



## **Cisco Unified Mobility Advantage のクライアントのサポート の有効化**

### **Enabling Support for Clients in Cisco Unified Mobility Advantage**

初版: 2009 年 09 月 24 日

最終変更: 2010 年 04 月 28 日

Text Part Number: N/A

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)



## 目次

### クライアントのサポートの有効化 1

クライアント ソフトウェアおよびサポートされるデバイスのリストの入手方法 1

Cisco Unified Mobility Advantage への新しいクライアント リリースのアップロード 2

サポートされているデバイスとサービス プロバイダーの確認 2

ユーザが iPhone を持たない場合の、Apple Push Notification サービスの無効化 4

### Cisco Unified Mobility Advantage でクライアントにメッセージと通知を送信するための設定 5

Cisco Unified Mobility Advantage でクライアントにプロビジョニング メッセージを送信するための設定 5

iPhone クライアントへの不在着信およびボイスメールの通知 6

### BlackBerry デバイス用 Cisco Mobile または Cisco Unified Mobile Communicator の導入 9

BlackBerry 用の Release 3.x クライアントの導入について 9

BlackBerry 用の Release 7.1 クライアントの導入方法 10

BlackBerry Enterprise Server によるクライアント接続 10

BlackBerry クライアント導入の要件および制約事項 10

BlackBerry デバイスにモバイル ボイス システム (MVS) がともにインストールされている場合の要件 11

BlackBerry デバイス用 Release 7.1 をサポートするための Cisco Unified Mobility Advantage の設定方法 12

セキュアなトランザクションの確保について 12

Cisco Unified Mobility Advantage からの BlackBerry クライアント インストーラのダウンロード 12

ネットワーク プロパティの設定 (Cisco 適応型セキュリティ アプライアンスを使用しない導入の場合のみ) 13

Cisco Mobile を配布およびサポートするための BlackBerry Enterprise Server の設定方法 14

BlackBerry Enterprise Server からのサードパーティアプリケーションのダウンロード許可 14

BlackBerry Enterprise Server へのクライアント ソフトウェアの配置 15

ユーザがクライアント アプリケーションを使用できるようにするには 15

ソフトウェア設定ファイルの作成とユーザへの導入 16

BlackBerry Enterprise Server での MDS 接続サービス ポリシーの設定 17



# 第 1 章

## クライアントのサポートの有効化

この章では、iPhone、BlackBerry、Nokia Symbian および Windows Mobile デバイス用クライアントソフトウェアの導入手順について説明します。サポートするデバイスを特定し、クライアントソフトウェアをダウンロードできるようにします。



(注) iPhone クライアントソフトウェアは Cisco Unified Mobility Advantage 経由ではなく、Apple AppStore 経由で提供されますが、この章の手順に従って、iPhone をサポートされるデバイスとして指定する必要があります。

- [クライアントソフトウェアおよびサポートされるデバイスのリストの入手方法, 1 ページ](#)
- [Cisco Unified Mobility Advantage への新しいクライアントリリースのアップロード, 2 ページ](#)
- [サポートされているデバイスとサービスプロバイダーの確認, 2 ページ](#)
- [ユーザが iPhone を持たない場合の、Apple Push Notification サービスの無効化, 4 ページ](#)

## クライアントソフトウェアおよびサポートされるデバイスのリストの入手方法

サポートされているプラットフォーム、デバイス、サービスプロバイダー、および言語用の Cisco Mobile for BlackBerry および Cisco Unified Mobile Communicator クライアントソフトウェアは、.oar という拡張子が付いた 1 つのファイルで配布されます。

この .oar ファイルはまた、サポートされているモバイルデバイスやオペレーティングシステムのバージョンを識別します。また Release 3.x クライアントでは、サポートされているサービスプロバイダーも識別します。



**重要** iPhone ユーザは Cisco Mobile クライアント ソフトウェアを Apple App Store から入手しますが、すべてのユーザが iPhone を使用する場合でも、最新の .oar ファイルを入手およびアップロードする必要があります。

