BlackBerry UEM

電子メール、カレンダー、連絡先の管理

12.20

目次

デバイスの仕事用メールの設定

デバイスの仕事用メールを設定する場合は、次のオプションを使用できます。

仕事用メールオプション	主な機能
BlackBerry Work	BlackBerry Work は、仕事用メール、カレンダ、および連絡先を安全に同期します。オンラインプレゼンスを表示したり、仕事用ドキュメントにアクセスしたりすることもできます。組み込みのメールクライアントとは異なり、BlackBerry Work はこれらの機能を単一の使いやすいアプリに統合します。 BlackBerry Work を管理する方法の詳細については、「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	メールプロファイルを使用して、デバイスを組織のメールサーバーに接続し、Exchange ActiveSync または IBM Notes Traveler を使用してメールメッセージ、カレンダエントリ、およびオーガナイザデータを同期できます。 たとえば、メールプロファイルを使用して、組み込みのメールアプリを設定できます。メールプロファイルは BlackBerry Work には必要ありません。
IMAP/POP3 メールプロファイル	IMAP および POP3 メールプロファイルを使用してデバイスが IMAP または POP3 メールサーバーに接続して、メールメッセージのみを同期することができます。

Exchange ActiveSync 仕事用メールおよびオーガナイザデータにアクセスできるデバイスの制御

組織が Microsoft Exchange ActiveSync を使用している場合、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 へのアクセス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、自動的に追加して、デバイスを許可リストに簡単に追加できます。ユーザーのデバイスのメール、カレンダ、連絡先へのアクセスを管理するために BlackBerry Dynamics アプリ（BlackBerry Work など）を使用しているか、メールプロファイルを使用しているかに関係なく、BlackBerry Gatekeeping Service を使用できます。

BlackBerry Gatekeeping Service を設定して使用するには、次の手順を実行します。

1. Microsoft Exchange Server または Microsoft 365 のゲートキーピング設定を作成します。.
2. ゲートキーピングプロファイルをユーザーアカウント、ユーザーグループ、およびデバイスグループに割り当てます。
3. メールプロファイルを設定するか、BlackBerry Work 自動ゲートキーパーサーバーを参照するように設定します。

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。

ほとんどのデバイスでは、各デバイスの許可リストに追加できる E メールクライアントは 1 つだけです。Exchange Server の許可されたデータを含むアプリ設定を使用する Android Enterprise および Samsung Knox デバイスの場合、メールアプリケーションを許可する優先順位は次のとおりです。

1. Exchange Server の許可された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. 登録時に 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 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。

組織で 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。

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、BlackBerry Connectivity Node 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。設定関連の資料で「地域接続を管理するためのサーバーグループの作成」を参照してください。

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	組織が Microsoft Exchange Server 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のみに Exchange ActiveSync へのアクセスを許可」を参照してください。 組織が Microsoft 365 を使用している場合は、「Microsoft 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。
3	ゲートキーピングのための Microsoft IIS 権限を設定する。
4	モダン認証を設定するために Entra アプリを追加して Entra の詳細情報を取得する
5	ゲートキーピング設定の作成。
6	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 365 でユーザーアカウントを作成し、ゲートキーピングのために必要な権限を与える必要があります。

Microsoft 365 を使用している場合、Microsoft 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 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、管理ロールの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ための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、ゲートキーピングを設定する Microsoft Exchange Server をホストするコンピューターのデフォルト設定になっています。管理者としてコマンドプロンプトからコマンド「`Winrm quickconfig`」を実行する必要があります。ツールに `Make these changes [y/n]` が表示されたら、y を入力します。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 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. Microsoft Exchange Management Shell を開きます。
2. 「`New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`」を入力します。Enter キーを押します。
3. 「`New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`」を入力します。Enter キーを押します。
4. 「`New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`」を入力します。Enter キーを押します。
5. 「`Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`」を入力します。Enter キーを押します。
6. 「`Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`」を入力します。Enter キーを押します。
7. 「`Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`」を入力します。Enter キーを押します。
8. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`」を入力します。Enter キーを押します。
9. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`」を入力します。Enter キーを押します。
10. 「`Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox`」を入力します。Enter キーを押します。
11. 「`Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox`」を入力します。Enter キーを押します。
12. 「`Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`」を入力します。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>"`」を入力します。Enter キーを押します。

