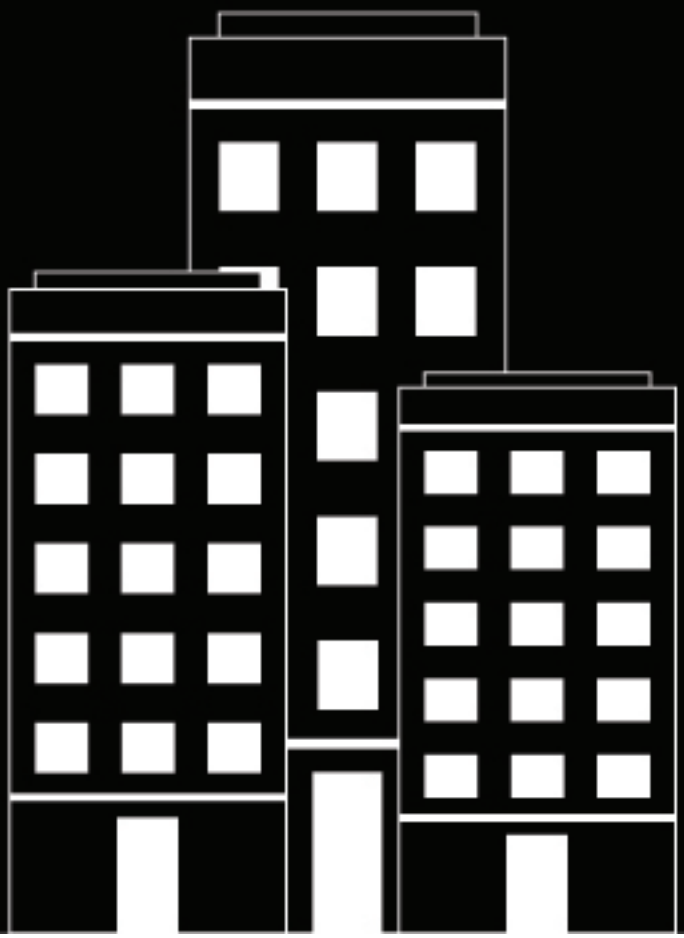

BlackBerry UEM

管理者、ユーザー、およびグループの管理

12.20

Contents

BlackBerry UEM 管理者、ユーザー、およびグループの管理

このガイドでは、組織の BlackBerry UEM 環境を管理するための管理者アカウント、ユーザーアカウント、およびグループの作成と設定の指示と詳細について説明します。

タスク	説明
管理コンソールのログインオプションを設定します。	パスワードの複雑さ、ログイン通知、セッションタイムアウト制限、およびディレクトリベースの認証やシングルサインオンなどのオプションなど、管理者とユーザが UEM コンソールで認証する方法を設定します。
管理者ロールを作成および管理します。	管理コンソールで管理者が持つ制御レベルと権限を設定するには、事前設定された管理者ロールを使用するか、カスタムロールを作成します。
管理者の作成。	管理者ユーザーを作成して、組織の UEM 環境を管理します。
ユーザーアカウントを作成および管理します。	UEM で直接ユーザーアカウントを作成するか、組織の会社のディレクトリからユーザーアカウントを作成します。
ユーザーグループを作成および管理します。	ユーザーグループを作成して、設定と構成を複数のユーザーに適用します。
デバイスグループを作成および管理します。	デバイスグループを作成して、特定のデバイスタイプに設定と構成を適用します。
共有デバイスグループを作成および管理します。	共有デバイスグループを作成して、複数のユーザーが iOS デバイスを共有できるようにします。
公開デバイスグループを作成して管理します。	公開デバイスグループを作成して、単一目的の iOS または特定のアプリセットにロックされている Android Enterprise デバイスを管理します。
共有 iPad グループを作成および管理します。	共有 iPad グループを作成して、複数のユーザーが共有 iPad デバイスにサインインして使用できるようにします。
Chrome OS デバイスを管理します。	UEM を使用して、Chrome OS デバイスの管理アクションを実行します。
BlackBerry UEM Self-Service をセットアップする。	ユーザーが UEM Self-Service にアクセスして、セルフサービスデバイス管理タスクを実行できるようにします。
UEM Self-Service のユーザーロールを作成します。	ロールを使用して、UEM Self-Service のエンドユーザー権限を管理します。
ユーザーリストのカスタマイズ。	必要に応じて、管理コンソールのユーザーアカウントのリストを変更します。

コンソールログインオプションの設定

必要なパスワードの複雑さ、ログイン通知、セッションタイムアウト制限など、管理者とユーザーが BlackBerry UEM コンソールを使用して認証する方法を設定できます。

管理者とユーザーが次の認証方式を使用してログインするようにできます。

認証オプション	説明
ローカルパスワードベースの認証	ローカル管理者およびユーザーは、ユーザー名とパスワードを使用して認証できます。
ディレクトリベースの認証	BlackBerry UEM を社内ディレクトリに接続した場合、管理者およびユーザーは、ディレクトリ証明書を使用してログインできます。詳細については、設定関連の資料で「会社のディレクトリに接続する」を参照してください。
シングルサインオン	オンプレミス環境で UEM を Microsoft Active Directory に接続する場合は、シングルサインオン認証を設定すると、管理者またはユーザーがログイン Web ページをバイパスし、管理コンソールまたは BlackBerry UEM Self-Service に直接アクセスできるようになります。ログインにパスワードや証明書は必要ありません。『BlackBerry UEM のシングルサインオンの設定』を参照してください。 この機能は UEM Cloud ではサポートされていません。
証明書ベースの認証	管理者とユーザーが認証証明書を使用してログインできるように、証明書ベースの認証を設定できます。『証明書ベースのコンソール認証の設定』を参照してください。 この機能は UEM Cloud ではサポートされていません。
BlackBerry 2FA 認証	管理者とユーザーが 2 要素認証でログインできるように、BlackBerry 2FA 認証を設定できます。詳細については、KB 73371 を参照してください。 この機能はオンプレミス環境ではサポートされていません。
BlackBerry Online Account 認証	管理者が BlackBerry Online Account 資格情報を使用してログインできるように、BlackBerry Online Account 認証を設定できます。 この機能はオンプレミス環境ではサポートされていません。

ローカル管理者を対象としたパスワードの最小限の複雑さの設定

ローカル管理者のアカウントに対して、パスワードの最小長と複雑さの要件を設定できます。この設定は、管理者がアカウントのパスワードを変更すると有効になります。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［コンソール］をクリックします。
2. ［最小文字数］フィールドで、コンソールパスワードの要件とする最小文字数を指定します。
3. ［最低限のパスワードの複雑さ］フィールドで、コンソールパスワードの最低限の複雑さを選択します。

4. ［保存］をクリックします。

コンソールのログイン通知の作成

オンプレミス環境で管理者またはユーザーが BlackBerry UEM 管理コンソールや BlackBerry UEM Self-Service にログインした際に表示されるログイン通知を作成できます。この通知は、コンソールを使用する際に承諾する必要がある使用条件を管理者またはユーザーに通知します。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［ログイン通知］の順にクリックします。
2. をクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
UEM 管理コンソールのログイン通知を設定します。	a. ［管理コンソールのログイン通知を有効にする］チェックボックスをオンにします。 b. 管理者がログインしたときに表示する情報を入力します。
UEM Self-Service のログイン通知を設定します。	a. ［セルフサービスコンソールのログイン通知を有効にする］チェックボックスをオンにします。 b. ユーザーがログインしたときに表示する情報を入力します。

4. ［保存］をクリックします。

管理コンソールへのテキストバナーの追加

管理コンソールで各ページの右上のヘッダーに表示される、カスタマイズ可能なテキストバナーを追加できます。このバナーを使用して、コンソールを使用する管理者向けの重要な情報を表示できます（たとえば、UEM テナントの情報を表示できます）。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［コンソールをカスタマイズ］をクリックします。
2. ［バナーテキスト］フィールドで、表示するテキストを入力します。
3. ［保存］をクリックします。
4. ポップアップメッセージで、［送信］をクリックします。
5. バナーテキストの変更を表示するには、管理者はログアウトしてから再度ログインする必要があります。

終了したら： 管理コンソールからログアウトし、再度ログインしてテキストバナーを表示します。

セッションタイムアウト制限の設定

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［コンソール］をクリックします。
2. ［セッションタイムアウト］フィールドに、セッションがタイムアウトしてユーザーがログアウトされるまでの時間を分単位で入力します。

3. ［セッションタイムアウトの警告］フィールドに、ユーザーをログアウトする前に、セッションタイムアウト警告を表示する時間を分単位で入力します。
4. ［保存］をクリックします。

BlackBerry UEM のシングルサインオンの設定

BlackBerry UEM を Microsoft Active Directory に接続する場合は、シングルサインオン認証を設定すると、管理者またはユーザーがログイン Web ページをバイパスし、管理コンソールまたは BlackBerry UEM Self-Service に直接アクセスできるようになります。管理者またはユーザーが Windows にログインした場合、ブラウザーは資格情報を使用して、UEM で自動的に認証を行います。Windows のログイン情報は、Active Directory の資格情報または派生した資格情報を含めることができます（たとえば、CAC リーダーやデジタルトークンから）。

この機能は UEM Cloud ではサポートされていません。

作業を始める前に：

- 次の操作を実行して、Active Directory がディレクトリ接続に使用する UEM アカウントの制約付き委任を設定します。
  1. Windows Server の ADSI Edit ツールまたは setspn コマンドラインツールを使用して、UEM の次の SPN を Active Directory アカウントに追加します。
     HTTP/*<host_FQDN_or_pool_name>*（HTTP/domain123.example.com など）
     BASPLUGIN111/*<host_FQDN_or_pool_name>*（BASPLUGIN111/domain123.example.com など）
  2. Microsoft Active Directory Users and Computers の Microsoft Active Directory アカウントプロパティの［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］および［**Kerberos** のみを使用］を有効にします。
  3. SPN をサービスリストに追加します。
- 複数の Active Directory 接続用にシングルサインオンを有効にする場合は、Active Directory フォレスト間に信頼関係がないことを確認します。

1. UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. ［設定されたディレクトリ接続］セクションで、Active Directory 接続をクリックします。
3. ［認証］タブで、［**Windows** シングルサインオンを有効にする］チェックボックスをオンにします。
4. ［保存］をクリックします。
5. ［保存］を再度クリックします。
6. ［閉じる］をクリックします。

終了したら：

- UEM インスタンスをホストする各コンピューターで、UEM サービスを再起動します。
- 管理者とユーザーに次の URL を使用するように指示します。
  - 管理コンソール：https://*<host_FQDN_or_pool_name>*:*<port>*/admin/index.jsp?tenant=*<tenant_ID>*&redirect=no
  - UEM Self-Service ：https://*<host_FQDN_or_pool_name>*:*<port>*/mydevice/index.jsp?tenant=*<tenant_ID>*&redirect=no

  メモ：UEM を Entra ID と統合すると、UEM コンソール URL は次のように変更されます（URL の末尾から「&redirect=no」が削除されます）。

  - 管理コンソール：https://<*server_name*>:<*port*>/admin/index.jsp?tenant=<*tenant_ID*>
  - セルフサービスコンソール：https://<*server_name*>:<*port*>/mydevice/index.jsp?tenant=<*tenant_ID*>

  シングルサインオン認証は、他の認証方式よりも優先されます。組織のセキュリティ標準で、管理者またはユーザーが別の認証方法を使用する必要がある場合は、上記の URL の末尾に「?sso=n」を追加することで、シングルサインオン方式を回避できます。
- 管理者および UEM Self-Service ユーザーに、UEM のシングルサインオンをサポートするようにブラウザを設定するよう指示します。
  - Microsoft Edge ：管理コンソールおよび UEM Self-Service の URL は、ローカルイントラネットゾーンに割り当てられる必要があります。統合 Windows 認証を有効にします。
  - Mozilla Firefox ：about:config リストで、https://、<*host_FQDN_or_pool_name*> を「network.negotiate-auth.trusted-uris」設定に追加します。
  - Google Chrome ：管理コンソールおよび UEM Self-Service の URL は、ローカルイントラネットゾーンに割り当てられる必要があります。

証明書ベースのコンソール認証の設定

オンプレミス BlackBerry UEM 環境では、管理者が認証証明書を使用してログインできるように、証明書ベースの認証を設定できます。UEM は、証明書を発行元と照合し、証明書の OCSP または CRL 設定を使用して証明書が有効であることを確認し、証明書が UEM データベース内のユーザーと一致することを確認します。この機能は UEM Cloud ではサポートされていません。

作業を始める前に： 管理者のクライアント証明書およびユーザーのクライアント証明書を .cer または .der 形式で配布する CA 証明書のコピーを取得します。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［証明書ベースのコンソール認証］をクリックします。
2. ［証明書ベースの認証を有効化］チェックボックスをオンにします。
3. ［参照］をクリックして、CA 証明書のファイルに移動します。

   UEM は、その CA によって発行されたすべての証明書を信頼します。追加の証明書をアップロードするには、この手順を繰り返します。
4. 証明書内のユーザープリンシパル名が UEM データベース内のユーザーと一致していることを UEM が確認するように要求するには、［**SAN** のユーザープリンシパル名を確認］チェックボックスをオンにします。