.oar ファイルはディスクで入手できます。または、次の手順で Cisco.com からダウンロードできます。

#### 手順

- ステップ 1 次のサイトにアクセスします。 <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001428>
- ステップ 2 適切なクライアントリリースを Cisco Unified Mobility Advantage サーバからアクセスできるボリュームにダウンロードします。

## Cisco Unified Mobility Advantage への新しいクライアントリリースのアップロード

新しいデバイスとクライアントソフトウェアバージョンをサポートするための新しいクライアント ファイルをアップロードします。

#### 手順

- ステップ 1 [Handset Platform Management] の横の [+] を選択します。
- ステップ 2 [Upload New Version] を選択します。
- ステップ 3 [Browse] を選択し、クライアント ファイルを探します。  
このファイルには、.oar 拡張子が付いています。
- ステップ 4 [Submit] を選択します。  
アップロードが完了すると、サポートされているクライアントの要約が表示されます。
- ステップ 5 [Here] を選択して要約を終了します。

## サポートされているデバイスとサービスプロバイダーの確認

導入環境でサポートされるデバイスとクライアントバージョンを選択します。

Cisco Unified Mobility Advantage が、Release 3.x クライアントでサポートするデバイスは、国やサービス プロバイダーによって異なります。Release 7.x クライアントでのサポートは、国やサービス プロバイダーとは関係ありません。この項の手順に従って、使用可能なデバイスオプションを表示して選択します。

サポートされる国、サービス プロバイダー、デバイスを制限できます。サポート対象を増やすと、ユーザの柔軟性を高めることができます。サポート対象を減らすと、クライアントベースの管理が簡単になります。



#### 重要

- ユーザが Cisco Unified Mobility Advantage サーバからクライアント ソフトウェアをダウンロードするかどうかに関係なく、導入環境でサポートされるすべてのクライアントを選択する必要があります。

たとえば、iPhone がサポートされる場合、ユーザは Apple App Store からクライアント ソフトウェアをダウンロードしますが、iPhone を選択し、サポートされるデバイスとして有効にする必要があります。

- 既存のクライアント リリースからアップグレードする場合：

新しいリリースのサポートを有効にする際、従来のリリースを絶対に選択解除しないでください。解除すると、ユーザ デバイスにある既存のクライアントのプロビジョニングが即座に解除されてしまいます。まずユーザに新しいリリースへの移行を指示し、移行後、古いリリースに対するサポートを選択解除します。

#### 手順

**ステップ 1** [Handset Platform Management] の横の [+] を選択します。

**ステップ 2** [Provisioning Management] を選択します。

**ステップ 3** [Provisioning Configuration] を選択します。

**ステップ 4** 国を選択して、その国でサポートされているサービス プロバイダーを表示します。次の場合、[Other] を選択します。

- 必要な国が表示されない。
- 必要なデバイスまたはプラットフォームが、必要な国の下に表示されない。

**ステップ 5** サービス プロバイダーを選択して、そのプロバイダーがサポートしているデバイスを表示します。必要なプロバイダーが表示されない場合は、[Other] を選択します。

**ステップ 6** サポートする国、サービス プロバイダー、およびデバイスを選択します。エンティティを選択すると、そのエンティティのリスト内にある各項目が選択されます（リストが表示されているかどうかは関係ありません）。必要に応じて項目の選択を解除するか、サポートする各デバイスを選択して開始します。

**ステップ 7** [Submit] を選択します。

---

## ユーザがiPhoneを持たない場合の、ApplePushNotificationサービスの無効化

ユーザが iPhone を持たない場合は、Apple Push Notification サービス（APNS）を無効にします。  
この機能はデフォルトで有効になっています。

### 手順

---

- ステップ 1 Admin Portal にサインインします。
  - ステップ 2 [System Management] の横の [+] を選択します。
  - ステップ 3 [APNS Configuration] を選択します。
  - ステップ 4 [Enable APNS] で [False] を選択します。
  - ステップ 5 [Submit] を選択します。
  - ステップ 6 変更が完了したら、Cisco Unified Mobility Advantage を再起動します。
-