14. 「`Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`」を入力します。Enter キーを押します。
15. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"`」を入力します。Enter キーを押します。
16. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`」を入力します。Enter キーを押します。
17. 「`Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`」を入力します。Enter キーを押します。

終了したら：

- 組織が Microsoft Exchange Server 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のみに Exchange ActiveSync へのアクセスを許可」を参照してください。
- 組織が Microsoft 365 を使用している場合は、「Microsoft 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するには、Microsoft Exchange Server 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。

このタスクを実行するには、Set-ActiveSyncOrganizationSettings コマンドに対する適切な権限を保有する Microsoft Exchange 管理者である必要があります。https://technet.microsoft.com にアクセスして、コマンドおよび Exchange ActiveSync にアクセスするデバイスの管理の詳細を確認します。

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。
- 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。組織の Exchange ActiveSync のデフォルトアクセスレベルが［許可］に設定されており、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には、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーが個人的例外またはユーザーアカウントに関連付けられているデバイスルールを持ってい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`」を入力します。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 365 でのモバイルデバイスアクセスポリシーの設定

BlackBerry Gatekeeping Service で Microsoft 365 を使用するには、Microsoft 365 でモバイルデバイ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。
- 組織の Exchange ActiveSync のデフォルトアクセスレベルが［許可］に設定されており、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には、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーが個人的例外またはユーザーアカウントに関連付けられているデバイスルールを持ってい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 33531 を参照してください。

1. Microsoft 365 管理ポータルにログインします。
2. 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。

作業を始める前に：

- 組織が Microsoft Exchange Server 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のみに Exchange ActiveSync へのアクセスを許可」を参照してください。
- 組織が Microsoft 365 を使用している場合は、「Microsoft 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。

1. 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、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］をクリックします。
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。

モダン認証を設定するために Entra アプリを追加して Entra の詳細情報を取得する

BlackBerry UEM を設定し、モダン認証を使用して Microsoft 365 に接続する場合、アプリの 2 つの詳細情報（アプリケーション ID と組織）を入力する必要があります。これらの手順を実行すると、［メンバーの選択］セクションに Entra アプリ ID が表示されます。Entra の組織情報は、ディレクトリのプロパティとして Microsoft Entra ID ページに表示されます。ゲートキーピングプロファイルでのモダン認証のために BlackBerry UEM を設定するときに使用するこれらの 2 つのエントリを記録します。

1. portal.azure.com にサインインします。
2. ［アプリの登録］をクリックします。
3. ［新しい登録］をクリックします。
4. ［名前］フィールドに、アプリの名前を入力します。
5. ［登録］をクリックします。
6. ［**API** のアクセス許可］ **>** ［アクセス許可の追加］をクリックします。
7. **Exchange** または **Office 365 Exchange Online** のアクセス許可グループを探します。
8. ［アプリケーションの許可］ **>** ［**Exchange.ManageAsApp**］ **>** ［アクセス許可の追加］をクリックします。
9. 管理者の同意を与える場合は、［**Exchange.ManageAsApp**］ **>** ［管理者の同意を与えます］を選択します。
10. ［管理］セクションで、［証明書とシークレット］ **>** ［証明書のアップロード］の順にクリックし、公開鍵（cert.pem）を選択します。
11. アプリにロールを割り当てる場合は、Entra のホームページで **Microsoft Entra ID** をクリックします。
12. ［ロールと管理者］をクリックします。
13. ［管理者ロール］セクションで「Exchange」と入力して、Microsoft Exchange でサポートされるロールを表示します。
14. ロールをクリックすると、ロールの詳細が表示されます。
15. ［割り当ての追加］をクリックします。
16. ［メンバーの選択］で、［メンバーが選択されていません］をクリックします。
17. Entra アプリ ID を、アプリ名またはアプリ ID で検索します。
18. ［選択されたアイテム］セクションに移動するアプリを選択します。
19. ［選択］をクリックします。
20. ［次へ］をクリックします。
21. ［割り当ての追加］ページで、［割り当ての種類］が［アクティブ］に設定されていることを確認します。割り当てタイプの詳細については、Microsoft の情報を参照してください。
22. ［割り当て］をクリックします。