   証明書内のユーザープリンシパル名が既知のユーザーと一致する場合、UEM はユーザーの権限に従ってアクセスを許可します。
5. 証明書内のユーザーメールアドレスが UEM データベース内のユーザーメールアドレスと一致していることを UEM が確認するように要求するには、［メールアドレスを確認］チェックボックスをオンにします。

   証明書内のユーザーメールアドレスが既知のユーザーと一致する場合、UEM はユーザーの権限に従ってアクセスを許可します。［**SAN** のユーザープリンシパル名を確認］と［メールアドレスを確認］の両方を選択した場合、UEM はメールアドレスの前にプリンシパル名を確認し、プリンシパル名が一致する場合はアクセスを許可します。いずれのチェックでも証明書と既知のユーザーとの間に一致が見つからない場合、UEM はアクセスを拒否します。
6. ［保存］をクリックします。

終了したら： ユーザーが Mozilla Firefox を使用して UEM にアクセスする場合、ユーザーはクライアント証明書を Firefox 証明書ストアに追加し、証明書ベースの認証を使用して UEM で認証する必要があります。

管理者ロールの作成および管理

事前に設定されたロールを管理者に割り当てることも、組織の要件に合わせてカスタムロールを作成することもできます。カスタムロールの作成、ロールに関する情報の表示、ロール設定の変更、ロールのランク付け、およびロールの削除を実行するには、セキュリティ管理者である必要があります。

事前設定済みの管理者ロールの権限

BlackBerry UEM には、管理者用の 4 つの事前設定されたロールが含まれます。セキュリティ管理者ロールには、ロールと管理者の作成と管理を含め、すべての権限が含まれています。このロールは編集することも削除することもできません。少なくとも 1 人の管理者にセキュリティ管理者ロールを割り当てる必要があります。エンタープライズ管理者ロール（ロールと管理者の作成と管理を除くすべての権限）、シニアヘルプデスクロール（中間管理タスクを実行する権限）、およびジュニアヘルプデスクロール（基本管理タスクを実行する権限）は、編集または削除できます。次の表には、事前設定済みロールごとに、デフォルトで有効になっている権限が示されています。

一部の権限は、カスタムロールでのみサポートされます。

ロールと管理者

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
ロールの表示	√	NA	NA	NA
ロールの作成および編集	√	NA	NA	NA
ロールの削除	√	NA	NA	NA
ロールのランク付け	√	NA	NA	NA
管理者の作成	√	NA	NA	NA
管理者の削除	√	NA	NA	NA
管理者の非管理属性の編集	√	NA	NA	NA
他の管理者のパスワードの変更	√	NA	NA	NA
管理者のロールメンバーシップの変更	√	NA	NA	NA

ディレクトリアクセス

管理者が検索できる会社のディレクトリを指定できます。

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
会社の全ディレクトリ	√	√	√	√
会社の選択されたディレクトリのみ				

グループ管理

管理者が管理できるグループを指定できます。グループに属さないユーザーを管理するには、管理者がすべてのグループとユーザーを管理する権限を持っている必要があります。

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
すべてのグループとユーザー	√	√	√	√
選択されたグループ				

ユーザーとデバイス

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
ユーザーとアクティブ化されたデバイスを表示	√	√	√	√
ユーザーを作成	√	√	√	
ユーザーを編集	√	√	√	√
ユーザーロールを割り当てる	√	√	√	√
ユーザーを削除	√	√	√	
ユーザーリストをエクスポート	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
アクティベーションパスワードを生成してメールを送信	√	√	√	√
アクティベーションパスワードを生成して複数のユーザーにアクティベーションメールを送信する	√	√	√	
アクティベーションパスワードを指定	√	√	√	√
ユーザーに固有のアクティベーションプロファイルを使用して複数のアクティベーションパスワードを指定する	√	√		
最初のデバイスのアクティベーション後にアクティベーションパスワードを期限切れにするかどうかを指定する	√	√		
ユーザー認証 QR コードとアクセスキーを表示する	√	√		
アカウントパスワードを指定する	√	√	√	√
複数のアカウントパスワードを変更する	√	√	√	
BlackBerry 2FA の事前認証を設定する	√	√		
デバイスの管理	√	√	√	√
仕事用領域を有効化	√	√	√	√
仕事用領域を無効にする	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
仕事用領域をロックする	√	√	√	√
仕事用領域パスワードをリセット	√	√	√	√
デバイスパスワードを指定する	√	√	√	√
デバイスをロックしてメッセージを設定	√	√	√	√
デバイスをロック解除してパスワードをクリア	√	√	√	√
仕事用データのみを削除	√	√	√	√
複数のデバイスから仕事用データのみを削除する	√			
すべてのデバイスデータを削除	√	√	√	√
複数のデバイスからすべてのデバイスデータを削除する	√			
デバイスを削除	√	√		
複数のデバイスを削除する	√			
仕事用パスワードを指定してロック	√	√	√	√
デバイスログを取得	√	√	√	
アクティベーションロックを有効にする	√	√	√	√
アクティベーションロックを無効にする	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
紛失モード	√	√	√	√
紛失モードをオンにする	√	√	√	√
紛失モードをオフにする	√	√	√	√
デバイスを検索	√	√	√	√
デバイスをチェックインする	√	√	√	
デバイスを再起動する	√	√	√	√
iOS ソフトウェアを更新する	√	√	√	√
複数のデバイス上で iOS ソフトウェアを更新する	√			
デバイスをオフにする	√	√	√	√
デバイスの位置情報を表示する	√	√	√	
デバイスの位置履歴を表示する	√	√		
Exchange ゲートキーピング情報を表示する	√	√		
Apple DEP デバイス情報を表示する	√	√	√	√
登録設定を割り当て	√	√		
ワンタイムパスワードトークンを表示する	√	√	√	√
ワンタイムパスワードトークンを割り当てる	√	√		
ユーザーへのメールの送信	√	√	√	

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
アクティベーションロックバイパス履歴を表示する	√	√	√	
BlackBerry Dynamics アプリを管理する	√	√	√	√
アプリをロックする	√	√	√	
アプリのロックを解除する	√	√	√	√
アプリデータを削除する	√	√	√	√
アプリのログを制御する	√	√	√	
Intune アプリを管理する	√	√	√	

専用デバイス

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
共有デバイスグループの設定を表示する	√	√		
共有デバイスグループを作成して編集する	√	√		
共有デバイスグループを削除する	√	√		
公開デバイスグループの設定を表示する	√	√		
公開デバイスグループを作成して編集する	√	√		
公開デバイスグループを削除する	√	√		

グループ

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
グループ設定を表示	√	√	√	√
ユーザーグループを作成して編集	√	√	√	
ユーザーロールを割り当てる	√	√	√	
ユーザーグループに対してユーザーを追加および削除	√	√	√	
ユーザーグループを削除	√	√		
デバイスグループを作成して編集	√	√	√	
デバイスグループを削除	√	√		

ポリシーとプロファイル

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
IT ポリシーを表示する	√	√	√	√
IT ポリシーを作成および編集する	√	√		
IT ポリシーを削除する	√	√		
メールプロファイルを表示する	√	√	√	√
メールプロファイルを作成および編集する	√	√		
メールプロファイルを削除する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
IMAP/POP3 メールプロファイルを表示する	√	√	√	√
IMAP/POP3 メールプロファイルを作成および編集する	√	√		
IMAP/POP3 メールプロファイルを削除する	√	√		
エンタープライズ接続プロファイルを表示する	√	√	√	√
エンタープライズ接続プロファイルを作成および編集する	√	√		
エンタープライズ接続プロファイルを削除する	√	√		
デバイス SR 要件プロファイルを表示する	√	√	√	√
デバイス SR 要件プロファイルを作成および編集する	√	√		
デバイス SR 要件プロファイルを削除する	√	√		
アクティベーションプロファイルを表示する	√	√	√	√
アクティベーションプロファイルを作成および編集する	√	√		
アクティベーションプロファイルを削除する	√	√		
Wi-Fi プロファイルを表示する	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Wi-Fi プロファイルを作成および編集する	√	√		
Wi-Fi プロファイルを削除する	√	√		
VPN プロファイルを表示する	√	√	√	√
VPN プロファイルを作成および編集する	√	√		
VPN プロファイルを削除する	√	√		
コンプライアンスプロファイルを表示する	√	√	√	√
コンプライアンスプロファイルを作成および編集する	√	√		
コンプライアンスプロファイルを削除する	√	√		
デバイスプロファイルを表示する	√	√	√	√
デバイスプロファイルを作成および編集する	√			
デバイスプロファイルを削除する	√	√		
プロキシプロファイルを表示する	√	√	√	√
プロキシプロファイルを作成および編集する	√	√		
プロキシプロファイルを削除する	√	√		
Web コンテンツフィルタープロファイルを表示する	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Web コンテンツフィルタープロファイルを作成および編集する	√	√		
Web コンテンツフィルタープロファイルを削除する	√	√		
FileVault プロファイルを表示する	√	√	√	√
FileVault プロファイルを作成および編集する	√	√		
FileVault プロファイルを削除する	√	√		
位置情報サービスプロファイルを表示する	√	√	√	√
位置情報サービスプロファイルを作成および編集する	√	√		
位置情報サービスプロファイルを削除する	√	√		
アプリロックモードプロファイルを表示する	√	√	√	√
アプリロックモードプロファイルを作成および編集する	√	√		
アプリロックモードプロファイルを削除する	√	√		
シングルサインオンプロファイルを表示する	√	√	√	√
シングルサインオンプロファイルを作成および編集する	√	√		
シングルサインオンプロファイルを削除する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
CA 証明書プロファイルを表示する	√	√	√	√
CA 証明書プロファイルを作成および編集する	√	√		
CA 証明書プロファイルを削除する	√	√		
共有証明書プロファイルを表示する	√	√	√	√
共有証明書プロファイルを作成および編集する	√	√		
共有証明書プロファイルを削除する	√	√		
SCEP プロファイルを表示する	√	√	√	√
SCEP プロファイルを作成および編集	√	√		
SCEP プロファイルを削除する	√	√		
OCSP プロファイルを表示する	√	√	√	√
OCSP プロファイルを作成および編集する	√	√		
OCSP プロファイルを削除する	√	√		
証明書取得プロファイルを表示する	√	√	√	√
証明書取得プロファイルを作成および編集する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
証明書取得プロファイルを削除する	√	√		
CRL プロファイルを表示する	√	√	√	√
CRL プロファイルを作成および編集する	√	√		
CRL プロファイルを削除する	√	√		
管理されているドメインプロファイルを表示する	√	√	√	√
管理されているドメインプロファイルを作成および編集する	√	√		
管理されているドメインプロファイルを削除する	√	√		
ユーザー資格情報プロファイルを表示する	√	√	√	√
ユーザー資格情報プロファイルを作成および編集する	√	√		
ユーザー資格情報プロファイルを削除する	√	√		
カスタムペイロードプロファイルを表示する	√	√	√	√
カスタムペイロードプロファイルを作成および編集する	√	√		
カスタムペイロードプロファイルを削除する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
IT ポリシーとプロファイルをユーザーに割り当て	√	√	√	√
IT ポリシーとプロファイルをユーザーグループに割り当て	√	√	√	√
IT ポリシーとプロファイルをデバイスグループに割り当て	√	√	√	√
IT ポリシーとプロファイルを共有デバイスグループに割り当てる	√	√		
IT ポリシーとプロファイルを公開デバイスグループに割り当てる	√	√		
IT ポリシーとプロファイルをランク付け	√	√		
CardDAV プロファイルを表示する	√	√	√	√
CardDAV プロファイルを作成および編集する	√	√		
CardDAV プロファイルを削除する	√	√		
CalDAV プロファイルを表示する	√	√	√	√
CalDAV プロファイルを作成および編集する	√	√		
CalDAV プロファイルを削除する	√	√		
AirPrint プロファイルを表示する	√	√	√	√
AirPrint プロファイルを作成および編集する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
AirPrint プロファイルを削除する	√	√		
ネットワーク使用プロファイルを表示	√	√	√	√
ネットワーク使用プロファイルを作成および編集	√	√		
ネットワーク使用プロファイルを削除	√	√		
AirPlay プロファイルを表示する	√	√	√	√
AirPlay プロファイルを作成および編集する	√	√		
AirPlay プロファイルを削除する	√	√		
Enterprise Management Agent プロファイルを表示する	√	√	√	√
Enterprise Management Agent プロファイルを作成および編集する	√	√		
Enterprise Management Agent プロファイルを削除する	√	√		
BlackBerry Dynamics コンプライアンスプロファイルを表示する	√	√	√	√
BlackBerry Dynamics コンプライアンスプロファイルを削除する	√	√		
BlackBerry Dynamics プロファイルを表示する	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
BlackBerry Dynamics プロファイルを作成および編集する	√	√		
BlackBerry Dynamics プロファイルを削除する	√	√		
BlackBerry Dynamics 接続プロファイルを表示する	√	√	√	√
BlackBerry Dynamics 接続プロファイルを作成および編集する	√	√		
BlackBerry Dynamics 接続プロファイルを削除する	√	√		
サイレントプロファイルを表示する	√	√	√	√
サイレントプロファイルを作成および編集する	√	√		
サイレントプロファイルを削除する	√	√		
BlackBerry 2FA プロファイルを表示する	√	√	√	√
BlackBerry 2FA プロファイルを作成および編集する	√	√		
BlackBerry 2FA プロファイルを削除する	√	√		
Windows 情報保護プロファイルを表示する	√	√	√	√
Windows 情報保護プロファイルを作成および編集する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Windows 情報保護プロファイルを削除する	√	√		
アプリごとの通知プロファイルを表示する	√	√	√	√
アプリごとの通知プロファイルを作成および編集する	√	√		
アプリごとの通知プロファイルを削除する	√	√		
ゲートキーピングプロファイルを表示する	√	√	√	√
ゲートキーピングプロファイルを作成および編集する	√	√		
ゲートキーピングプロファイルを削除する	√	√		
Microsoft Intune アプリ保護プロファイルを表示する	√	√	√	√
Microsoft Intune アプリ保護プロファイルを作成および編集する	√	√		
Microsoft Intune アプリ保護プロファイルを削除する	√	√		
ホームスクリーンレイアウトプロファイルを表示する	√	√	√	√
ホームスクリーンレイアウトプロファイルを作成および編集する	√	√		
ホームスクリーンレイアウトプロファイルを削除する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Enterprise Identity 認証ポリシーを表示する	√	√		
Enterprise Identity 認証ポリシーを作成および編集する	√	√		
Enterprise Identity 認証ポリシーを削除する	√	√		
Enterprise Identity 認証ポリシーをユーザーおよびグループに割り当てる	√	√		

