンロードする頻度を指定します。 使用できる値： • 手動 • 15 分 • 30 分 • 60 分 • 2 時間 デフォルト値は［15 分］です。
初期取得量	この設定では、過去何日まで遡って、メールとオーガナイザーデータを Windows デバイスに同期するかを指定します。 使用できる値： • すべて • 7 日 • 14 日 • 30 日 デフォルト値は［7 日］です。
Wi-Fi は使用せず携帯電話ネットワークのみを使用	この設定は、メールメッセージがワイヤレスネットワーク経由でのみ送受信されるかどうかを指定します。

iOS および macOS デバイス用 CardDAV プロファイルおよび CalDAV プロファイルの設定

CardDAV プロファイルおよび CalDAV プロファイルを使用すると、iOS および macOS デバイスでリモートサーバー上の連絡先とカレンダー情報にアクセスできます。CardDAV プロファイルと CalDAV プロファイルはユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。複数のデバイスで同じ情報にアクセスできます。

macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。CardDAV および CalDAV プロファイルはユーザーアカウントに適用されます。

CardDAV プロファイルの作成

作業を始める前に：

- デバイスがアクティブ CardDAV サーバーにアクセスできることを確認します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［メール、カレンダー、および連絡先］ > ［**CardDAV**］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. プロファイルのサーバーアドレスを入力します。これは、カレンダーアプリケーションをホストするコンピューターの FQDN です。
6. ［ユーザー名］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合、ユーザー名を入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserName%` と入力します。
7. 必要に応じて、CardDAV サーバーのポートを入力します。
8. 必要に応じて、［**SSL** を使用］チェックボックスをオンにして、SSL サーバーの URL を入力します。
9. ［追加］をクリックします。

終了したら： プロファイルをユーザー、ユーザーグループ、またはデバイスグループに割り当てます。

CalDAV プロファイルの作成

作業を始める前に：

- デバイスがアクティブ CalDAV サーバーにアクセスできることを確認します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［メール、カレンダー、および連絡先］ > ［**CalDAV**］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. プロファイルのサーバーアドレスを入力します。これは、カレンダーアプリケーションをホストするコンピューターの FQDN です。

6. ［ユーザー名］フィールドで、次の操作のいずれかを実行します。
   - プロファイルが 1 人のユーザーに対応している場合、ユーザー名を入力します。
   - プロファイルが複数のユーザーに対応している場合は、`%UserName%` と入力します。
7. 必要に応じて、CalDAV サーバーのポートを入力します。
8. 必要に応じて、［**SSL** を使用］チェックボックスをオンにして、SSL サーバーの URL を入力します。
9. ［追加］をクリックします。

終了したら： プロファイルをユーザー、ユーザーグループ、またはデバイスグループに割り当てます。

商標などに関する情報

©2020 BlackBerry Limited. BLACKBERRY、BBM、BES、EMBLEM Design、ATHOC、CYLANCE、SECUSMART などの商標（ただし、これらに限定されるとは限らない）は BlackBerry Limited、その子会社および関連会社の商標または登録商標であり、ライセンスに基づいて使用され、当該の商標に対する独占権は明確に留保されています。その他すべての商標は各社の所有物です。

本書は、参照用として本書で取り上げるすべての文書（提供される文書または BlackBerry の Web サイトで参照可能な文書）を含めて「現状のまま」または「参照可能な形で」提供されるか、またはアクセスすることができ、BlackBerry Limited およびその関連会社（「BlackBerry」）はいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry は本書の誤記、技術的な誤りまたはその他の誤り、エラー、遺漏について何ら責任を負いません。BlackBerry の所有権、機密情報および/または企業秘密を保護するため、本書では一部の BlackBerry テクノロジの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

本書は、第三者をソースとする情報、ハードウェアまたはソフトウェア、製品またはサービス（コンポーネントや、著作権保護されたコンテンツなど）、および/または第三者の Web サイト（これらをまとめて「サードパーティ製品およびサービス」という）への参照を含んでいる可能性があります。BlackBerry は、サードパーティ製品およびサービスの内容、正確性、著作権遵守、互換性、性能、信頼性、適法性、品格、リンク、他の側面などに限定することなく、サードパーティ製品およびサービスを一切管理することはなく、責任も負いません。本書においてサードパーティ製品およびサービスを参照することは、BlackBerry がサードパーティ製品およびサービスまたは第三者を保証することを意味するものではありません。