終了したら： モダン認証のための UEM の Entra アプリ ID と証明書の関連付け

モダン認証のための UEM の Entra アプリ ID と証明書の関連付け

新しいクライアント証明書を要求して CA サーバーからエクスポートすることも、自己署名証明書を使用することも可能です。秘密鍵は .pfx 形式にする必要があります。公開鍵は、Microsoft Entra ID にアップロードするために、.cer または .pem ファイルとしてエクスポートできます。

1. 次のタスクのいずれかを実行します。

証明書	タスク
既存の CA サーバーを使用する場合	a. 証明書を要求します。要求する証明書では、証明書の件名にアプリ名を含める必要があります。ここで <*app name*> は、「モダン認証を設定するためにアプリを追加して Entra の詳細情報を取得する」の手順 4 でアプリに割り当てた名前です。 b. 証明書の公開鍵を .cer または .pem ファイルとしてエクスポートします。公開鍵は、作成された Entra アプリ ID に使用されます。 c. 証明書の秘密鍵を .pfx ファイルとしてエクスポートします。

証明書	タスク
自己署名証明書を使用する場合	**a.** New-SelfSignedCertificate コマンドを使用して、自己署名証明書を作成します。詳細については、docs.microsoft.com にアクセスして New-SelfSignedCertificate の情報を参照してください。 **1.** Microsoft Windows を実行しているコンピューターで、Windows PowerShell を開きます。 **2.** コマンド「`$cert=New-SelfSignedCertificate -Subject "CN=<app name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`」を入力します。ここで <*app name*> は、「モダン認証を設定するためにアプリを追加して Entra の詳細情報を取得する」の手順 4 でアプリに割り当てた名前です。要求する証明書では、件名フィールドに Entra アプリ名を含める必要があります。 **3.** **Enter** キーを押します。 **b.** Microsoft 管理コンソール（MMC）から公開鍵をエクスポートします。公開証明書は、.cer または .pem ファイルとして保存してください。公開鍵は、作成された Entra アプリ ID に使用されます。 **1.** Windows を実行しているコンピューターで、ログインしているユーザーの証明書マネージャーを開きます。 **2.** ［個人］を開きます。 **3.** ［証明書］をクリックします。 **4.** <*user*>@<*domain*> を右クリックし、［すべてのタスク］ **>** ［エクスポート］をクリックします。 **5.** ［証明書のエクスポート ウィザード］で、［いいえ、秘密キーをエクスポートしません］をクリックします。 **6.** ［次へ］をクリックします。 **7.** ［**Base-64 encoded X.509 (.cer)**］を選択します。［次へ］をクリックします。 **8.** 証明書の名前を入力し、デスクトップに保存します。 **9.** ［次へ］をクリックします。 **10.** ［完了］をクリックします。 **11.** ［**OK**］をクリックします。 **c.** Microsoft 管理コンソール（MMC）から秘密鍵をエクスポートします。必ず秘密鍵を含めて、.pfx ファイルとして保存してください。 **1.** Windows を実行しているコンピューターで、ログインしているユーザーの証明書マネージャーを開きます。 **2.** ［個人］を開きます。 **3.** ［証明書］をクリックします。 **4.** <*user*>@<*domain*> を右クリックし、［すべてのタスク］ **>** ［エクスポート］をクリックします。 **5.** 証明書のエクスポート ウィザードで、［はい、秘密キーをエクスポートします］をクリックします。 **6.** ［次へ］をクリックします。 **7.** ［**Personal Information Exchange – PKCS #12 (.pfx)**］を選択します。［次へ］をクリックします。 **8.** セキュリティ方式を選択します。 **9.** 証明書の名前を入力し、デスクトップに保存します。 **10.** ［次へ］をクリックします。 **11.** ［完了］をクリックします。 **12.** ［**OK**］をクリックします。