アプリ

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
アプリおよびアプリグループを表示	√	√	√	√
アプリおよびアプリグループを作成して編集	√	√		
アプリおよびアプリグループを削除	√	√		
アプリデータをエクスポートする	√	√	√	√
アプリおよびアプリグループをユーザーに割り当て	√	√	√	√
アプリおよびアプリグループをユーザーグループに割り当て	√	√	√	√
アプリおよびアプリグループをデバイスグループに割り当て	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
アプリおよびアプリグループを共有デバイスグループに割り当てる	√	√		
アプリおよびアプリグループを公開デバイスグループに割り当てる	√	√		
アプリのレーティングとレビューの設定を編集する	√	√		
アプリのレーティングとレビューの削除	√	√	√	√
アプリのインストールランキングを表示する	√	√	√	√
アプリのインストールランキングを編集する	√	√		
アプリライセンスを表示する	√	√	√	√
アプリライセンスを作成する	√	√		
アプリライセンスを編集	√	√		
アプリライセンスを削除	√	√		
アプリライセンスをアプリまたはアプリグループに割り当てる	√	√	√	√

制限されたアプリ

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
制限されたアプリを表示	√	√	√	√

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
制限されたアプリを作成	√	√		
制限されたアプリを削除	√	√		

個人用アプリ

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
個人用アプリを表示	√	√		

設定

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
全般設定を表示	√	√	√	√
アクティベーションのデフォルトを編集	√	√		
メールテンプレートを作成および編集する	√	√		
メールテンプレートを削除する	√	√		
コンソール設定を編集する	√	√		
自動メールの言語を編集する	√	√		
セルフサービスコンソール設定を編集	√	√		
仕事用領域のバックアップおよび復元設定を作成する [1]	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
仕事用領域のバックアップおよび復元設定を削除する [1]	√	√		
デフォルトの変数を編集する [1]	√	√		
ログイン通知を編集する [1]	√	√		
カスタム変数を編集	√	√		
組織の通知を編集する	√	√		
メールドメインを編集する	√	√		
位置情報サービス設定を編集する	√	√		
カスタマイズコンソール設定を編集する	√	√		
コマンドの有効期限の削除設定を編集する	√	√		
立証設定を編集する	√	√		
証明書設定を編集する	√	√		
イベント通知を作成および編集する	√	√		
イベント通知を削除する	√	√		
デバイスサポートメッセージを編集する	√	√		
証明書ベースの認証設定を編集する [1]	√			
パブリック Web サービスのアクセス設定を編集する	√			

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
アプリ管理を表示	√	√	√	√
仕事用 BlackBerry World を編集	√	√		
内部アプリのストレージを編集する [1]	√	√		
iOS 用 Work Apps を編集	√	√		
Windows 10 アプリを編集する	√	√		
アプリのレーティングおよびレビューのデフォルト設定を編集する	√	√		
外部統合設定を表示	√	√	√	√
Apple プッシュ通知を編集する	√	√		
SMTP サーバー設定を編集する [1]	√	√		
Apple DEP 設定の編集	√	√		
BlackBerry 2FA サーバー設定を編集する	√	√		
BlackBerry Connectivity Node 設定を編集する [2]	√	√		
ワンタイムパスワードトークンを表示する	√	√	√	√
ワンタイムパスワードトークンを作成および編集する	√	√		
会社のディレクトリ設定を編集する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Microsoft Intune 設定を編集する	√	√		
Microsoft Exchange ゲートキーピング設定を編集する	√	√		
Android 仕事用プロファイル設定を編集する	√	√		
認証局設定を編集	√	√		
Samsung Knox 一括登録設定を編集する	√	√		
信頼済み証明書を表示する	√	√		
信頼済み証明書を追加する	√	√		
信頼済み証明書を削除する	√	√		
BlackBerry Connectivity Node サーバーを表示する	√	√		
BlackBerry Connectivity Node サーバーを作成および編集する	√	√		
BlackBerry Connectivity Node サーバーを削除する	√	√		
BlackBerry Secure Gateway 設定を表示する	√	√		
BlackBerry Secure Gateway 設定を編集する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
管理者ユーザーおよびロールを表示	√	√	√	√
ライセンスの概要を表示する	√	√	√	√
ライセンス設定を編集	√	√		
移行設定を表示	√	√		
移行設定を編集	√	√		
インフラストラクチャ設定を表示する	√	√	√	
ログ設定を編集する [1]	√	√		
サーバー側のプロキシ設定を編集する [1]	√	√		
サーバーを表示する [1]	√	√		
サーバーを編集する [1]	√	√		
サーバーを削除する [1]	√	√		
サーバーを管理する [1]	√	√		
監査設定を表示する [1]	√	√		
監査設定を編集してデータを消去する [1]	√	√		
BlackBerry Secure Connect Plus 設定を表示する [1]	√	√		
BlackBerry Secure Connect Plus 設定を編集する [1]	√	√		
サーバー証明書を表示する [1]	√	√		
サーバー証明書を更新する [1]	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
BlackBerry Control 設定を表示する	√	√	√	√
BlackBerry Control 設定を編集する	√	√		
BlackBerry Dynamics NOC プロキシサーバー設定を表示する [1]	√	√	√	√
BlackBerry Dynamics NOC プロキシサーバー設定を編集する [1]	√	√	√	√
SNMP 設定を編集する [1]	√	√		
IT ポリシーパックとデバイスメタデータをインポートする [1]	√			
Collaboration Service 設定を表示する [1]	√	√	√	√
Collaboration Service 設定を編集する [1]	√	√		
BlackBerry Dynamics 設定を表示する	√	√	√	√
BlackBerry Dynamics アプリサービスを表示する	√	√		
BlackBerry Dynamics アプリサービスを編集する	√			
BlackBerry Dynamics アプリサービスを作成する	√			
BlackBerry Dynamics アプリサービスを削除する	√			

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
BlackBerry Dynamics サーバープロパティを表示する [1]	√	√		
BlackBerry Dynamics サーバープロパティを編集する [1]	√			
BlackBerry Dynamics Direct Connect 設定を表示する	√	√		
BlackBerry Dynamics Direct Connect 設定を編集する	√			
BlackBerry Dynamics サーバークラスター設定を表示する [1]	√	√		
BlackBerry Dynamics サーバークラスター設定を編集する [1]	√			
BlackBerry Dynamics レポートを表示する	√	√	√	
BlackBerry Dynamics 通信設定を表示する [1]	√	√	√	
BlackBerry Dynamics 通信設定を編集する [1]	√			
BEMS メール設定を表示する [2]	√	√		
BEMS メール設定を編集する [2]	√			
BEMS 文書設定を表示する [2]	√	√		
BEMS 文書設定を編集する [2]	√			
Enterprise Identity 設定を表示する	√	√		

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
Enterprise Identity エンタープライズ設定を表示する	√	√		
Enterprise Identity エンタープライズ設定を編集する	√	√		
Enterprise Identity サービス設定を表示する	√	√		
Enterprise Identity サービス設定を編集する	√	√		

[1] オンプレミス環境のみ

[2] クラウド環境のみ

ダッシュボード

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
ダッシュボードを表示	√	√	√	√

監査

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
システム監査ログを表示する[1]	√	√		
デバイスパフォーマンスログを表示する [1]	√	√		

[1] オンプレミス環境のみ

ワークスペース

権限	セキュリティ管理者	エンタープライズ管理者	シニアヘルプデスク	ジュニアヘルプデスク
組織管理者	√			
ヘルプデスク管理者	√			
監査ヘルプデスク管理者	√			

カスタム管理者ロールの作成

事前設定済みのロールが組織の要件を満たしていない場合は、カスタム管理者ロールを作成できます。また、管理タスクを定義されたユーザーグループのリストに限定するためにカスタムロールを作成することもできます。たとえば、権限をトレーニング用のユーザーグループのみに限定した新しい管理者のロールを作成できます。

作業を始める前に：

- カスタムロールを作成するには、セキュリティ管理者である必要があります。
- 事前設定済みの管理者ロールの権限 ロールを確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［管理者］ > ［ロール］をクリックします。
2. をクリックします。
3. ロールの名前と説明を入力します。
4. 別のロールから権限をコピーするには、［ロールからコピーする権限］ドロップダウンリストでロールをクリックします。
5. 次の操作のいずれかを実行します。

タスク	手順
このロールの管理者に会社の全ディレクトリの検索を許可します。	［会社の全ディレクトリ］オプションを選択します。
このロールの管理者に選択した会社のディレクトリの検索を許可します。	a. ［会社の選択されたディレクトリのみ］オプションを選択します。 b. ［ディレクトリを選択］をクリックします。 c. 1 つまたは複数のディレクトリを選択し、 をクリックします。 d. ［保存］をクリックします。

6. 次の操作のいずれかを実行します。

タスク	手順
このロールの管理者にすべてのユーザーとグループの管理を許可します。	［すべてのグループとユーザー］オプションを選択します。
このロールの管理者に選択したグループの管理を許可します。	**a.** ［選択されたグループのみ］オプションを選択します。 **b.** ［グループを選択］をクリックします。 **c.** 1 つまたは複数のグループを選択し、➡ をクリックします。 **d.** ［保存］をクリックします。

7. このロールの管理者の権限を設定します。
8. ［保存］をクリックします。

終了したら： ロールのランク付け、ロール設定の変更、またはロールの削除については、「管理者ロールの管理」を参照してください。

管理者ロールの管理

管理者ロールを作成したら、ロールのランク付け、ロールの権限の変更、またはロールの削除を行うことができます。管理者が、異なるロールを持つ複数のユーザーグループのメンバである場合、BlackBerry UEM はランク付けを使用して、管理者に割り当てるロールを決定します。ユーザーアカウントに直接割り当てられたロールは、ユーザーグループに割り当てられたロールより優先されます。管理者が、異なるロールを持つ複数のユーザーグループのメンバーである場合、UEM はランキングが最も高いロールを割り当てます。

作業を始める前に： 管理者ロールを管理するには、セキュリティ管理者である必要があります。

1. 管理コンソールのメニューバーで、［設定］ > ［管理者］ > ［ロール］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
ロールをランク付けします。	**a.** 矢印を使用して、ロールのランクを変更します。 **b.** ［保存］をクリックします。
ロールの設定を変更します。	**a.** 変更するロールの名前をクリックします。 **b.** ［編集］をクリックします。 **c.** 変更を加えます。 **d.** ［保存］をクリックします。
ロールを削除します。	**a.** 削除するロールの名前をクリックします。 **b.** 🗑 をクリックします。

管理者の作成

管理者ロールをユーザーアカウントまたはユーザーグループに追加することで、管理者を作成できます。ディレクトリにリンクされたグループまたはローカルグループをユーザーグループにすることができます。1 つのロールを 1 人のユーザーに追加することも、1 つのロールをユーザーが属する各グループに追加することもできますが、BlackBerry UEM は、1 つのロールだけをユーザーに割り当てます。

ロールがユーザーアカウントまたはユーザーグループに割り当てられると、UEM は管理者にユーザー名と管理コンソールへのリンクを含むメールを送信します。また、UEM は、管理コンソールのパスワードが記載された別のメールも管理者に送信します。管理者のアカウントパスワードがない場合は、UEM によって一時パスワードが生成され、管理者に送信されます。

作業を始める前に：

- 管理者を作成するには、セキュリティ管理者である必要があります。
- 必要に応じて、カスタム管理者ロールの作成。

1. 管理コンソールのメニューバーで、［設定］ > ［管理者］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
ユーザーアカウントにロールを割り当てる。	a. ［ユーザー］をクリックします。 b. をクリックします。 c. ロールを割り当てるユーザーアカウントの名前をクリックします。
ユーザーグループにロールを割り当てる。	a. ［グループ］をクリックします。 b. をクリックします。 c. ロールを割り当てるユーザーグループの名前をクリックします。