該当する司法管轄地域の適用法で明確に禁じられている場合を除き、本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスについて、耐久性、特定の目的または使用に対する適合、商品性、適性品質、権利侵害の不存在、品質満足度、権原、または制定法、慣習法、取引過程、商慣習から生じる、本書またはその使用に関する、または性能または性能の不履行に関する条件付け、承認、表明、保証などに限定することなく、明示的または黙示的に、いかなる条件付け、承認、表明、または保証も除外されます。ユーザーは、国や地域によって異なる他の権利を有する場合もあります。一部の司法管轄地域では、黙示的な保証および条件の除外事項または限定事項は禁止されています。法律で認められている範囲で、本書に関連する黙示的な保証または条件は、上記に定めるように除外できないが限定できる場合、ユーザーが本書または該当する対象物を初めて入手してから 90 日間に限定されます。

該当する司法管轄地域の適用法で認められている最大限の範囲で、本書またはその使用に関連して、または本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスの性能または性能の不履行に関連して、直接的、必然的、典型的、偶発的、間接的、特殊的、懲罰的、または加重的損害、金銭的損失による損害（利益または収益の損失、予想される貯蓄の未達成、事業の中断、ビジネス情報の消失、ビジネス機会の喪失、データの破損または消失、データの送受信の失敗、BlackBerry 製品またはサービスと併用したアプリケーションに関連する問題、ダウンタイムコスト、BlackBerry 製品またはサービスあるいはその一部の使用機会や通信サービスの使用機会の喪失、代替品コスト、保険料、設備費、保守費、資本コストなど）に限定することなく、損害を予想できたかどうかを問わず、BlackBerry が損害の可能性について勧告を受けていた場合を含め、いかなる場合においても、BlackBerry はいかなる損害の責任も負わないものとします。

該当する司法管轄地域の適用法で認められている最大限の範囲で、契約、不法行為、またはユーザーに対する過失責任または厳格責任について、BlackBerry は他のいかなる義務、責務、または責任も負わないものとします。

本書の限定事項、除外事項、および免責事項は、（A）訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、（B）BlackBerry およびその関連会社、その後継

者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

上記に定める限定事項および除外事項に加えて、いかなる場合においても、BlackBerry の取締役、従業員、代理業者、販売業者、納入業者、請負業者または BlackBerry の関連会社は、本書に起因または関連する責任を負わないものとします。

ユーザーは、サードパーティ製品およびサービスの加入、インストール、または使用前に、通信事業者がサードパーティ製品およびサービスのすべての機能をサポートすることに同意していることを確認する責任を負います。一部の通信事業者は、BlackBerry® Internet Service への加入によるインターネット閲覧機能を提供しない場合があります。サービスの利用、ローミング、サービスプラン、その他の機能については、通信事業者に問い合わせてください。BlackBerry 製品およびサービスにおけるサードパーティ製品およびサービスのインストールまたは使用には、第三者の権利を侵害または妨害しないように、特許、商標、著作権、または他のライセンスが必要になる場合があります。ユーザーは、サードパーティ製品およびサービスを使用するかどうかを決定し、使用するためにサードパーティライセンスが必要かどうかを確認する責任を負います。必要な場合、ユーザーはライセンスを取得する責任を負います。ユーザーは、必要なライセンスをすべて取得するまで、サードパーティ製品およびサービスをインストールまたは使用してはなりません。BlackBerry 製品およびサービスで提供されるサードパーティ製品およびサービスは、ユーザーの便宜のために「現状のまま」提供され、BlackBerry は明示的にも黙示的にもいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry はそれに関連するいかなる責任も負わないものとします。ユーザーによるサードパーティ製品およびサービスの使用は、ライセンスまたは BlackBerry との他の契約で明示的に対象になっている場合を除き、個別のライセンスおよび第三者との他の該当契約の条件に従うものとし、その制約を受けるものとします。

BlackBerry 製品またはサービスの使用条件は、個別のライセンスまたは BlackBerry との他の該当契約に定められています。本書の内容は、本書以外に BlackBerry 製品またはサービスの一部に対して BlackBerry が提供した文書による明示的な契約または保証を破棄するものではありません。

BlackBerry Enterprise Software には、特定のサードパーティ製ソフトウェアが組み込まれています。このソフトウェアに関連するライセンスおよび著作権情報は、http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp でご確認いただけます。

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

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

Published in Canada