2. 手順 1 でエクスポートした公開証明書（.pem または.cer ファイル）をアップロードし、証明書の資格情報を UEM の Entra アプリ ID に関連付けます。
   a) portal.azure.com で <*app name*> を開きます。このアプリ名は、「モダン認証を設定するためにアプリを追加して Entra の詳細情報を取得する」の手順 4 でアプリに割り当てた名前です。
   b) ［証明書とシークレット］をクリックします。
   c) ［証明書］セクションで［証明書のアップロード］をクリックします。
   d) ［ファイルの選択］検索フィールドで、証明書をエクスポートした場所に移動します。
   e) ［追加］をクリックします。

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 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 Microsoft IIS 権限を設定する。
- モダン認証を使用する場合は、「モダン認証を設定するために Entra アプリを追加して Entra の詳細情報を取得する」に従います。

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. 次のタスクのいずれかを実行します。

タスク	手順
モダン認証を使用して Microsoft 365 に接続します	モダン認証を使用するように BlackBerry UEM を設定する前に、公開鍵と秘密鍵を持つ証明書を生成する必要があります。証明書は、OpenSSL または PowerShell を使用して生成できます。詳細については、「モダン認証のための Entra アプリ ID と証明書の関連付け」を参照してください。 **a.** ［モダン認証］チェックボックスをオンにします。 **b.** ［**Exchange Online** 接続名］フィールドに、接続の名前を入力します。 **c.** ［参照］をクリックして、認証に使用する証明書を選択します。 **d.** ［証明書のパスワード］フィールドに、証明書のパスワードを入力します。 **e.** ［**Entra** アプリケーション **ID**］を指定します。 **f.** ［**Entra** 組織］を指定します。

タスク	手順
基本認証を使用して、Microsoft Exchange Server または Microsoft 365 に接続します。	a. ［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 365 環境の名前を入力します。 b. 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。 c. ［認証の種類］ドロップダウンリストで、Microsoft Exchange Server または Microsoft 365 で使用する認証の種類を選択します。 d. BlackBerry UEM と Microsoft Exchange Server または Microsoft 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。 e. ［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 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）。 f. 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。 g. 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。

4. ［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。
5. ［保存］をクリックします。

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 BlackBerry Connectivity Node 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

自動ゲートキーピングに BlackBerry Gatekeeping Service を設定した後、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 ゲートキーピングサーバーまたは BlackBerry Connectivity Node サーバーグループを選択できます。

BlackBerry Connectivity Node サーバーグループを使用している場合は、BlackBerry Gatekeeping Service の 1 つ以上のアクティブなインスタンスを持つ適切なサーバーグループを選択します。こ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。

1. 管理コンソールのメニューバーで、［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 つまたは複数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。

終了したら：

- ゲートキーピングプロファイル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。
- ユーザーが仕事用メールにアクセスするには、メールプロファイルまたは BlackBerry Work アプリをユーザーに割り当てる必要があります。BlackBerry Work を管理している場合は、アプリ設定で BlackBerry Gatekeeping Service サービスを有効にする必要があります。

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

組織が BlackBerry Gatekeeping Service を使用して、Exchange ActiveSync から仕事用メールおよびオーガナイザデータへのアクセスを許可するデバイスを制御する場合、デバイスと Exchange ActiveSync の間の接続ステータスを確認できます。接続を確立するために、ユーザーには、少なくとも 1 つのゲートキーパーサーバーが関連付けられたメールプロファイルが割り当てられます。接続ステータスは、IT ポリシーとプロファイルセクションのメールプロファイルの横にあるユーザーアカウントのデバイス詳細ページに表示されます。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントの名前を検索してクリックします。
3. 確認するデバイスのタブを選択します。
4. ［**IT** ポリシーおよびプロファイル］セクションで、以下のステータスに注意します。
   - ［接続が許可されています］：このステータスは、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に表示されます。
   - ［接続を保留中］：このステータスは、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に表示されます。
   - ［不明］：このステータスは、BlackBerry UEM がデバイスの ID を判別できない場合に表示されます。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。

Exchange ActiveSync へのアクセスの手動での許可またはブロック

デバイスが自動的に許可リストに追加されず Exchange ActiveSync にアクセスできない場合は、BlackBerry UEM 管理コンソールからデバイスへのアクセスを手動で許可できます。たとえば、UEM 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 Android デバイスなど、デバイスの Exchange ActiveSync ID を取得できない場合、デバイスにアクセスを許可するには、手動でデバイスを許可する必要があります。