3. ［ロール］ドロップダウンリストで、割り当てるロールをクリックします。
4. ［保存］をクリックします。

終了したら：

- 割り当てられたロールを変更するには、ユーザーアカウントまたはユーザーグループの名前をクリックし、割り当てるロールをクリックして、［保存］をクリックします。
- 管理者を削除するには、そのロールを削除するユーザーアカウントまたはユーザーグループを選択して、 > ［削除］をクリックします。

ユーザーアカウントの作成と管理

ユーザーアカウントを直接 BlackBerry UEM で作成することができます。また、UEM を会社のディレクトリに接続している場合は、そのディレクトリからユーザーアカウントを追加できます。また、.csv ファイルを使用して、複数のユーザーアカウントを同時に UEM へ追加することもできます。

ユーザーアカウントを作成した後は、ユーザーのサービスを有効にしたり、ユーザーをグループに追加したり、UEM でユーザーのデバイスを有効にしたり、ユーザーに通信を送信したりできます。

ユーザーアカウントの作成

作業を始める前に：

- ディレクトリユーザーを追加する場合は、BlackBerry UEM が会社のディレクトリに接続されていることを確認します。UEM を会社のディレクトリに接続して、ディレクトリにリンクされたグループを有効にする方法の詳細については、設定関連の資料で「会社のディレクトリへの接続」を参照してください。
- ユーザーのために BlackBerry Workspaces サービスを有効にする場合、UEM 用の Workspaces プラグインが環境内の UEM の各インスタンスにインストールされてい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、［ユーザー］ > ［管理対象デバイス］ > ［ユーザーを追加］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
ディレクトリユーザーを追加します。	a. ［会社のディレクトリ］タブで、追加するディレクトリユーザーを検索します。姓、名、表示名、ユーザー名、またはメールアドレスで検索できます。 b. 検索結果で、ユーザーアカウントを選択します。
ローカルユーザーを追加します。	a. ［ローカル］タブで、ユーザーの名と姓を指定します。 b. 必要に応じて、ユーザーの表示名を編集します。 c. ［ユーザー名］フィールドに固有のユーザー名を入力します。 d. ［メールアドレス］フィールドに、ユーザーアカウントの連絡先メールアドレスを入力します。ユーザーアカウントのメールアドレスは、Workspaces またはデバイス管理などのサービスを有効にする場合に必要です。 e. オプションで［その他のユーザー詳細］をクリックして、必要に応じてこのフィールドに入力します。
BlackBerry Online Account ユーザーを追加します（UEM Cloud のみ）。	a. ［非ディレクトリ］タブで、ユーザーの名と姓を指定します。 b. 必要に応じて、ユーザーの表示名を編集します。 c. ［メールアドレス］フィールドに、ユーザーアカウントの連絡先メールアドレスを入力します。ユーザーアカウントのメールアドレスは、Workspaces またはデバイス管理などのサービスを有効にする場合に必要です。 d. オプションで［その他のユーザー詳細］をクリックして、必要に応じてこのフィールドに入力します。

3. ローカルグループが UEM に存在し、ユーザーアカウントをグループに追加する場合は、［利用可能なグループ］リストで、1 つ以上のグループをクリックし、➡ をクリックします。

ユーザーアカウントを作成する場合は、ローカルグループのみに追加できます。ユーザーアカウントがディレクトリにリンクされたグループのメンバーである場合は、UEM と会社のディレクトリとの同期が実行されたときに、自動的にそのグループに関連付けられます。

4. Cloud 環境では、［**UEM Self-Service**］の下で、［**BlackBerry Online Account**］または［ローカル **UEM** ユーザーアカウント］を選択します。［ローカル UEM ユーザーアカウント］を選択した場合は、BlackBerry UEM Self-Service のパスワードを作成します。管理ロールが割り当てられているユーザーは、パスワードを使用して管理コンソールにアクセスすることもできます。
5. オンプレミス環境で、ローカルユーザーを追加する場合は、［パスワード］フィールドで UEM Self-Service のパスワードを作成します。管理ロールが割り当てられているユーザーは、パスワードを使用して管理コンソールにアクセスすることもできます。
6. ［有効にされたサービス］セクションで、［デバイス管理のユーザーを有効にする］チェックボックスを選択します。
7. ドメインに Workspaces plug-in for UEM がインストールされている場合、Workspaces サービスを有効にするには、次の手順を実行します。
   a) ［**BlackBerry Workspaces**］セクションで、［**BlackBerry Workspaces** を有効にする］チェックボックスをオンにします。Workspaces サービスが有効になっているユーザーには、デフォルトでビジターロールが割り当てられます。
   b) 1 つ以上のユーザーロールを選択し、➡ をクリックします。
8. 次の操作のいずれかを実行します。

タスク	手順
現在割り当てられているアクティベーションプロファイルで、ユーザー自身にデバイスのアクティベーションをしてもらう	**a.** ［アクティベーションオプション］ドロップダウンリストで、［デフォルトのデバイスアクティベーション］を選択します。 **b.** ［アクティベーションパスワード］ドロップダウンリストで、パスワードを設定するかパスワードを自動生成するかを選択します。 **c.** オプションで、アクティベーション期間の有効期限を変更します。 **d.** 1 回のデバイスアクティベーションに対してのみアクティベーションパスワードを有効にする場合は、［最初のデバイスがアクティブになったら、アクティベーションの有効期限が切れる］を選択します。 **e.** ［アクティベーションメールテンプレート］ドロップダウンリストで、アクティベーションメールに使用するテンプレートを選択します。
アクティベーションパスワードと特定のアクティベーションプロファイルをペアリングする	**a.** ［アクティベーションオプション］ドロップダウンリストで、［指定されたアクティベーションプロファイルでデバイスアクティベーション］をクリックします。 **b.** ［アクティベーションプロファイル］ドロップダウンリストで、パスワードとペアリングするアクティベーションプロファイルを選択します。 **c.** ［アクティベーションパスワード］ドロップダウンリストで、パスワードを設定するかパスワードを自動生成するかを選択します。 **d.** オプションで、アクティベーション期間の有効期限を変更します。 **e.** 1 回のデバイスアクティベーションに対してのみアクティベーションパスワードを有効にする場合は、［最初のデバイスがアクティブになったら、アクティベーションの有効期限が切れる］を選択します。 **f.** ［アクティベーションメールテンプレート］ドロップダウンリストで、アクティベーションメールに使用するテンプレートを選択します。

タスク	手順
BlackBerry Dynamics アプリに限定してユーザーにアクティベーションを許可する	**a.** ［アクティベーションオプション］ドロップダウンリストで、［**BlackBerry Dynamics** アクセスキー生成］を選択します。 **b.** ［生成するアクセスキーの数］ドロップダウンリストで、キーの数を選択します。BlackBerry Dynamics アプリをアクティブにする場合、各キーを 1 回のみ使用できます。 **c.** アクセスキーの有効期間を日数で選択します。 **d.** ［アクティベーションメールテンプレート］ドロップダウンリストで、アクティベーションメールに使用するテンプレートを選択します。
ユーザーを UEM のみに追加する	［アクティベーションオプション］ドロップダウンリストで、［設定しない］を選択します。

9. カスタム変数を使用する場合は、［カスタム変数］を開き、定義した変数に適した値を指定します。

10.次の操作のいずれかを実行します。

- ユーザーアカウントを保存するには、［保存］をクリックします。
- ユーザーアカウントを保存して、別のユーザーアカウントを作成するには、［保存して新規に作成］をクリックします。

.csv ファイルからのユーザーアカウントの作成

複数のユーザーアカウントを 1 つの .csv ファイルから BlackBerry UEM にインポートして、複数のユーザーアカウントを同時に作成できます。管理コンソールからダウンロードできるサンプル .csv ファイル（［ユーザー］ > ［すべてのユーザー］ > ［ユーザーを追加］ > ［インポート］ > ［サンプル .csv ファイルをダウンロード］）を使用して、.csv ファイルを手動で作成できます。

要件に応じて、.csv ファイルに次の列を含めることで、ユーザーアカウントのグループメンバーシップやアクティベーション設定を指定できます。

列見出し	説明
グループメンバーシップ	1 つ以上のユーザーグループを各ユーザーアカウントに割り当てます。 複数のユーザーグループを区切るには、セミコロン（;）を使用します。 ［グループメンバーシップ］列を含めないと、ファイルのインポート時に、インポートされたすべてのユーザーアカウントを追加するグループを選択するためのオプションが表示されます。
MDM（BlackBerry UEM）	ユーザーを MDM で有効にするかどうかを指定します。MDM でユーザーを有効にするには、「Enabled」と入力します。
アクティベーションパスワード	アクティベーションパスワードを指定します。 ［アクティベーションパスワードの生成］の値が［手動］に設定されている場合、この値は必要です。

列見出し	説明
アクティベーションテンプレート	ユーザーに送信するアクティベーションメールテンプレートの名前を指定します。名前を指定しない場合は、デフォルトのアクティベーションメールテンプレートが使用されます。
アクティベーションパスワードの有効期限	アクティベーションパスワードの有効期限が切れるまでの時間を秒単位で指定します。
アクティベーションパスワードの生成	次のいずれかを指定します。 • 自動：アクティベーションパスワードは自動的に作成され、ユーザーに送信されます。（デフォルト） • 手動：アクティベーションパスワードは、［アクティベーションパスワード］列に設定されます。 • 無視：アクティベーションパスワードは生成されません。
アクティベーションメールを送信	次のいずれかを指定します。 • True：アクティベーションメールがユーザーに送信されます。 • False：アクティベーションメールはユーザーに送信されません。 ［アクティベーションパスワードの生成］が［自動］に設定されている場合は、この列の値に関係なくアクティベーションメールはユーザーに送信されます。［アクティベーションパスワードの生成］の値が［手動］で、この値が空の場合、デフォルトは［True］です。［アクティベーションパスワードの生成］の値が［無視］の場合、ユーザーはセルフサービスのアクティベーションメールを受信しません。
ユーザーのタイプ	.csv ファイルにローカルユーザーアカウントとディレクトリユーザーアカウントの両方が含まれる場合、この列は常に必須です。次のいずれかを指定します。 • L：ローカルユーザーアカウント • D：ディレクトリユーザーアカウント
ディレクトリ UID	この列は、ディレクトリユーザーアカウントのメールアドレスを入力する代わりに使用します。デフォルトでは、ディレクトリユーザーアカウントの検証にはメールアドレスが使用されますが、代わりにディレクトリ UID を使用するように指定できます。ユーザーアカウントをディレクトリ UID に対して検証できない場合は、エラーがレポートされます。 いずれかのユーザーのディレクトリ UID 値を含める場合は、列の見出しにディレクトリ UID が含まれており、.csv ファイルのすべての行にディレクトリ UID が含まれているか、ディレクトリ UID 列に空のプレースホルダ（,）が含まれている必要があります。

.csv ファイルを使用した UEM へのユーザーアカウントの追加

作業を始める前に：

- .csv ファイルを準備します。詳細については、「.csv ファイルからのユーザーアカウントの作成」を参照してください。

- .csv ファイルにディレクトリユーザーアカウントが含まれる場合は、BlackBerry UEM が会社のディレクトリに接続されてい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、［ユーザー］をクリックします。
2. ［すべてのユーザー］または［管理されているデバイス］タブで、［ユーザーを追加］をクリックします。
3. ［インポート］タブで、［参照］をクリックし て.csv ファイルに移動します。
4. ［ロード］をクリックします。
5. .csv ファイルで［グループメンバーシップ］列が使用されておらず、ユーザーアカウントをグループに追加する場合は、［利用可能なグループ］リストで、1 つ以上のグループを選択し、➡ をクリックします。［次へ］をクリックします。

   .csv ファイルをインポートする場合は、すべてのユーザーアカウントが、選択したローカルグループに追加されます。ユーザーアカウントがディレクトリにリンクされたグループのメンバーである場合は、UEM と会社のディレクトリとの同期が実行されたときに、自動的にそのグループに関連付けられます。
6. ユーザーアカウントのリストを調べ、次のいずれかを実行します。
   - 無効なディレクトリユーザーアカウントのエラーを修正するには、［キャンセル］をクリックし、ファイルを修正して、再度アップロードします。
   - 有効なユーザーアカウントを追加するには、［インポート］をクリックします。無効なディレクトリユーザーアカウントは無視されます。

ユーザーのサービスの有効化

1 つ以上のサービス（たとえば、Workspaces、BBM Enterprise、または Enterprise Identity）に対して BlackBerry UEM を有効にした場合、ユーザーにサービスを有効にできます。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［すべてのユーザー］をクリックします。
2. ユーザーアカウントを検索してクリックします。
3. ユーザーの詳細ページで、使用可能なサービスがユーザー名の下にリストされます。
4. サービスが現在有効になっていない場合は、［+］アイコンで表示されます。［+］をクリックして、サービスを追加します。
5. 必要に応じてサービスを設定し、保存します。