## 第 2 章

# Cisco Unified Mobility Advantage でクライアントにメッセージと通知を送信するための設定

---

- [Cisco Unified Mobility Advantage でクライアントにプロビジョニングメッセージを送信するための設定, 5 ページ](#)
- [iPhone クライアントへの不在着信およびボイスメールの通知, 6 ページ](#)

## Cisco Unified Mobility Advantage でクライアントにプロビジョニングメッセージを送信するための設定

Cisco Unified Mobility Advantage から iPhone および BlackBerry デバイスへの、プロビジョニングメッセージ（ユーザがクライアントアプリケーションを使用できるように、すばやく簡単に設定するためのメッセージ）などの E メール メッセージ送信を有効化します。

### 操作を行う前に

SMTP Server で、Cisco Unified Mobility Advantage からのリレーが有効になっている必要があります。詳細については、SMTP サーバ管理者にお問い合わせください。または、お使いの SMTP サーバのマニュアルを参照してください。

### 手順

---

- ステップ 1 [System Management] の横の [+] を選択します。
- ステップ 2 [SMTP Server Configuration] をクリックします。
- ステップ 3 情報を入力します。

オプション	説明	設定した値
[Host Name]	SMTP ゲートウェイのホスト名。Exchange サーバを SMTP ゲートウェイとして使用している場合は、Exchange ホスト名と同じである必要があります。	
[Port]	SMTP ゲートウェイのポート番号。通常は 25 です。	
[Authentication Required]	組織のメール サーバで認証が必要かどうかを識別します。このフィールドの値が [True] の場合、Admin Email アカウントのパスワードを入力する必要があります（次の 2 つのオプションを参照）。	
[Admin Email]	Cisco Unified Mobility Advantage の管理を担当する管理者の E メールアドレス。  Cisco Unified Mobility Advantage は、この E メールアドレスを使用して、BlackBerry ユーザにプロビジョニングメッセージやアラートを送信し、iPhone ユーザにプロビジョニングメッセージを送信します。	
[SMTP Authentication Password]	Admin Email アドレスに関連付けられているパスワード。  SMTP サーバで認証が必要な場合に限り、このパスワードが必要です。	

ステップ 4 [Submit] を選択します。

ステップ 5 左側のナビゲーションバーで、[System Management] の [System Properties] を選択します。

ステップ 6 [Domain] に、ユーザの E メールアドレスを補完するドメイン（cisco.com など）を入力します。Cisco Unified Presence を導入する場合、このドメインは、[Cisco UP SIP Proxy Service Parameters] ページで指定される Cisco Unified Presence サーバのプロキシドメインに一致する必要があります。

ステップ 7 Cisco Unified Mobility Advantage を再起動して設定を有効にします。

## iPhone クライアントへの不在着信およびボイスメールの通知

クライアントが動作していない場合、Cisco Unified Mobility Advantage は Apple が提供する Apple Push Notification サービス（APNS）を使用して、iPhone ユーザに新しいボイスメッセージおよび不在着信を通知します。この機能はデフォルトで設定され、有効になっていますが、重要な要件に関してはこのトピックの前提条件を参照してください。

この機能は、直接ソケット接続を通じて、暗号化されたデータを APNS ゲートウェイに送信します。

この機能を無効にすると、iPhone ユーザは、次にクライアントアプリケーションを起動させるまで、デスクフォンの電話番号への新しいボイスメッセージと不在着信について知ることはできません。

### 操作を行う前に

Cisco Unified Mobility Advantage は Apple Push Notification サービス ゲートウェイ (gateway.push.apple.com) にポート 2195 でアクセスできる必要があります。このアドレスおよびポートに telnet 接続できることを確認します。Cisco Unified Mobility Advantage サーバがこのサービスにアクセスできない場合、このトピックの手順を使用して機能を無効にします。