以前に許可したデバイスが Exchange ActiveSync にアクセスするのをブロックできます。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取得できなくなります。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［**Exchange** ゲートキーピング］をクリックします。
2. ［制限されたデバイス］リストで、デバイスを検索します。

3. ［アクション］列で、次のいずれかを実行します。
   - Exchange ActiveSync へのアクセスを許可するには、✓ をクリックします。
   - Exchange ActiveSync へのアクセスをブロックするには、⊘ 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、デバイスがどのような方法で組織のメールサーバーに接続し、Exchange ActiveSync または IBM Notes Traveler を使用してメールメッセージ、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かを指定できます。

組織が BlackBerry Work を使用してユーザーデバイスのメール、カレンダー、連絡先を管理している場合は、メールプロファイルを使用する必要はありません。BlackBerry Work を管理する方法の詳細については、「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。

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

- Exchange ActiveSync を設定してどのデバイスがアクセスできるかを制御できます。
- 拡張メールセキュリティの場合は、iOS および Android デバイスの S/MIME を有効にすることができます。
- 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、iOS デバイスで使用するには、BlackBerry Secure Gateway を有効にする必要があります。

また、IMAP/POP3 メールプロファイル を使用すると、iOS、macOS、Android、および Windows デバイスがどのような方法で IMAP または POP3 メールサーバーに接続し、メールメッセージを同期するかを指定できます。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。

1. 管理コンソールのメニューバーで、［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%` を入力します。
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%` を入力します。

- 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%` を入力します。

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。
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。
- MDM 制御 アクティベーションを使用する Android デバイスの場合、BlackBerry UEM はメールプロファイルをデバイスに送信しますが、ユーザーはメールサーバーへの接続を手動で設定する必要があります。

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

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。
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。 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% を使用します。
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、この設定は適切なサーバーグループを指定します。

iOS ：メールプロファイル設定

これらの設定は iPadOS デバイスにも適用されます。

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デバイス上の別の既存するメールアカウントにメッセージ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、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、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メッセージ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、ユーザーが S/MIME で保護されたメールメッセージ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。
署名資格情報	この設定では、メッセージの署名に必要な証明書をデバイスが見つけるための手段を指定します。 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、メッセージの署名のためにデバイスが使用するクライアント証明書用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、S/MIME を使用したメッセージの署名に必要な証明書を取得するためにデバイスが使用できる 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。

iOS ：メールプロファイル設定	説明
署名ユーザー資格情報	この設定では、S/MIME を使用したメッセージの署名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 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、［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、［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。
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メッセージを S/MIME 方式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、メッセージの暗号化に必要な証明書をデバイスが見つけるための手段を指定します。 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、メッセージの暗号化のためにデバイスが使用するクライアント証明書用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、S/MIME を使用したメッセージの暗号化に必要な証明書を取得するためにデバイスが使用できる 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。

iOS ：メールプロファイル設定	説明
暗号化ユーザー資格情報	この設定では、S/MIME を使用したメッセージの暗号化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、［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、［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（［許可する］）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。 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、メッセージとオーガナイザーデータをデバイスに同期するかを指定します。 メモ：この設定は、MDM 制御 アクティベーションタイプが設定されたデバイス上の、デフォルトのメールアプリとオーガナイザアプリにのみ適用されます。
アカウントごとの VPN	この設定は、このアカウントのネットワーク通信に使用される VPN プロファイルを指定します。この設定は、iOS 14 以降または iPadOS 14 以降のデバイスにのみ適用されます。
認証	

iOS ：メールプロファイル設定	説明
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が設定されたデバイスで、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。
認証の種類	この設定では、メールサーバーに接続するためにデバイスが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。
共有証明書プロファイル	この設定では、メールサーバーに接続するためにデバイスが使用するクライアント証明書用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、メールサーバー認証に使用されるクライアント証明書を登録するためにデバイスが使用する、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、メールサーバー認証に使用されるクライアント証明書を登録するためにデバイスが使用する、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、メールサーバー認証のために、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デバイスが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。