終了したら： ユーザーからサービスを削除する場合は、⛔ をクリックします。削除するサービスで ⛔ をクリックします。MDM コントロールを削除するには、ユーザーからアクティブなデバイスを削除する必要があります。Enterprise Identity サービスを削除するには、ユーザーから Enterprise Identity のすべての割り当てを削除する必要があります。

ユーザーグループへのユーザーの追加

ユーザーグループの詳細については、「ユーザーグループの作成と管理」を参照してください。ユーザーのメンバーシップをディレクトリリンクグループに変更することはできません。

作業を始める前に： 管理者ロールが割り当てられるユーザーをユーザーグループに追加するには、セキュリティ管理者である必要があります。

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. ユーザーグループに追加するユーザーの横のチェックボックスを選択します。

3. をクリックします。
4. ［利用可能なグループ］リストで、1 つ以上のグループを選択し、 をクリックします。
5. ［保存］をクリックします。

終了したら：

- ユーザーが属するユーザーグループを変更するには、メンバーシップを変更するユーザーアカウントの名前をクリックします。 をクリックし、［グループメンバーシップ］セクションで、左矢印と右矢印を使用してユーザーをグループに追加するか、グループからユーザーを削除します。
- ユーザーグループから複数のユーザーを削除するには、メニューバーで［グループ］をクリックします。ユーザーを削除するユーザーグループをクリックします。削除するユーザーを選択して、 をクリックします。

ユーザーアカウントの管理

作業を始める前に： ユーザーアカウントの作成。

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. 次の操作のいずれかを実行します。
   - 個々のユーザーを管理するには、ユーザーアカウントを検索してクリックし、次の手順に進みます。
   - 複数のユーザーアカウントに対して一度にアクションを実行するには、管理する各ユーザーアカウントの横にあるチェックボックスをオンにします。ユーザーリストの上にあるアクション（たとえば、選択したユーザーアカウントをユーザーグループに追加できます）をクリックし、画面の指示に従います。
3. 次の操作のいずれかを実行します。

タスク	手順
ユーザーの情報を編集します。	a. をクリックします。 b. ユーザーのアカウントを変更します。 c. ［保存］をクリックします。
ユーザーのアカウントにメモを追加します。	a. をクリックします。 b. メモを入力します。入力したメモは、自動的に保存され、個々のデバイスではなく、ユーザーアカウントと共に保存されます。
ユーザーへの IT ポリシー、プロファイル、アプリ、またはアプリグループの割り当て	a. 適切なセクションで、 をクリックします。 b. 割り当てる IT ポリシー、プロファイル、アプリ、またはアプリグループを選択します。プロンプトに従って適切な設定を選択し、割り当てを完了します。 c. ユーザーから IT ポリシー、プロファイル、アプリ、またはアプリグループを削除するには、削除するプロパティの横にある をクリックします。
ディレクトリユーザーの情報の同期	をクリックします。

タスク	手順
ユーザーアカウントを削除します。	**a.** をクリックします。 **b.** ［削除］をクリックします。

ユーザーへの通信の送信

BlackBerry UEM Self-Service パスワードを含むメールメッセージを含むメールを、1 人以上のユーザーに送信できます。パスワードを選択すると、パスワードはランダムに生成され、そのパスワードを記載したメールメッセージが各ユーザーに送信されます。UEM オンプレミスでは、SMTP サーバー設定でメールの送信元のメールアドレスを設定できます。

作業を始める前に： メールメッセージを送信するユーザーは、ユーザーアカウントに関連付けられたメールアドレスを持っている必要があります。

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. メッセージを送信する各ユーザーの横にあるチェックボックスをオンにします。
3. 次の操作のいずれかを実行します。

タスク	手順
ユーザーにメールを送信します。	**a.** をクリックします。 **b.** 必要に応じて、自分または他のユーザーにメールをコピーするには、［**CC**］をクリックして 1 つまたは複数のメールアドレスを入力します。アドレスはカンマまたはセミコロンで区切ります。
ユーザーに BlackBerry UEM Self-Service パスワードを送信します。	**a.** をクリックします。 **b.** ［続行］をクリックします。

ユーザーグループの作成と管理

ユーザーグループは共通のプロパティを共有する関連するユーザーの集合です。グループとしてユーザーを管理した方が、同時にグループのすべてのメンバーに対してプロパティを追加、変更、または削除できるため、個々のユーザーを管理するより効率的です。ユーザーは、一度に複数のグループに所属できます。ユーザーグループを作成および管理する場合は、管理コンソールで IT ポリシー、プロファイル、およびアプリを割り当てることができます。1 つのグループを別のグループのメンバとして定義することもできます。

2 種類のユーザーグループを作成できます。

- ディレクトリにリンクされたグループ：これらのグループは、会社のディレクトリ内のグループにリンクします。ディレクトリのユーザーアカウントのみがディレクトリにリンクされたグループのメンバーになることができます。
- ローカルグループ：これらのグループは、BlackBerry UEM で作成および維持され、それらにローカルユーザーアカウントとディレクトリユーザーアカウントの両方を割り当てることができます。

ディレクトリにリンクされたグループの場合、UEM はグループのメンバーシップを関連付けられている会社のディレクトリグループと定期的に同期します。会社のディレクトリに対して追加または削除されたユーザーは、ディレクトリにリンクされたグループに対して追加または削除されます。ディレクトリにリンクされたグループにリンクした会社のディレクトリグループにユーザーを追加すると、そのユーザーには、グループに割り当てられたプロパティが割り当てられます。ユーザーがディレクトリリンクグループから削除されると、プロパティはユーザーから削除されます。

ディレクトリにリンクされている各グループは、単一の会社ディレクトリにリンクできます。たとえば、UEM に 2 つの Microsoft Active Directory 接続（A および B）があり、接続 A にリンクしたディレクトリにリンクされたグループを作成した場合、接続 A からのディレクトリグループのみにリンクできます。他のすべてのディレクトリ接続について、ディレクトリにリンクされたグループを新たに作成する必要があります。

ディレクトリにリンクされたグループを同期しても、UEM でユーザーが追加または削除されることはありません。新しい会社のディレクトリユーザーが作成されたときに UEM でユーザーアカウントの作成を許可するには、オンボーディングを有効にする必要があります。

ディレクトリにリンクされたグループの作成

会社のディレクトリ内のグループにリンクするユーザーグループを作成できます。BlackBerry UEM は、定期的に、ディレクトリにリンクされたグループのメンバーシップを、それに関連付けられた会社のディレクトリグループと自動的に同期します。会社のディレクトリグループに対してユーザーが追加または削除された場合、ディレクトリにリンクされたグループに対して追加または削除されます。ディレクトリリンクグループに割り当てるプロファイル、ポリシー、およびアプリは、そのグループ内のユーザーに割り当てられます。ユーザーがグループから削除されると、それらのプロパティは削除されます。

作業を始める前に： ディレクトリにリンクされたグループを有効にします。

1. 管理コンソールのメニューバーで、［グループ］ > ［ユーザー］をクリックします。
2. をクリックします。
3. グループ名を入力します。
4. ［リンクされたディレクトリグループ］セクションで、次の操作を実行します。
   a) ＋をクリックします。
   b) リンク先となる会社のディレクトリグループの名前または名前の一部を入力します。

c) 複数の会社のディレクトリ接続がある場合は、検索する接続を選択します。この選択を行った後、ディレクトリにリンクされたグループは、選択した接続に、永続的に関連付けられます。
d) 🔍 をクリックします。
e) 会社のディレクトリグループを選択します。
f) ［追加］をクリックします。
g) 必要に応じて、ディレクトリ設定でネストされたグループの数を制御できるようにするには、［ネストされたグループをリンク］チェックボックスをオンにします。ネストされたすべてのグループにリンクするには、チェックボックスをオフのままにします。
h) 追加のグループをリンクするには、これらの手順を繰り返します。

5. 次の操作のいずれかを実行します。

タスク	手順
ディレクトリにリンクされたグループにユーザーロールを割り当てます。	**a.** ［ユーザーロール］セクションで ＋ をクリックします。 **b.** ドロップダウンリストで、グループに割り当てるユーザーロールの名前をクリックします。 **c.** ［追加］をクリックします。
ディレクトリにリンクされたグループに IT ポリシーまたはプロファイルを割り当てます。	**a.** ［**IT** ポリシーおよびプロファイル］セクションで ＋ をクリックします。 **b.** ［**IT** ポリシー］またはプロファイルの種類をクリックします。 **c.** ドロップダウンリストで、グループに割り当てる IT ポリシーまたはプロファイルの名前をクリックします。 **d.** ［割り当て］をクリックします。
ディレクトリにリンクされたグループにアプリを割り当てます。	**a.** ［割り当てられたアプリ］セクションで ＋ をクリックします。 **b.** 割り当てるアプリを検索して選択します。 **c.** ［次へ］をクリックします。 **d.** ［種別］ドロップダウンリストで、次のいずれかを実行します。 • アプリをデバイスへ自動的にインストールし、ユーザーがこのアプリをアンインストールできないようにするには、［必須］を選択します。 • ユーザーにアプリのインストールを要求し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしで必須］を選択します。 • ユーザーにアプリのインストールおよびアンインストールを許可するには、［オプション］を選択します。 • ユーザーにアプリのインストールと削除を許可し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしでオプション］を選択します。 **e.** iOS デバイスの場合、アプリごとの VPN 設定をアプリまたはアプリグループに割り当てるには、アプリまたはアプリグループの［**per-app VPN**］ドロップダウンリストで、アプリまたはアプリグループに関連付けられた設定を選択します。 **f.** ［割り当て］をクリックします。

6. ［追加］をクリックします。

会社のディレクトリグループの既存のディレクトリにリンクされたグループへの追加

作業を始める前に： ディレクトリにリンクされたグループの作成。

1. 管理コンソールのメニューバーで、［グループ］ > ［ユーザー］をクリックします。
2. ディレクトリにリンクされたグループをクリックします。
3. ［設定］タブで、 をクリックします。
4. ［リンクされたディレクトリグループ］セクションで ＋ をクリックします。
5. 既存のディレクトリリンクグループに追加する会社のディレクトリグループを検索して選択します。
6. ［追加］をクリックします。
7. 必要な場合は、［ネストされたグループをリンク］を選択します。

ローカルグループの作成

では、BlackBerry UEM IT ポリシー、プロファイル、およびアプリをに割り当てることができるローカルユーザーグループを作成できます。グループにユーザーアカウントを追加すると、グループに割り当てるプロパティがグループの各メンバに割り当てられます。ローカルユーザーアカウントとディレクトリユーザーアカウントの両方をローカルグループに追加できます。

1. 管理コンソールのメニューバーで、［グループ］ > ［ユーザー］をクリックします。
2. をクリックします。
3. グループの名前と説明を入力します。
4. 次の操作のいずれかを実行します。

タスク	手順
ローカルグループへのユーザーロールの割り当て	a. ［ユーザーロール］セクションで ＋ をクリックします。 b. ドロップダウンリストで、グループに割り当てるユーザーロールの名前をクリックします。 c. ［追加］をクリックします。
ローカルグループに IT ポリシーまたはプロファイルを割り当てます。	a. ［IT ポリシーおよびプロファイル］セクションで ＋ をクリックします。 b. ［IT ポリシー］またはプロファイルの種類をクリックします。 c. ドロップダウンリストで、グループに割り当てる IT ポリシーまたはプロファイルの名前をクリックします。 d. ［割り当て］をクリックします。

タスク	手順
ローカルグループにアプリを割り当てます。	**a.** ［割り当てられたアプリ］セクションで＋をクリックします。 **b.** グループに割り当てるアプリを検索して選択します。 **c.** ［次へ］をクリックします。 **d.** ［種別］ドロップダウンリストで、次のいずれかを実行します。 • アプリをデバイスへ自動的にインストールし、ユーザーがこのアプリをアンインストールできないようにするには、［必須］を選択します。このオプションは、BlackBerry アプリでは使用できません。 • ユーザーにアプリのインストールを要求し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしで必須］を選択します。 • ユーザーにアプリのインストールおよびアンインストールを許可するには、［オプション］を選択します。 • ユーザーにアプリのインストールと削除を許可し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしでオプション］を選択します。 同じアプリが、ユーザーアカウントと、ユーザーが属するユーザーグループに割り当てられている場合、ユーザーアカウントに割り当てられているアプリの種別が優先されます。 **e.** iOS デバイスの場合、アプリごとの VPN 設定をアプリまたはアプリグループに割り当てるには、［**per-app VPN**］ドロップダウンリストで、アプリまたはアプリグループに関連付けられた設定を選択します。 **f.** iOS および Android デバイスの場合、使用可能な場合は、アプリに割り当てるアプリ設定を選択します。 **g.** Android Enterprise を使用していて、Google Play コンソールでアプリのトラックを作成してある場合は、トラックを選択してアプリに割り当てます。 **h.** ［割り当て］をクリックします。

5. ［追加］をクリックします。

ユーザーグループへのネストされたグループの追加

グループをユーザーグループ内でネストする場合、ネストされたグループのメンバーはユーザーグループのプロパティを継承します。BlackBerry UEM でネスト構造を作成および維持します。ディレクトリにリンクされたグループとローカルグループのどちらもそれぞれのタイプのユーザーグループ内でネストできます。1 つのネストされたグループをユーザーグループに追加すると、ネストされたグループに属するすべてのグループも追加されます。