### 手順

- ステップ 1 Admin Portal にサインインします。
- ステップ 2 [System Management] の横の [+] を選択します。
- ステップ 3 [APNS Configuration] を選択します。
- ステップ 4 情報を入力します。

オプション	値
[Enable APNS]	[True] を選択すると、クライアントが動作していないときに、iPhone ユーザが新しいボイスメッセージと不在着信の通知を受け取ることができます。  セキュリティ上の懸念がある場合または Cisco Unified Mobility Advantage が APNS サーバにアクセスできない場合は、[False] を選択します。
[APNS gateway IP address]	gateway.push.apple.com  この値は自動的に入力されます。正当な理由のある場合以外はこの値を変更しないでください。
[APNS port]	2195  この値は自動的に入力されます。正当な理由のある場合以外はこの値を変更しないでください。
[Security Context]	<b>apns_production</b>  このセキュリティコンテキストは、このリリースのインストール時に自動的に作成されます。削除または修正しないでください。

**ステップ 5** [Submit] を選択します。

**ステップ 6** 変更が完了したら、Cisco Unified Mobility Advantage を再起動します。

---



## 第 3 章

# BlackBerry デバイス用 Cisco Mobile または Cisco Unified Mobile Communicator の導入

Cisco Mobile は、BlackBerry デバイス用 Cisco Unified Mobile Communicator クライアント Release 7.1 の名称です。



重要

導入環境では、BlackBerry 用の Release 7.1 クライアントまたは BlackBerry 用の Release 3.x クライアントのいずれかをサポートできますが、両方はサポートできません。

- BlackBerry 用の Release 3.x クライアントの導入について、9 ページ
- BlackBerry 用の Release 7.1 クライアントの導入方法、10 ページ

## BlackBerry 用の Release 3.x クライアントの導入について



重要

導入環境では、BlackBerry 用の Release 7.1 クライアントまたは BlackBerry 用の Release 3.x クライアントのいずれかをサポートできますが、両方はサポートできません。

BlackBerry デバイス用 Cisco Unified Mobile Communicator の Release 3.x をサポートする場合は、次の手順を実行します。

- この章のその他の手順は省略します。代わりに [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuma/7\\_0/english/install/guide/cuma\\_70\\_IAG\\_17a\\_BB\\_clients.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuma/7_0/english/install/guide/cuma_70_IAG_17a_BB_clients.html) の手順に従って、BlackBerry Enterprise Server の設定を行います。
- サーバ、クライアントおよびユーザの設定は、Cisco Unified Mobility Advantage のマニュアルセットにあるすべての一般的な手順に従います。個別の要件はすべて、関連する章に説明されています。

## BlackBerry 用の Release 7.1 クライアントの導入方法

特に断りがない限り、ユーザのシステムに Cisco 適応型セキュリティ アプライアンスが含まれているかどうかに関係なく、このセクションのすべての手順を実行します。