iOS ：メールプロファイル設定	説明
OAuth サインイン URL	この設定は、このアカウントが OAuth にサインインするために使用する URL を指定します。この URL を指定する場合は、自動検出が使用されないため、ホストを指定する必要があります。 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。
OAuth トークン要求 URL	この設定は、OAuth を使用するトークン要求にこのアカウントが使用する URL 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。
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。
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。

iOS ：メールプロファイル設定	説明
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。
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。
メモ	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。
アカウントの変更	
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対するアクセスの有効/無効状態を変更できるかどうかを指定します。
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対するアクセスの有効/無効状態を変更できるかどうかを指定します。
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対するアクセスの有効/無効状態を変更できるかどうかを指定します。
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対するアクセスの有効/無効状態を変更できるかどうかを指定します。
メモ	この設定では、ユーザーがデバイス上の仕事用メモに対するアクセスの有効/無効状態を変更できるかどうかを指定します。

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。

macOS ：メールプロファイル設定	説明
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

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。 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。 Samsung Knox MDM を使用する Android デバイスは、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の種類が MDM 制御 の Android 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。
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に使用するクライアント証明書を取得するための関連付けられた 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、メールサーバー認証のために、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デバイスが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。

Android ：メールプロファイル設定	説明
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。 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。
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。

Android ：メールプロファイル設定	説明
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。
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。
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。

Android ：メールプロファイル設定	説明
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	
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。

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。
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。
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。
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。

Windows ：メールプロファイル設定	説明
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 Secure Gateway を使用して iOS デバイスに送信されるメールデータの保護

BlackBerry Secure Gateway を使用して、メールデータを保護し、iOS および iPadOS デバイスが仕事用メールを送受信できるようにすることができます。ゲートウェイは、ファイアウォールの外側にメールサーバーを公開したり、DMZ 内のメールサーバーを検索したりすることなく、BlackBerry Infrastructure と BlackBerry UEM を介して組織のメールサーバーへの安全な接続を提供します。

デバイスは MDM 制御 アクティベーションタイプでアクティブ化する必要があります。

手順	アクション
1	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。
2	環境に iOS または iPadOS 13.0以降のデバイスが含まれており、組織のメールサーバーが モダン認証（OAuth）を使用するように設定されている場合： • メールプロファイルで、［認証に OAuth を使用する］設定を選択します。 • Exchange ActiveSync サーバーまたは ID プロバイダー証明書を信頼するための BlackBerry UEM の設定 • メールサーバーで OAuth を使用するように BlackBerry Secure Gateway を設定します。
3	BlackBerry Infrastructure への地域接続をサポートし、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は、メールプロファイルで適切なサーバーグループ［BlackBerry Secure Gateway Service サーバーグループ］を選択します。

Exchange ActiveSync サーバーまたは ID プロバイダー証明書を信頼するための BlackBerry UEM の設定

モダン認証（設定の変更）を使用して Microsoft Exchange Online に接続する iOS および iPadOS 13.0 以降のデバイスが環境にある場合、ID プロバイダーの証明書（またはルート証明書）を BlackBerry UEM に追加する必要があります。BlackBerry Secure Gateway は、接続を確立するときに、ID プロバイダ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 サーバーの証明書（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、サーバーを信頼するための証明書を必要とします。

作業を始める前に： 次のサーバーから 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。

- モダン認証が環境でサポートされている場合は、Active Directory ID プロバイダー
- Exchange ActiveSync が TLS 接続を必要とするように設定されている場合は、Exchange ActiveSync サーバー

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［信頼済み証明書］の順にクリックします。

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。

終了したら： サポートされる TLS バージョンと暗号で OAuth を使用するための BlackBerry Secure Gateway の設定。

サポートされる TLS バージョンと暗号で OAuth を使用するための BlackBerry Secure Gateway の設定

BlackBerry Secure Gateway を設定して、モダン認証に OAuth を使用できます。OAuth を使用するには、メールプロファイルからメールサーバー URL を指定し、ID プロバイダーの検出ドキュメントを取得する URL を指定する必要があります。検出ドキュメントの詳細については、Microsoft のマニュアルを参照してください。