1. 管理コンソールのメニューバーで、［グループ］**>**［ユーザー］をクリックします。

2. ユーザーグループの名前を検索してクリックします。

3. ［ネストされたグループ］タブで、＋をクリックします。

4. 1 つ以上のグループを選択します。
5. ［追加］をクリックします。

終了したら： ユーザーグループに直接割り当てられているネストされたグループを削除するには、［グループ］で、グループを削除するユーザーグループの名前をクリックします。［ネストされたグループ］タブで、削除するネストされたグループの横にある ✕ をクリックします。

ユーザーグループの追加

作業を始める前に： ローカルグループの作成 または ディレクトリにリンクされたグループの作成

1. 管理コンソールのメニューバーで、［グループ］ > ［ユーザー］をクリックします。
2. 管理するユーザーグループを検索してクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
ユーザーグループに関する情報を表示します。	a. グループに割り当てられているユーザーアカウントを表示するには、［ユーザー］をクリックします。 b. グループに割り当てられているネストされたグループを表示するには、［ネストされたグループ］をクリックします。 c. リンクされたディレクトリグループ（使用可能な場合）またはグループの割り当てられたプロパティを表示するには、［設定］をクリックします。
ユーザーグループの名前または説明を変更します。	a. ✎ をクリックします。 b. ユーザーグループの名前または説明を変更します。 c. ［保存］をクリックします。
割り当てられたロール、割り当てられたプロファイル、またはユーザーグループの割り当てられたアプリを管理します。	a. ［設定］タブをクリックします。 b. ロール、プロファイル、またはアプリをユーザーグループに割り当てるには、該当するセクションの横にある ＋ をクリックします。 c. ユーザーグループからロール、プロファイル、またはアプリを削除するには、削除するプロパティの横にある ✕ をクリックします。
ユーザーグループを削除します。	a. 🗑 をクリックします。 b. ［削除］をクリックします。

デバイスグループの作成と管理

デバイスグループは、機種と製造元、OS のタイプとバージョン、通信事業者、所有権などの共通の属性を持つデバイスのグループです。定義した属性に基づいて、BlackBerry UEM はデバイスをデバイスグループの内外に自動的に移動します。

デバイスグループを使用して、特定のデバイスに、ポリシー、プロファイル、アプリのさまざまなセットを適用できます。デバイスグループに割り当てられるプロパティは、ユーザーまたはユーザーグループに割り当てられるものより優先されます。アクティベーションプロファイルまたはユーザー証明書をデバイスグループに割り当てることはできません。

デバイスグループの作成

1. 管理コンソールのメニューバーで、［グループ］ > ［デバイス］をクリックします。
2. をクリックします。
3. デバイスグループの名前を入力します。
4. 必要に応じて、［ユーザーグループへの領域］セクションで、デバイスグループを適用するユーザーグループを選択します。ユーザーグループを選択しない場合、デバイスグループはすべてのアクティブ化されたデバイスに適用されます。
5. ［デバイスクエリ］セクションの最初のドロップダウンリストで、次のいずれかを実行します。
   - 定義したすべての属性に一致するデバイスを含める場合は、［すべて］を選択します。
   - 定義した属性の少なくとも 1 つに一致するデバイスを含める場合は、［任意］を選択します。
6. ［デバイスクエリ］セクションで、デバイスグループのパラメーターを設定します。『デバイスグループのパラメーター』を参照してください。
7. ［次へ］をクリックします。
8. 次の操作のいずれかを実行します。

タスク	手順
デバイスグループへの IT ポリシーまたはプロファイルの割り当て	a. ［**IT** ポリシーおよびプロファイル］セクションで ＋ をクリックします。 b. ［**IT** ポリシー］またはプロファイルの種類をクリックします。 c. ドロップダウンリストで、グループに割り当てる IT ポリシーまたはプロファイルの名前をクリックします。 d. ［割り当て］をクリックします。

タスク	手順
アプリまたはアプリグループのデバイスグループへの割り当て	**a.** ［割り当てられたアプリ］セクションで＋をクリックします。 **b.** グループに割り当てるアプリを検索して選択します。 **c.** ［次へ］をクリックします。 **d.** ［種別］ドロップダウンリストで、次のいずれかを実行します。 • iOS および Android アプリの場合、ユーザーに割り当てられたコンプライアンスプロファイルでアプリ向けに定義された操作に従うことをユーザーに対して要求するには、［必須］を選択します。 • ユーザーにアプリのインストールを要求し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしで必須］を選択します。 • ユーザーにアプリのインストールおよびアンインストールを許可するには、［オプション］を選択します。このオプションは、Android Enterprise をサポートするアプリグループでは使用できません。 • ユーザーにアプリのインストールと削除を許可し、Apple VPP アプリが自動的に更新されないようにするには、［更新なしでオプション］を選択します。 **e.** iOS デバイスの場合、アプリごとの VPN 設定をアプリまたはアプリグループに割り当てるには、［**per-app VPN**］ドロップダウンリストで、アプリまたはアプリグループに関連付けられた設定を選択します。 **f.** iOS および Android デバイスの場合、使用可能な場合は、アプリに割り当てるアプリ設定を選択します。 **g.** Android Enterprise を使用していて、Google Play コンソールでアプリのトラックを作成してある場合は、トラックを選択してアプリに割り当てます。 **h.** ［割り当て］をクリックします。 権限はユーザーのみに付与できるため、デバイスグループに BlackBerry Dynamics アプリを追加できないことに注意してください。アプリグループに含まれている BlackBerry Dynamics アプリで、管理者がデバイスグループに追加したものは、ユーザーに割り当てられません。 Android Enterprise がサポートされる環境の場合、オプションの種別になっている Android アプリをデバイスグループに追加できません。Google Play for Work は、Google ユーザー ID にのみアプリを割り当てることができ、デバイス ID には割り当てることができません。必須の種別になっている Android アプリをデバイスグループに追加すると、そのアプリはインストールされますが、Google Play for Work のリストには表示されません。

9. ［保存］をクリックします。

デバイスグループのパラメーター

デバイスグループを作成する場合は、1 つ以上の属性ステートメントを含むデバイスクエリを設定します。デバイスが任意の属性ステートメントに一致した場合、またはすべての属性ステートメントに一致した場合にのみ、デバイスをデバイスグループに所属させるかどうかを指定できます。各属性ステートメントには、属性、演算子、値が含まれます。

属性	演算子	値
所有権	• = • !=	ドロップダウンリストで、次のオプションのいずれかを選択します。 • 仕事用 • 個人 • 指定なし
OS バージョン	• = • != • >= • <=	OS のバージョンを指定します（例：7.1.1 または 10.3）。この属性を使用する場合は、OS 属性も指定する必要があります。
OS	• = • !=	ドロップダウンリストで、適切な OS を選択します。
保留中の OS 更新期間（日）	>=	デバイスがデバイスグループに含まれる前に、ユーザーがデバイス OS を更新する日数を指定します。 この属性は、iOS デバイスと Android デバイスに適用されます。
製造元	• = • != • 次で始まる	デバイスの製造元の名前を指定します（例：Apple ）。
機種	• = • != • 次で始まる	デバイスモデルの名前を指定します（例：iPhone 15）。
通信事業者	• = • != • 次で始まる	T-Mobile または Bell などの通信事業者の名前を指定します。
アクティベーションタイプ	• = • !=	ドロップダウンリストで、アクティベーションタイプを選択します。リストには、アクティベーションプロファイルにある割り当て可能なアクティベーションタイプと同じものが含まれています。

属性	演算子	値
Knox Workspace	• = • != • 次で始まる	Samsung Knox Workspace バージョンを指定します（例：3.2.1）。
BlackBerry Dynamics	• = • !=	ドロップダウンリストで、次のオプションのいずれかを選択します。 • 無効 • 有効
Apple DEP	• = • !=	ドロップダウンリストで、次のオプションのいずれかを選択します。 • いいえ • はい

デバイスグループの管理

作業を始める前に： デバイスグループの作成。

1. 管理コンソールのメニューバーで、［グループ］ > ［デバイス］をクリックします。
2. 管理するデバイスグループを検索してクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
デバイスグループに関する情報を表示します。	**a.** デバイスグループに割り当てられたデバイスを表示するには、［デバイス］タブをクリックします。 **b.** デバイスグループに割り当てられたユーザーグループ、デバイスクエリ、IT ポリシー、プロファイル、またはアプリを表示するには、［設定］タブをクリックします。
デバイスグループを編集します。	**a.** をクリックします。 **b.** 変更を加えます。 **c.** ［保存］をクリックします。
デバイスグループを削除します。	**a.** をクリックします。 **b.** ［削除］をクリックします。

共有デバイスグループの作成と管理

複数のユーザーによる iOS デバイスの共有を許可する場合は、共有デバイスグループを作成できます。各ユーザーに固有のグループ、またはすべてのユーザーに同じグループの設定を行うことができます。共有デバイスグループを作成すると、BlackBerry UEM は共有デバイスグループを所有するローカルユーザーアカウントを作成します。

デバイスをチェックアウトするために、ユーザーはローカルまたは Microsoft Active Directory 認証のいずれかを使用できます。ユーザーが共有デバイスをチェックアウトするために受け入れる必要がある使用条件をカスタマイズすることができます。デバイスをチェックインすると、次のユーザーが使用できるようになります。チェックアウトおよびチェックイン中、共有デバイスは UEM に管理されます。

この機能は、次の設定で、監視対象のデバイス用に設計されています。

- アプリロックモード有効
- VPP アプリ割り当て済み

この機能は BlackBerry Dynamics アプリをサポートしていません。共有デバイスグループを所有しているユーザーアカウントのほか、共有デバイスグループ自体に同じ BlackBerry Dynamics プロファイルを割り当てる必要があります。プロファイルで、［UEM Client を BlackBerry Dynamics に登録可能にする］オプションが選択されていないことを確認する必要があります。

共有デバイスグループの作成

共有デバイスグループを作成すると、ローカルユーザーアカウントが作成されます。このローカルユーザーアカウントは、共有デバイスグループを所有しています。

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［共有デバイスグループ］をクリックします。
2. ＋ をクリックします。
3. 共有デバイスグループの名前と説明を入力します。
4. デバイスのアクティベーションのためにユーザー名を入力します。
5. ユーザーが共有デバイスをチェックアウトするときにサービス利用規約に同意するように要求するには、［サービスの条件を有効にする］を選択し、サービスの条件を指定します。
6. グループに追加する各ユーザーについて、［付与されたユーザー］セクションでユーザーを検索してクリックします。

   ユーザーは、複数の共有デバイスグループに属することができます。
7. アプリまたはアプリグループを割り当てるには、［割り当てられたアプリ］セクションで ＋ をクリックし、次の操作を実行します。
   a) グループに割り当てるアプリを検索して選択します。
   b) ［次へ］をクリックします。
   c) iOS または Android アプリの場合、自分たちに割り当てられたコンプライアンスプロファイルでアプリ向けに定義された操作に従うことをユーザーに対して要求するには、グループの［種別］ドロップダウンリストで［必須］を選択します。

      アプリグループが Android Enterprise をサポートしている場合、種別は［必須］にのみ設定できます。
   d) ユーザーがアプリをインストールおよびアンインストールできるようにするには、［種別］ドロップダウンリストで、［オプション］を選択します。

e) iOS デバイスの場合、アプリごとの VPN 設定をアプリまたはアプリグループに割り当てるには、［**per-app VPN**］ドロップダウンリストで、アプリまたはアプリグループに関連付けられた設定を選択します。
f) iOS および Android デバイスの場合、使用可能な場合は、アプリに割り当てるアプリ設定を選択します。
g) Android Enterprise を使用していて、Google Play コンソールでアプリのトラックを作成してある場合は、トラックを選択してアプリに割り当てます。
h) ［割り当て］をクリックします。

権限はユーザーのみに付与できるため、管理者はデバイスグループに BlackBerry Dynamics アプリを追加できません。アプリグループに含まれている BlackBerry Dynamics アプリで、管理者がデバイスグループに追加したものは、ユーザーに割り当てられません。

Android がサポートされる環境の場合、オプションの種別になっている Android Enterprise アプリをデバイスグループに追加できません。Google Play for Work は、Google ユーザー ID にのみアプリを割り当てることができ、デバイス ID には割り当てることができません。必須の種別になっている Android アプリをデバイスグループに追加すると、そのアプリはインストールされますが、Google Play for Work のリストには表示されません。

8. ［保存］をクリックします。

終了したら：

- 共有デバイスのアクティベーション。
- 共有デバイスグループに変更を加えるには、「共有デバイスグループの管理」を参照してください。

共有デバイスのアクティベーション

共有デバイスをユーザーがチェックアウトできるようにするには、事前にこれらをアクティブにしておく必要があります。ユーザーのプライバシー - ユーザー登録 アクティベーションタイプはサポートされていません。