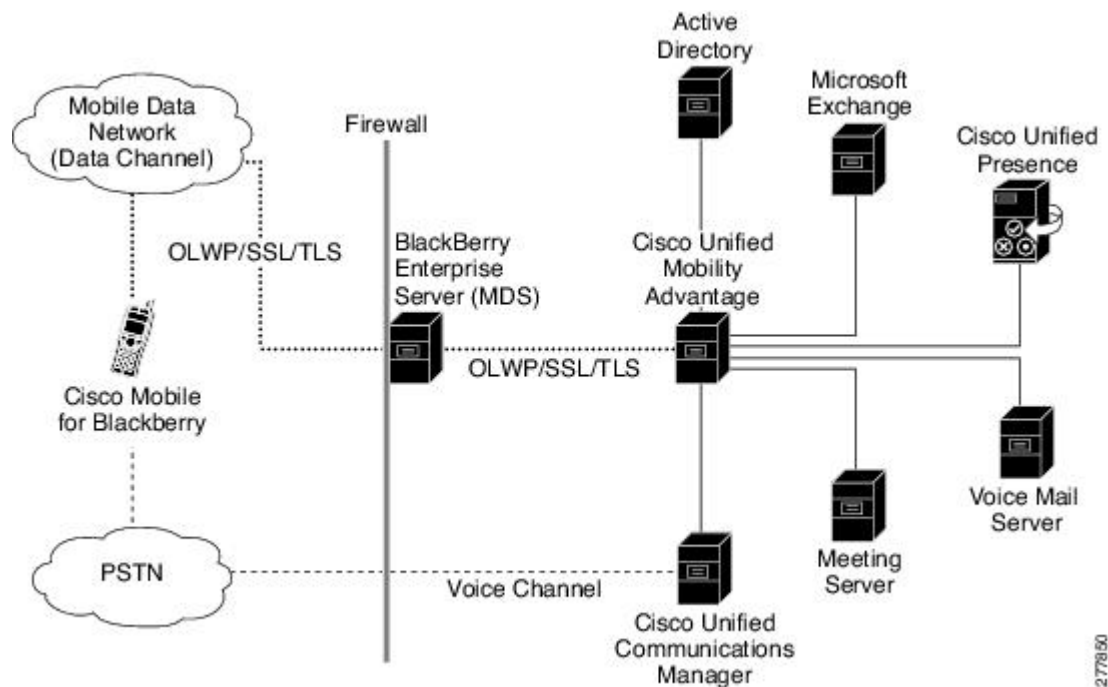
### BlackBerry Enterprise Server によるクライアント接続

BlackBerry クライアントの Release 7.1 は、Cisco 適応型セキュリティ アプライアンスではなく BlackBerry Enterprise Server 経由で、Cisco Unified Mobility Advantage サーバに接続します。

BlackBerry デバイスおよび BlackBerry クライアントの Release 7.1 のみを含む導入の場合、Cisco 適応型セキュリティ アプライアンスは必要ありません。

他のデバイス タイプを含む導入の場合、システムは Cisco 適応型セキュリティ アプライアンスが必要です。

図 1 : BlackBerry Enterprise Server を使用した導入



### BlackBerry クライアント導入の要件および制約事項

- このリリースをサポートしている正しいリリースの Cisco Unified Mobility Advantage が用意されていることを確認します。 [http://www.cisco.com/en/US/products/ps7270/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html) の『Compatibility Matrix』を参照してください。

- Cisco Unified Mobility Advantage に対して公開されているアップデートを <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001413> で確認します。
- 導入に BlackBerry デバイスのみが含まれている場合、システムに Cisco 適応型セキュリティアプライアンスは必要ありません。代わりに、BlackBerry Enterprise Server (BES) が、必要なセキュリティを提供できるからです。  
この設定がポート変換をサポートしないことに注意してください。
- BlackBerry Enterprise Server (BES) がインストールされ、セットアップのタイプが「BlackBerry Enterprise Server with BlackBerry MDS Connection Service」に設定されている必要があります。BES サーバは、Cisco Unified Mobility Advantage の導入前に、動作している必要があります。  
すでに導入済みのセットアップタイプは変更できません。詳細については、BlackBerry Enterprise Server のマニュアルを参照してください。サポートについては、Research in Motion (RIM) にお問い合わせください。
- BES/MDS の管理は、その製造業者である Research In Motion (RIM) が提供するマニュアルに従い、BES 管理者が実行する必要があります。
- サポートされているクライアントリリースについては、[http://www.cisco.com/en/US/products/ps7270/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html) の『Compatibility Matrix』を参照してください。
- 社内 WiFi を通じて Cisco Mobile を Cisco Unified Mobility Advantage に接続する場合、BlackBerry デバイスがネットワークに接続できる必要があります。この目的のための、Cisco Mobile に固有の要件はありません。

## BlackBerry デバイスにモバイルボイスシステム (MVS) がともにインストールされている場合の要件

BlackBerry モバイルボイスシステム (MVS) が Cisco Mobile と BlackBerry デバイス上で共存している場合は、次の手順を実行します。