BlackBerry Secure Gateway が Exchange ActiveSync との接続に使用する TLS バージョンと Microsoft Exchange SSL 暗号も指定できます。Exchange ActiveSync サーバーのセキュリティ要件に従って、このリストを更新する必要がある場合があります。

作業を始める前に： Exchange ActiveSync サーバーまたは ID プロバイダー証明書を信頼するための BlackBerry UEM の設定

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Secure Gateway**］をクリックします。
2. TLS バージョンまたは SSL 暗号を追加または削除するには、該当するテーブルで ＋ 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。
6. モダン認証を使用するには、［メールサーバー認証の **OAuth** を有効にする］を選択します。
7. ［検出エンドポイント］フィールドに、BlackBerry Secure Gateway が ID プロバイダーの検出ドキュメントを取得しキャッシュするために使用する URL を入力します。
   - 形式：`https://<identity provider>/.well-known/openid-configuration`
   - 例： `https://login.microsoftonline.com/common/.well-known/openid-configuration`
   - 例： `https://login.windows.net/common/.well-known/openid-configuration`

   BlackBerry Secure Gateway は、バージョン管理されていない検出ドキュメントと v2.0 検出ドキュメントの両方を取得し、キャッシュされたドキュメントを定期的に更新します。
8. ［メールサーバーリソース］フィールドに、メールプロファイルで指定されたメールサーバーの URL を「https://」で始まる形式で入力します（例：`https://outlook.office365.com`）。
9. ［保存］をクリックします。

Android Enterprise デバイスの BlackBerry Hub アプリの有効化

BlackBerry Hub は、メッセージ、通知、およびイベントを 1 か所で表示できるようにする Android アプリです。

Android Enterprise デバイスのユーザーに、BlackBerry Hub の仕事用メッセージと個人用メッセージの両方の表示を許可するには、BlackBerry UEM の一部の設定を確認する必要があります。

1. ユーザーに割り当てられた IT ポリシーについては、BlackBerry Productivity Suite セクションで［**BlackBerry Hub** で統合アカウントの表示を許可する］IT ポリシールールが選択されていることを確認します。
2. BlackBerry Hub のアプリの設定で、次の項目が選択されていることを確認します。
   - プロファイル間の **IPC**
   - 仕事用コンテンツへのアクセス

終了したら： メールアカウントの追加、BlackBerry Hub 設定のカスタマイズなど、デバイスでの BlackBerry Hub の使い方については、BlackBerry Hub 関連の資料を参照してください。

詳細については、KB 37721 を参照してください。

S/MIME を使用したメールセキュリティの強化

メールプロファイルから S/MIME を有効にして、iOS および Android デバイスユーザーがメールセキュリティを拡張できるようにすることができます。S/MIME は、メッセージの暗号化と署名を行うための標準的な方式です。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する場合、ユーザーは S/MIME を使用して仕事用メールの暗号化、署名、または暗号化と署名を行うかどうかを指定できます。個人用メールアカウントに対しては S/MIME を有効にできないことに注意してください。

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、指定された各 LDAP 証明書サーバーを対象に、Android および iOS デバイスによる受信者の 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。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、デバイスが単純な認証または Kerberos 認証のいずれかを使用して LDAP 証明書サーバーでの認証を実行するように要求することができます。必須認証証明書を証明書取得プロファイルに含めることにより、デバイスが LDAP 証明書サーバーを使って自動的に認証できます。必須証明書を含めない場合、デバイスが LDAP サーバーでの認証を初めて試行する際に、ユーザーはデバイスから資格情報を入力するように求められます。

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、「iOS デバイスの自動認証を有効にする」を参照してください。

1. 管理コンソールのメニューバーで、［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. テーブルで、＋ をクリックします。
6. ［サービス **URL**］フィールドに、ldap://*<fqdn>*:*<port>* 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 5〜12 を繰り返します。
14. ［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。

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、iOS および Android デバイスに S/MIME 証明書のステータスの確認を許可して、それが有効な証明書かどうかを確認できます。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。