作業を始める前に： 共有デバイスグループに割り当てられる BlackBerry Dynamics プロファイルで、［BlackBerry Dynamics に登録する UEM Client を有効にする］オプションが選択されていないことを確認します。共有デバイスグループを所有しているユーザーアカウントにも、同じプロファイルが割り当てられ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、［専用デバイス］ > ［共有デバイスグループ］をクリックします。
2. 共有デバイスグループの名前を検索してクリックします。
3. デバイスのアクティブ化に使用するサーバーアドレスとデバイスアクティベーション資格情報を取得するには、［デバイスのアクティベーション］をクリックします。
4. デバイスをアクティブ化するには、画面の指示に従います。

終了したら： アクティブなデバイスが［共有デバイス］セクションに表示されていることを確認します。デバイス名を生成するために、BlackBerry UEM はグループ名に番号を追加します。例えば、グループ名が Example の場合、アクティブにした最初のデバイスは Example 01 という名前になります。

共有デバイスグループの管理

作業を始める前に： 共有デバイスグループの作成。

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［共有デバイスグループ］をクリックします。
2. 管理する共有デバイスグループの名前を検索してクリックします。

3. 次の操作のいずれかを実行します。

タスク	手順
デバイスがチェックインされている場合にのみ BlackBerry UEM Client ログイン画面を表示します。	**a.** をクリックします。 **b.** ［**UEM Client** アプリロックを有効にする］チェックボックスをオンにします。 **c.** ［保存］をクリックします。
共有デバイスグループのユーザーメンバーシップを編集します。	**a.** ［付与されたユーザー］セクションに移動します。 **b.** グループにユーザーを追加するには、ユーザーの名前を検索してクリックします。 **c.** グループからユーザーを削除するには、［アクション］列で ✕ をクリックします。
共有デバイスグループに IT ポリシーまたはプロファイルを割り当てます。	デバイスがチェックインされたとき、またはユーザーによってチェックアウトされたときのいずれかの状態で適用される、IT ポリシーとプロファイルを共有デバイスグループに割り当てることができます。デバイスがチェックインされているかチェックアウトされているかに関わらず、同じ IT ポリシーまたはプロファイルが適用されるようにするには、両方の状態に割り当てられます。割り当てられた IT ポリシーまたはプロファイルが各状態で異なる場合は、デバイスがチェックインまたはチェックアウトされるたびに、適切なポリシーとプロファイルが適用されます。 **a.** ［チェックアウト設定］タブの［割り当てられた **IT** ポリシーおよびプロファイル］セクションで ＋ をクリックします。 **b.** ［**IT** ポリシー］またはプロファイルの種類をクリックします。 **c.** ドロップダウンリストで、デバイスがチェックアウトされた際にデバイスに割り当てる IT ポリシーまたはプロファイルの名前をクリックします。 **d.** ［割り当て］または［置換］をクリックします。 **e.** ［チェックイン設定］タブで、共有デバイスがチェックインされたときに適用する IT ポリシーとプロファイルを割り当てる手順を繰り返します。

タスク	手順
共有デバイスグループにアプリを割り当てます。	デバイスがチェックインされたとき、またはユーザーによってチェックアウトされたときのいずれかの状態で利用可能になる、アプリまたはアプリグループを共有デバイスグループに割り当てることができます。アプリが常にデバイスに残るようにするには、アプリを両方の状態に割り当てます。割り当てられたアプリは、デバイスがチェックインまたはチェックアウトされるたびに、1 つの状態でのみ使用可能になり、適切に追加または削除されます。 以下の手順に従う前に、使用可能なアプリリストにアプリを追加するか、アプリグループを作成します。 **a.** ［チェックアウト設定］タブの［割り当てられたアプリ］セクションで ＋ をクリックします。 **b.** 割り当てるアプリまたはアプリグループを検索して選択します。 **c.** ［次へ］をクリックします。 **d.** アプリの種別、アプリごとの VPN、アプリ設定を構成し、必要に応じて追跡します。 **e.** ［次へ］をクリックします。 **f.** アプリにライセンスを割り当て、必要に応じてライセンス設定を構成する場合は、［はい］を選択します。ライセンスを割り当てない場合、または、アプリに割り当てるライセンスがない場合には、［いいえ］を選択します。 **g.** ［割り当て］をクリックします。 支払い済みのアプリをインストールするには、ユーザーは手順に従ってデバイスで組織の VPP に登録する必要があります。一度はこのタスクを完了する必要があります。 **h.** ［チェックイン設定］タブで、デバイスのチェックイン時にデバイスにインストールされたままにする必要があるアプリまたはアプリグループを割り当てる手順を繰り返します。
共有デバイスグループからデバイスを削除します。	**a.** ［共有デバイス］セクションの［アクション］列で、✕ をクリックします。 **b.** ［仕事用データのみを削除］をクリックします。
共有デバイスグループを削除します。	**a.** 共有デバイスグループからすべてのデバイスを削除します。 **b.** 🗑 をクリックします。 **c.** ［削除］をクリックします。

公開デバイスグループの作成と管理

公開デバイスは、その目的を実行するために特定のアプリケーションセットにロックされた単一目的のデバイスです。この機能は、iOS および Android Enterprise デバイスでのみサポートされています。

パブリックデバイスグループには、アプリロックモードプロファイルとサポートされているアクティベーションプロファイルが割り当てられている必要があります。Android Enterprise の場合、アクティベーションタイプは仕事用領域のみである必要があります（Android Enterprise 完全管理のデバイス）。iOS の場合、デバイスは MDM コントロールを備えた管理対象の iOS デバイスである必要があります。

公開デバイスグループの作成

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［公開デバイスグループ］をクリックします。
2. ＋をクリックします。
3. パブリックデバイスグループの名前と説明を入力します。
4. デバイスのアクティベーションのためにユーザー名を入力します。
5. アプリまたはアプリグループをグループに割り当てるには、［割り当てられたアプリ］セクションで＋をクリックし、次の操作を実行します。
   a) グループに割り当てるアプリを検索して選択します。
   b) ［次へ］をクリックします。
   c) iOS または Android アプリの場合、自分たちに割り当てられたコンプライアンスプロファイルでアプリ向けに定義された操作に従うことをユーザーに対して要求するには、グループの［種別］ドロップダウンリストで［必須］を選択します。

      アプリグループが Android Enterprise をサポートしている場合、種別は［必須］である必要があります。
   d) ユーザーがアプリをインストールおよびアンインストールできるようにするには、［種別］ドロップダウンリストで、［オプション］を選択します。
   e) iOS デバイスの場合、アプリごとの VPN 設定をアプリまたはアプリグループに割り当てるには、［**per-app VPN**］ドロップダウンリストで、アプリまたはアプリグループに関連付けられた設定を選択します。
   f) iOS および Android デバイスの場合、使用可能な場合は、アプリに割り当てるアプリ設定を選択します。
   g) Android Enterprise を使用していて、Google Play コンソールでアプリのトラックを作成してある場合は、トラックを選択してアプリに割り当てます。
6. ［割り当て］をクリックします。

   権限はユーザーのみに付与できるため、管理者はデバイスグループに BlackBerry Dynamics アプリを追加できません。アプリグループに含まれている BlackBerry Dynamics アプリで、管理者がデバイスグループに追加したものは、ユーザーに割り当てられません。

   Android Enterprise をサポートしている場合、Android オプションの種別を持つアプリをデバイスグループに追加することはできません。Google Play for Work は、Google ユーザー ID にのみアプリを割り当てることができ、デバイス ID には割り当てることができません。必須の種別になっている Android アプリをデバイスグループに追加すると、そのアプリはインストールされますが、Google Play for Work のリストには表示されません。
7. ［保存］をクリックします。

終了したら：

- アプリロックモードプロファイルを作成して、パブリックデバイスグループに割り当てます。

- アクティベーションプロファイルを作成して、パブリックデバイスグループに割り当てます。Android Enterprise のアクティベーションタイプは、仕事用領域専用（Android Enterprise 完全管理のデバイス）である必要があります。iOS のアクティベーションタイプは、MDM コントロールを備えた監視対象の iOS デバイスである必要があります。
- 公開デバイスのアクティベーション。
- 公開デバイスグループを削除するには、削除するグループの横にあるチェックボックスをオンにして、🗑 をクリックします。

公開デバイスのアクティベーション

作業を始める前に： 公開デバイスグループの作成。

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［公開デバイスグループ］をクリックします。
2. パブリックデバイスグループの名前を検索してクリックします。
3. デバイスのアクティブ化に使用するサーバーアドレスとアクティベーション資格情報を取得するには、［デバイスのアクティベーション］をクリックします。
4. デバイスをアクティブ化するには、画面の指示に従います。

終了したら： アクティブ化されたデバイスが［公開デバイス］セクションに表示されていることを確認します。デバイス名を生成するために、BlackBerry UEM はグループ名に番号を追加します。例えば、グループ名が Example の場合、アクティブにした最初のデバイスは Example 01 という名前になります。

公開デバイスグループの管理

作業を始める前に： 公開デバイスグループの作成。

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［公開デバイスグループ］をクリックします。
2. 公開デバイスグループを検索してクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
公開デバイスグループに IT ポリシー、プロファイル、またはアプリを割り当てます。	a. 適切なセクションで、＋ をクリックします。 b. 割り当てる IT ポリシー、プロファイル、またはアプリを選択します。プロンプトに従って適切な設定を選択し、割り当てを完了します。 c. IT ポリシー、プロファイル、またはアプリを削除するには、削除するプロパティの横にある ✕ をクリックします。
公開デバイスグループからデバイスを削除します。	［公開デバイス］セクションの［アクション］列で、 をクリックします。

共有 iPad グループの作成と管理

共有 iPad グループを作成すると、ユーザーは管理対象 Apple ID を持つ共有 iPad にサインインして、別々のユーザー詳細を維持および同期しながら、共通のアプリとブックマークを使用できるようになります。

次の要件を確認してください。

- iPad デバイスは、監視対象の MDM 登録デバイスである必要があります。
- iPad デバイスは DEP に登録する必要があります。
- iPad デバイスはサポートされている iPadOS バージョンを使用している必要があります。

この機能は BlackBerry Dynamics アプリをサポートしていません。BlackBerry Dynamics プロファイルで［BlackBerry Dynamics に登録する UEM Client を有効にする］オプションが選択されていないことを確認する必要があります。

共有 iPad グループの作成

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［共有 **iPad** グループ］をクリックします。
2. ＋ をクリックします。
3. 共有 iPad グループの名前と説明を入力します。
4. デバイスのアクティベーションのためにユーザー名を入力します。
5. アプリまたはアプリグループをグループに割り当てるには、［割り当てられたアプリ］セクションで ＋ をクリックし、次の操作を実行します。
   a) グループに割り当てるアプリを検索してクリックします。
   b) ［次へ］をクリックします。
   c) 割り当てられたコンプライアンスプロファイル内のアプリに定義されたアクションに従うようにユーザーに要求するには、［種別］ドロップダウンリストで、［必須］または［更新なしで必須］を選択します。
   d) per-app VPN 設定をグループに割り当てるには、グループの［**Per app VPN**］ドロップダウンリストで、グループに関連付ける設定を選択します。
   e) 使用可能な場合は、アプリに割り当てるアプリ設定を選択します。
   f) ［割り当て］をクリックします。
6. ［保存］をクリックします。

終了したら：

- オプションで、共有 iPad プロファイルの作成。
- 共有 iPad デバイスのアクティベーション。
- 共有 iPad グループを変更するには、「共有 iPad グループの管理」を参照してください。

共有 iPad プロファイルの作成

必要に応じて、共有 iPad プロファイルを作成して割り当て、ユーザーが共有 iPad デバイスを使用する方法を設定できます。

作業を始める前に： 共有 iPad グループの作成。

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］ > ［ポリシー］ > ［共有 **iPad**］をクリックします。
2. ＋をクリックします。
3. 共有 iPad プロファイルの名前と説明を入力します。
4. ［割り当てサイズ］フィールドでは、共有デバイスでの各ユーザーの割り当てサイズを MB 単位で指定します。この設定は、［常駐ユーザー］設定よりも優先されます。
5. ［常駐ユーザー］フィールドでは、残りのデバイス領域をパーティション化するためにユーザー数を指定します。
6. デバイスでゲストモードのみを使用する場合は、［一時セッション専用］オプションを選択します。
7. ［一時セッションタイムアウト］フィールドでは、一時セッションのタイムアウトを秒単位で指定します。
8. ［ユーザーセッションタイムアウト］フィールドでは、通常セッションのタイムアウトを秒単位で指定します。
9. ［保存］をクリックします。

終了したら：

- 共有 iPad グループにプロファイルを割り当てます。
- 共有 iPad デバイスのアクティベーション。

共有 iPad デバイスのアクティベーション

作業を始める前に：

- 共有 iPad グループの作成。オプションで、共有 iPad プロファイルの作成。
- ［共有 iPad モードを有効にする］オプションを選択して DEP 設定を作成し、DEP がアクティブ化されている iPad デバイスに割り当てます。
- iPad デバイスを消去します。
- 共有 iPad グループに割り当てられる BlackBerry Dynamics プロファイルで、［**BlackBerry Dynamics** に登録する **UEM Client** を有効にする］オプションが選択されていないことを確認します。共有 iPad グループを所有しているユーザーアカウントにも、同じプロファイルが割り当てられ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、［専用デバイス］ > ［共有 **iPad** グループ］をクリックします。
2. 共有 iPad グループの名前を検索してクリックします。
3. デバイスのアクティブ化に使用するアクティベーション資格情報を取得するには、［デバイスのアクティベーション］をクリックします。
4. デバイスをアクティブ化するには、画面上のデバイスのアクティベーション手順に従います。