- MVS と Cisco Mobile の両方をインストールしているユーザに Cisco Mobile ([Settings]) で Mobile Connect (Single Number Reach) を無効にするよう指示します。
- BlackBerry 以外のデバイスのユーザが存在し、それらのデバイスのユーザに Dial Via Office 機能を提供するように Cisco Unified Communications Manager を設定する場合は、[http://www.cisco.com/en/US/products/ps7270/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html) で『Configuring Features in Cisco Unified Mobile Advantage: Dial Via Office』ドキュメントモジュールを参照してください。

MVS ユーザには、このマニュアルで説明されているユーザごとまたはデバイスごとの設定を行わないでください。

- Cisco Unified Mobility Advantage Admin Portal の Dial via Office 機能が有効か無効かを判断します ([Enterprise Configuration] > [Manage Adapter Services] > [Call Control Service])。[Submit] を選択して、変更をすべて送信します。実行中のシステムを変更する場合は、Managed Server サービスを再起動する必要があります ([Server Controls] > [Cisco] > [Control Server])。
  - すべてのユーザが MVS を使用できる場合は、この機能は無効にします。

- 他のデバイスの多くのユーザに対して Dial Via Office 機能を提供する場合、Dial Via Office 機能を有効にすることが考えられます。その場合、MVS ユーザに対して、Cisco Mobile クライアントではこの機能を使用しないように通知します。

## BlackBerry デバイス用 Release 7.1 をサポートするための Cisco Unified Mobility Advantage の設定方法

### セキュアなトランザクションの確保について

トランザクションのセキュリティを確保するために、接続されたサーバの識別情報を検証し、クライアントとサーバ間で送信されるデータを暗号化することを推奨します。

この目的のために、サポートされている公認の認証局によって署名された証明書を Cisco Unified Mobility Advantage 上に導入します。またそのサーバ経由で接続されるデバイスのために、署名された証明書を Cisco 適応型セキュリティアプライアンス上に導入することもできます。手順については、[http://www.cisco.com/en/US/products/ps7270/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html) で、このリリースの『*Configuring Security*』ドキュメントモジュールを参照してください。

また BlackBerry Enterprise Server 上にも MDS セキュリティ設定を指定します。これについては、次で説明します。

### Cisco Unified Mobility Advantage からの BlackBerry クライアント インストーラのダウンロード

#### 操作を行う前に

クライアント ソフトウェアを Cisco Unified Mobility Advantage にアップロードします。[Cisco Unified Mobility Advantage への新しいクライアント リリースのアップロード](#)、2 ページを参照してください。

#### 手順

- ステップ 1 Cisco Unified Mobility Advantage Admin Portal にサインインします。
- ステップ 2 [Handset Platform Management] の横の [+] を選択します。
- ステップ 3 [Version Management] を選択します。
- ステップ 4 BlackBerry デバイスの横の [Download] を選択し、クライアントの .zip ファイルをシステムにダウンロードします。
- ステップ 5 .zip ファイルを解凍します。



## ネットワーク プロパティの設定 (Cisco 適応型セキュリティ アプライアンスを使用しない導入の場合のみ)

導入環境に BlackBerry 以外のデバイスが含まれる場合、この手順は使用しないでください。代わりに、初期設定の際に入力した、Cisco 適応型セキュリティ アプライアンスを使用した導入に必要な設定をそのまま使用します。

### 手順

- ステップ 1 Cisco Unified Mobility Advantage を実行している場合は、停止してください。
- ステップ 2 [System Management] の横の [+] を選択します。
- ステップ 3 [Network Properties] を選択します。
- ステップ 4 情報を入力します。