OSCP プロファイルを使用して、デバイスが S/MIME 証明書のステータスを取得する OSCP レスポンダを指定できます。

CRL プロファイルを使用して、デバイスが S/MIME 証明書内で定義されたレスポンダをチェックできるようにすることができます。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要求するように設定することもできます。証明書の取得に Exchange ActiveSync を使用する場合、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、デバイスは OCSP（オンライン証明書ステータスプロトコル）を使用して証明書のステータスをチェックします。

証明書ステータスインジケータは、デバイスによって異なる場合があります。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 iOS および Android デバイスでサポートされます。

1. 管理コンソールのメニューバーで、［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) テーブルで、＋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 3〜5 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 iOS および Android デバイスでサポートされます。

1. 管理コンソールのメニューバーで、［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
CRL に HTTP または HTTPS を使用する	**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 サーバーごとにこれらの手順を繰り返します。

タスク	手順
CRL に LDAP を使用する	**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>*:*<port>* 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>*:*<port>* 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.** ［検索範囲］ドロップダウンリストで、LDAP サーバー検索の適切な検索範囲を選択します。 **f.** 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。 **g.** ［**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）。 **h.** ［**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。 **i.** ［追加］をクリックします。 **j.** LDAP サーバーごとにこれらの手順を繰り返します。

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

iOS および Android 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上のメッセージを保護します。ユーザーは、仕事用メールアドレスの使用時に、PGP 保護によってメッセージの署名、暗号化、または署名と暗号化の両方を実行できます。個人用メールアドレスに対しては PGP を有効にできません。

管理者がメールプロファイルで有効にすることで、ユーザーは PGP を使用できるようになります。iOS および Android デバイスのユーザーに PGP の使用を強制することも、PGP の使用を許可しないことも、または使用を任意にすることも可能です。PGP の使用が任意の場合（デフォルト設定）、ユーザーはデバイスで PGP を有効にし、メッセージを暗号化するか、メッセージに署名するか、または暗号化と署名の両方を行うかを指定できます。

メッセージの署名と暗号化を行うには、受信者ごとに PGP キーをデバイスに保存する必要があります。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、iOS および Android 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、iOS および Android 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

iOS および Android デバイスでは、メッセージの分類を使用して、ユーザーによるメッセージの署名、暗号化、またはその両方を必須化したり、ユーザーのデバイスから送信され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するか、セキュリティ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よって、デバイスが送信メッセージに対して適用する分類ルールが特定されます。

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を作成する方法の詳細については、see KB 36736 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、iPadOS、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. 管理コンソールのメニューバーで、［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%` を入力します。
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%` を入力します。
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。以下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
    - Android ：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
14. ［追加］をクリックします。

iOSおよび macOS：IMAP/POP3 メールプロファイルの設定

これらの設定は iPadOS デバイスにも適用されます。

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。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。
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、S/MIME を使用したメッセージの署名に必要な証明書を取得するためにデバイスが使用できる 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、S/MIME を使用したメッセージの署名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、［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。

iOS ：**IMAP/POP3** メールプロファイルの設定	説明
暗号化資格情報	この設定では、メッセージの暗号化に必要な証明書をデバイスが見つけるための手段を指定します。 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。 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、S/MIME を使用したメッセージの暗号化に必要な証明書を取得するためにデバイスが使用できる 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、S/MIME を使用したメッセージの暗号化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。
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（［許可する］）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。
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。
アカウントごとの VPN	この設定は、このアカウントのネットワーク通信に使用される VPN プロファイルを指定します。

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。 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）。 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。
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。
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 および CalDAV プロファイルの設定

CardDAV および CalDAV プロファイルを使用すると、iOS、iPadOS、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。

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. 管理コンソールのメニューバーで、［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%` を入力します。
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. 必要な場合は、［**Per-account VPN**］フィールドで、このアカウントのネットワーク通信に使用する VPN プロファイルを選択します。
10. ［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. 管理コンソールのメニューバーで、［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%` を入力します。

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. 必要な場合は、［**Per-account VPN**］フィールドで、このアカウントのネットワーク通信に使用する VPN プロファイルを選択します。
10. ［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

該当する特許は、次の場所で確認できます：www.blackberry.com/patents。

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