終了したら： 共有 iPad グループからデバイスを削除するには、デバイスを削除するグループの名前をクリックします。［デバイス詳細］画面で、［デバイスを削除］または［すべてのデバイスデータを削除］をクリックします。

共有 iPad グループの管理

作業を始める前に： 共有 iPad グループの作成。

1. 管理コンソールのメニューバーで、［専用デバイス］ > ［共有 **iPad** グループ］をクリックします。

2. 共有 iPad グループを検索してクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
共有 iPad グループに IT ポリシーまたはプロファイルを割り当てます。	**a.** ［割り当てられた **IT** ポリシーおよびプロファイル］セクションで ＋ をクリックします。 **b.** ［**IT** ポリシー］またはプロファイルの種類をクリックします。 **c.** ドロップダウンリストで、割り当てる IT ポリシーまたはプロファイルの名前をクリックします。 **d.** ［割り当て］または［置換］をクリックします。
共有 iPad グループにアプリを割り当てます。	権限はユーザーのみに付与できるため、BlackBerry Dynamics アプリを iPad グループに追加できません。共有 iPad グループに追加するアプリグループに含まれている BlackBerry Dynamics アプリは、ユーザーに割り当てられません。 iOS アプリのショートカットに加えて、VPP アプリまたは内部 iOS アプリのみがサポートされます。VPP 以外のストアアプリはサポートされていません。 **a.** ［割り当てられたアプリ］セクションで ＋ をクリックします。 **b.** 割り当てるアプリまたはアプリグループを検索して選択します。 **c.** ［次へ］をクリックします。 **d.** もう一度［次へ］をクリックします **e.** 各アプリごとにデバイスに VPP アプリライセンスを割り当てます。 **f.** ［割り当て］をクリックします。

BlackBerry UEM での Chrome OS デバイスの管理

Chrome OS を BlackBerry UEM 管理コンソールと統合すると、UEM で一部の管理タスクを実行する機能を拡張できます。Chrome OS デバイスの登録を続行し、Google 管理コンソールで管理タスクを実行します。Chrome OS を UEM と統合すると、組織単位が Google 管理コンソールから UEM 組織単位グループにソートされます。Google ドメイン内で組織単位、ユーザー、またはデバイスに変更を加えると、UEM はそれに応じてデータベースを更新します。

Chrome OS デバイスをサポートするための UEM の設定の詳細については、「Chrome OS デバイスの管理を BlackBerry UEM に拡張」を参照してください。

Chrome OS デバイスの管理

作業を始める前に： Chrome OS デバイスの管理を BlackBerry UEM に拡張します。

次の操作のいずれかを実行します。

タスク	手順
Chrome OS ユーザーの組織単位を表示します。	a. 管理コンソールのメニューバーで、［ユーザー］ > ［すべてのユーザー］をクリックします。 b. Chrome OS ユーザーを検索してクリックします。 c. ユーザーが所属する組織単位がページの上部に表示されます。組織単位の名前をクリックすると、その現在の設定を表示できます。
組織単位を編集します。	組織単位に表示される情報は、Google 管理コンソールで設定した内容の複製です。組織単位で特定のフィールドを編集できますが、設定の多くは Google 管理コンソールでのみ変更できます。 a. 管理コンソールのメニューバーで、［グループ］ > ［組織単位］をクリックします。 b. 編集する組織単位をクリックします。 c. 必要な変更を行います。 d. ［保存］をクリックします。

タスク	手順
Chrome OS デバイスにコマンドを送信します。	**a.** 管理コンソールのメニューバーで、［ユーザー］ **>** ［すべてのユーザー］をクリックします。 **b.** Chrome OS ユーザーを検索してクリックします。 **c.** ［デバイスを管理］セクションで、次のコマンドのいずれかをクリックします。 • ［デバイスレポートを表示］：デバイスに関する詳細情報が表示されます。 • ［デバイスでの操作を表示］：デバイスで実行中のアクションが表示されます。 • ［デバイスを無効化］：デバイスが無効化されます。管理者がデバイスを無効にすると、ユーザーはデバイスを再度有効にすることはできません。 • ［デバイスを有効化］：デバイスが有効化されます。 • ［すべてのデバイスデータを削除］：ユーザー情報とアプリデータがすべて削除され、デバイスが工場出荷時のデフォルト設定に戻ります。 • ［仕事用データのみを削除］：仕事用データが削除され、デバイスのプロビジョニングが解除されます。 • ［デバイスを削除］：デバイスが削除されます。

BlackBerry UEM Self-Service をセットアップする

BlackBerry UEM Self-Service は、デバイスユーザーが、アクティベーションパスワードの作成、デバイスのリモートでのロック、デバイスからのデータの削除などの管理タスクを実行できる、Web ベースのアプリケーションです。UEM Self-Service を使用するには、ユーザーに Web アドレスとログイン情報を提供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［設定］>［セルフサービス］>［セルフサービス設定］をクリックします。
2. ［セルフサービスコンソールへのアクセスをユーザーに許可する］チェックボックスが選択されていることを確認します。
3. アクティベーションパスワードが期限切れになるまでに、ユーザーがデバイスをアクティブ化できる時間の長さを指定します。
4. アクティベーションパスワードに必要な最小文字数を指定します。
5. ［最低限のパスワードの複雑さ］ドロップダウンリストで、アクティベーションパスワードに必要な複雑さのレベルを選択します。
6. UEM Self-Service でアクティベーションパスワードを作成したときにアクティベーションメールをユーザーに自動的に送信するには、［アクティベーションメールを送信］チェックボックスをオンにします。デフォルトのアクティベーションメールテンプレートを使用するか、ドロップダウンリストから別のテンプレートを選択することができます。
7. UEM Self-Service にログインしたユーザーにログイン通知メールを送信するには、［セルフサービスログイン通知を送信］チェックボックスをオンにします。
8. ［保存］をクリックします。

終了したら：

- ユーザーに BlackBerry UEM Self-Service の Web アドレスとログイン情報を提供します。
- UEM Self-Service のユーザーロールを作成および管理するには、「BlackBerry UEM Self-Service のユーザーロールの管理」を参照してください。

BlackBerry UEM Self-Service のユーザーロールの管理

ユーザーロールを使用して、BlackBerry UEM Self-Service でユーザーが使用できる機能を指定できます。BlackBerry UEM には、事前設定されたデフォルトのユーザーロールが 1 つ含まれます。デフォルトのユーザーロールは、すべての UEM Self-Service 機能を許可するように設定されていて、［すべてのユーザー］グループに割り当てられています。

メモ：［すべてのユーザー］グループからデフォルトのユーザーロールの名前変更、削除、または除去を行うと、iOS デバイス上の［仕事用アプリ］で問題が発生する可能性があります。

ユーザーの特定の機能を制限する場合は、新しいユーザーロールを作成するか、既存のユーザーロールを編集できます。ユーザーロールは、グループまたは直接ユーザーに割り当てることができます。

1 人のユーザーには 1 つのロールのみが割り当てられます。ユーザーアカウントに直接割り当てられたロールは、ユーザーグループによって間接的に割り当てられたロールより優先されます。ユーザーが、異なるユーザーロールを持つ複数のユーザーグループのメンバーである場合、UEM はランキングが最も高いロールを割り当てます。

BlackBerry UEM Self-Service 機能

機能	説明
アクティベーションパスワードを指定	ユーザーは、BlackBerry UEM でデバイスをアクティブ化するために使用できるパスワードを作成できます。［設定］ > ［セルフサービス］ > ［セルフサービスの設定］をクリックして、デフォルトのパスワードの有効期間を設定したり、必須のパスワードの複雑さを設定したりできます。
アクセスキーを指定	ユーザーは BlackBerry Dynamics アプリのアクティブ化に使用できるアクセスキーを作成できます。
仕事用データのみを削除	ユーザーは［仕事用データのみを削除］コマンドをデバイスに送信できます。このコマンドは、IT ポリシー、プロファイル、アプリ、証明書などの仕事用データを削除します。
すべてのデバイスデータを削除	ユーザーは［すべてのデバイスデータを削除］コマンドをデバイスに送信できます。このコマンドは、仕事用領域内の情報を含め、デバイスに保存されているユーザー情報とアプリデータをすべて削除します。デバイスを工場出荷時のデフォルト設定に戻し、UEM からデバイスを削除します。
デバイスを検索	ユーザーは、iOS または Android デバイスの場所を地図上に表示できます。この機能では、位置情報サービスプロファイルがユーザーに割り当てられている必要があります。詳細については、「デバイスでの位置情報サービスを使用する」を参照してください。
ユーザー証明書の管理	ユーザーはデバイスのユーザー証明書をアップロードできます。必要な証明書に関して、またどこから証明書をアップロードするのかに関して、ユーザーに手順を提供できます。

機能	説明
BlackBerry Dynamics アプリのロックとロック解除	BlackBerry Dynamics 用にユーザーのデバイスが有効になっている場合、ユーザーはデバイスにインストールされている BlackBerry Dynamics アプリをロックしたり、ロック解除キーを生成してアプリをロック解除したりできます。ユーザーがアプリをロックすると、だれもアプリを起動できなくなります。
BlackBerry Dynamics のアプリデータの削除	BlackBerry Dynamics 用にユーザーのデバイスが有効になっている場合、ユーザーは、デバイスにインストールされている BlackBerry Dynamics アプリからすべてのデータを削除できます。このコマンドは、アプリで保存されたすべてのデータを削除しますが、アプリ自体は削除しません。

UEM Self-Service のユーザーロールの作成

カスタムのユーザーロールを作成して、ユーザーまたはグループに割り当てることで、ユーザーが BlackBerry UEM Self-Service で使用できる機能を指定できます。

1. 管理コンソールのメニューバーで［設定］**>**［セルフサービス］**>**［ユーザーロール］をクリックします。
2. をクリックします。
3. ユーザーロールの名前と説明を入力します。
4. 別のロールから権限をコピーするには、［ロールからコピーする権限］ドロップダウンリストでロールをクリックします。
5. ユーザーロールに提供する機能を選択します。
6. ［保存］をクリックします。

終了したら：

- 必要に応じてユーザーのロールに順位を付け、変更を保存します。
- ユーザーロールをユーザーグループ（［グループ］ > グループを検索してクリック > ［管理されているデバイス］）または個々のユーザー（［ユーザー］ > ［管理されているデバイス］ > ユーザーを検索してクリック > ［直接ロール割り当て］）に割り当てます。

ユーザーリストのカスタマイズ

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. 次の操作のいずれかを実行します。

タスク	手順
デフォルトビューまたは詳細ビューを設定します。	右上にある［デフォルト］または［詳細］をクリックします。 大規模な環境では、詳細ビューはデフォルトビューよりも時間がかかることがあります。
ユーザーリストに表示する情報を選択します。	a. ユーザーリストの一番上で、⋮をクリックします。 b. 含めるまたは除外する列を選択します。 ユーザーリストを列で並べ替えるには、列見出しをクリックします。 列を並べ替えるには、列ヘッダーをクリックしてドラッグします。
ユーザーリストをフィルターします。	複数選択を有効にした場合、複数のフィルターを選択してからそれらを適用でき、各カテゴリで複数のフィルターを選択できます。複数選択がオフになっている場合、各フィルターは選択時に適用され、各カテゴリで選択できるフィルターは 1 つのみになります。 a. 複数選択のオン/オフを切り替えるには、をクリックします。 b. ［フィルター］の下で 1 つ以上のカテゴリを展開します。各カテゴリには、結果が表示されるフィルターのみが含まれ、各フィルターは適用時に表示される結果の件数を示します。 c. 適用するフィルターを選択します。
ユーザーリストを .csv ファイルにエクスポートします。	ユーザーリストをエクスポートすると、ファイルには現在表示されているすべての列が含まれます。 a. エクスポートに含めるユーザーアカウントを選択します。ユーザーリストの一番上にあるチェックボックスをオンにして、すべてのユーザーを選択できます。 b. をクリックして、ファイルを保存します。

タスク	手順
デバイスの所有権ラベルを変更します。	アクティベーションされた各デバイスにはラベルがあります。そのデバイスの所有者が組織なのかユーザーなのか、またはその指定がないのかがわかります。デフォルト値は、アクティベーションプロファイルのデバイス所有権設定から取得されます。デバイスの所有権ラベルでユーザーリストをフィルターできます。特定のユーザーのデバイスの所有権ラベルを変更するには、次の手順に従います。複数のユーザーのラベルを変更する場合は、一括コマンドを送信できます。 **a.** ユーザーアカウントの名前を検索してクリックします。 **b.** ［アクティブ化されたデバイス］セクションで、所有権設定の横にある［編集］をクリックします。 **c.** 適切なデバイス所有権ラベルを設定します。 **d.** ［保存］をクリックします。

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