設定	説明
[Proxy Host Name]	Cisco Unified Mobility Advantage サーバのホスト名を入力します。
[Proxy Client Connection Port]	[Client Connection Port] に入力したのと同じ値を入力します。
[Proxy Client Download Port]	ダミーの値を入力します。
[Client Connection Port]	BlackBerry クライアントは BlackBerry Enterprise Server 経由でこのポートに接続します。 許可された範囲 : 5400 ~ 5500 デフォルト値 : 5443
[User Portal Port]	ポート ユーザが User Portal へのアクセスに使用するポート。 範囲は 9400 ~ 9500 です。 デフォルトは 9443 です。 セキュリティ上の理由から、このポートは、企業ファイアウォール内でのみ利用可能にする必要があります。
[Client Download Port]	デフォルトの値をダミーの値としてそのまま使用します。 BlackBerry ユーザは、BlackBerry Enterprise Server からクライアントを入手します。
[Security Context]	このセキュリティ コンテキストには、Cisco Unified Mobility Advantage が BlackBerry クライアントに表示する署名付き証明書が保存されます。

ステップ 5 [Submit] を選択します。

ステップ 6 設定の変更が完了したら、Cisco Unified Mobility Advantage を起動します ([Server Controls] > [Cisco] > [Control Server])。

## Cisco Mobile を配布およびサポートするための BlackBerry Enterprise Server の設定方法

### BlackBerry Enterprise Server からのサードパーティアプリケーションのダウンロード許可



(注) セキュリティ上の理由から、BlackBerry Enterprise Server の設定によっては、サードパーティのアプリケーションをダウンロードできないことがあります。BlackBerry デバイスに Cisco Mobile を導入するには、サードパーティのアプリケーションのダウンロードを一時的に許可する必要があります。

ポリシーおよびソフトウェア設定の設定値については、『*BlackBerry Enterprise Server Policy Reference Guide*』を参照してください。

#### 手順

ステップ 1 BlackBerry Manager を開きます。

ステップ 2 [Global] を選択します。

ステップ 3 [Edit Properties] を選択します。

ステップ 4 [IT Policy Administration] ウィンドウの [IT Policies] を選択します。

ステップ 5 [IT Policies] を強調表示し、画面の右端にある [More] ボタンを選択します。プロビジョニング済みのポリシーが表示されます。

ステップ 6 [Properties] を選択します。

ステップ 7 [Security Policy Group] を選択します。

ステップ 8 [Disallow Third Party Application Download] 設定で、[False] を選択します。

ステップ 9 [Allow Internal Connections] を [True] に設定します。

ステップ 10 [Allow External Connections] を [True] に設定します。

ステップ 11 [OK] を選択します。

## BlackBerry Enterprise Server へのクライアントソフトウェアの配置

操作を行う前に

[Cisco Unified Mobility Advantage](#) からの BlackBerry クライアントインストーラのダウンロード、12 ページの手順を完了します。

手順

- 
- ステップ 1** BlackBerry Enterprise Server 上で次の場所に移動し、新しい共有に Cisco Mobile ファイルを配置します。  
**C:\Program Files\Common Files\Research In Motion**
- ステップ 2** クライアントファイル用の **\Shared\Applications** という名前のプレースホルダフォルダを作成します。  
**C:\Program Files\Common Files\Research In Motion\Shared\Applications**
- ステップ 3** 作成した **\Applications** フォルダ内にこのリリース用の新しいフォルダを作成します。たとえば **\cisco\_mobile** となります。  
Release 3.x からのアップグレードの場合、リリースごとに異なったフォルダ名を使用します。
- ステップ 4** **\cisco\_mobile** フォルダに、次の 2 つのファイルを配置します (XX は言語を表します)。  
**cisco\_umc\_XX.cod**  
**cisco\_umc\_XX.alx**
- ステップ 5** **loader.exe** プログラムを実行します。  
a) **Apploader** ディレクトリに変更します。  
**C:\Program Files\Common Files\Research In Motion\Apploader**  
b) **loader.exe /index** を実行します。
- ステップ 6** フォルダを共有として設定します。  
a) 次の場所に移動します。  
**C:\Program Files\Common Files\Research In Motion**  
b) Share Permissions フォルダの [Group or user names] で [Everyone] を選択します。  
c) [Permissions for Everyone] で、[Read] の横の [Allow] を選択します。
- ステップ 7** [OK] を選択します。
- 

## ユーザがクライアントアプリケーションを使用できるようにするには

Cisco Mobile がユーザのデバイスに無線でプッシュするように、BlackBerry Enterprise Server を設定します。

## 手順

- 
- ステップ 1 BlackBerry Manager を開き、BlackBerry ドメインを選択します。
  - ステップ 2 [Software Configurations] タブを選択します。
  - ステップ 3 [Manage Application Policies] を選択します。
  - ステップ 4 [Policy] を選択してから [Properties] を選択します。
  - ステップ 5 [Internal Network Connection] プロパティを [Allowed] に設定します。
- 

## ソフトウェア設定ファイルの作成とユーザへの導入



- 
- (注) 詳細については、RIM のマニュアル『*Creating a Software Configuration - BlackBerry Enterprise Server Quick Start Supplement*』を参照してください。
- 

## 手順

- 
- ステップ 1 BlackBerry Manager-Security Administrator Authority にサインインします。
  - ステップ 2 (ウィンドウ上部の) BlackBerry ドメインの [Software Configurations] タブを選択します。
  - ステップ 3 [Add New Configuration] を選択します。
  - ステップ 4 Cisco Mobile アプリケーションが含まれているソフトウェア設定ファイルの名前と説明を、[Configuration Name] フィールドと [Configuration Description] フィールドに入力します。  
たとえば Cisco\_Mobile\_Deployment となります。
  - ステップ 5 [Device Software Share Location] フィールドに、(ローカル ファイルパスではなく) UNC 名を入力します。
  - ステップ 6 [OK] を選択します。  
デバイスのソフトウェアとアプリケーションのリストが表示されます。このリストには、Cisco Mobile アプリケーションが含まれます。
  - ステップ 7 [Delivery] を [Wireless Only] に設定します。
  - ステップ 8 [Policies] ボタンを選択します。
  - ステップ 9 Application Control ポリシーを次のように設定します。

設定	値
[Cross Application Communication]	[Allow]
[Internal network Connections]	[Allow]
[External network Connections]	[Allow]

設定	値
[Local Connection]	[Allow]
[Phone Access]	[Allow]
[Email]	[Allow]
[User Data]	[Allow]
[Event Injection]	[Allow]
[Bluetooth Serial Profile]	[Allow]
[Security Data]	[Allow]
[Blackberry Device Keystore Medium Security]	[Allow]

ステップ 10 [OK] を選択します。

ステップ 11 BlackBerry Handheld Manager を起動します。

ステップ 12 [Users] を選択します。

ステップ 13 ユーザ名を選択します。

ステップ 14 [Device Management] の下で [Assign Software Configuration] を選択します。

ステップ 15 この手順の最初に作成した Cisco Mobile ソフトウェア設定ファイルの名前を探します。  
たとえば **Cisco\_Mobile\_Deployment** となります。

ステップ 16 [OK] を選択します。

BlackBerry Enterprise Server は、4 時間ごとに BlackBerry デバイスをポーリングします。その際に、BlackBerry Enterprise Server は新規または不足アプリケーションをデバイスに導入します。

## BlackBerry Enterprise Server での MDS 接続サービス ポリシーの設定

トランザクションのセキュリティを確保するために、接続されたサーバの識別情報を検証し、クライアントとサーバ間で送信されるデータを暗号化することを推奨します。

### 操作を行う前に

Cisco Unified Mobility Advantage の署名付き SSL 証明書の導入手順については、[http://www.cisco.com/en/US/products/ps7270/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html) でこのリリースの『Configuring Security』ドキュメント モジュールを参照してください。

## 手順

---

- ステップ 1 BlackBerry Manager を開きます。
  - ステップ 2 [Explorer View] を選択します。
  - ステップ 3 左ペインで対象の MDS サーバを選択します。
  - ステップ 4 [Edit Properties] を選択します。
  - ステップ 5 左ペインで [TLS/HTTPS] を選択します。
  - ステップ 6 [Allow Untrusted TLS Connections] で [False] を選択します。
  - ステップ 7 [OK] を選択します。
-