VMware Horizon Mobile Manager のインストールおよび構成ガイド

Horizon Mobile Manager 1.3

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001072-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります

VMware の Web サイトでは最新の製品アップデートも提供されています。

このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware Horizon Mobile Manager のインストールおよび構成ガイド

『VMware Horizon Mobile Manager のインストールおよび構成ガイド』 は、VMware® Horizon Mobile Manager™ 仮想アプライアンスのインストールおよび構成方法とインストール操作の確認方法についての情報を提供します。

Horizon Mobile Manager 仮想アプライアンスは、Horizon Mobile ソリューションで使用されるサーバ側のコンポーネントを提供します。サーバ側のコンポーネントの全体のインストールおよび構成プロセスには次の項目が含まれます。

1 使用するデプロイの構成の決定

2 仮想アプライアンスのデプロイ

3 仮想アプライアンスのパワーオン

4 アプライアンスそのものの設定の構成

5 選択したデプロイの構成に必要な項目のインストールおよび構成

6 選択したデプロイの構成に従った、Horizon Mobile Manager の設定の構成

7 選択した設定を適用するための再起動

8 使用する適切なデジタル ID 証明書のアプローチ方法の決定と、任意でのデフォルトの証明書の置き換え

対象読者

この情報は、システム管理者としての経験があり、仮想マシン テクノロジーおよびデータ センターの運用に詳しい方を対象としています。

1 デプロイの構成

Horizon Mobile Manager 仮想アプライアンスは、ユーザーのモバイル デバイス上のビジネス ワークスペースの制御、カスタマイズおよび管理を行うよう設計されています。このアプライアンスは、サーバ側の管理機能を提供する組み込み Apache 2.2 サーバを使用し、Secure Sockets Layer （SSL） プロトコル接続を介して通信を行います。デバイスの通信が企業ネットワークを介して、あるいはインターネットを介して行われるかに関わらず、それらのデバイス上のワークスペースの管理を仮想アプライアンスが行えるようデプロイする必要があります。

Horizon Mobile Manager の一般的なデプロイの構成を次の表に示します。

表 1-1. Horizon Mobile Manager のデプロイの構成

構成	説明	メリット	デメリット
ネットワーク非武装地帯（DMZ）内の Horizon Mobile Manager。	ネットワーク コンピューティングのネットワーク DMZ とは、内部ネットワーク サービスとインターネットとの間の混合信頼ゾーンです。この構成では、Horizon Mobile Manager の IP アドレスは外部のパブリック IP アドレスとなり、インターネット上で直接アクセス可能です。デバイスは、SSL 要求付きで Horizon Mobile Manager の パブリック IP アドレスと通信します。	■ Horizon Mobile Manager を起動し実行する最も簡単な方法です。 ■ 外部 IP アドレス以外に特別なネットワーク構成が不要です。	■ すべての Horizon Mobile Manager サービスがインターネット上に公開されるため、本番環境には不適切です。 ■ Horizon Mobile Manager と Active Directory、LDAP あるいは会社のデータベース サービスなどの企業内サービスとの間の接続は、これらのサービスへのポートが企業のファイアウォールを通してアクセス可能な状態でない限り、遮断されます。
Horizon Mobile Manager は企業の内部ネットワーク内にあり、ネットワーク アドレス変換（NAT） を使用して Horizon Mobile Manager の内部 IP アドレスを外部で利用可能な IP アドレスに変換します。	この構成では、Horizon Mobile Manager がプライベート IP アドレスを持ちます。デバイスは、SSL 要求付きで外部で利用できる IP アドレスと通信します。それらの SSL 要求は、NAT を使用して Horizon Mobile Manager のプライベート IP アドレスに変換されます。	■ Horizon Mobile Manager サービスは、企業のファイアウォール内で保護されています。 ■ ファイアウォールを通じてポートを開かなくても、Horizon Mobile Manager が Active Directory、LDAP あるいは会社のデータベースなどの内部サービスに接続することができます。 ■ NAT は、企業内で一般的に使用され、理解されているネットワーク設定です。	■ パブリック IP 要求を Horizon Mobile Manager のプライベート IP アドレス上の TCP/IP ポート 443 に変換する NAT ルールを定義する必要があります。 ■ Horizon Mobile Manager のポート 433 が NAT からの要求を受信するために公開されている必要があります。 ■ 1 つあるいは複数の外部リバース プロキシ Apache サーバを持つクラスタ化された Horizon Mobile Manager サーバの環境にとっては理想的とは言えません。
Horizon Mobile Manager は企業の内部ネットワーク内にあり、DMZ のリバース プロキシ サーバを使用してインターネット上のデバイスからの SSL 要求を処理します。	この構成では、リバース プロキシ サーバがデバイスとの SSL 通信を処理し、その後コア ネットワーク内の内部に面した側の Horizon Mobile Manager に対して新しい要求を開始します。リバース プロキシ サーバは、Horizon Mobile Manager のログイン、リースおよびダウンロード サービスの要求を Horizon Mobile Manager によって使用される固有の URL に変換します。	■ Horizon Mobile Manager サービスは、企業のファイアウォール内で保護されています。 ■ ファイアウォールを通じてポートを開かなくても、Horizon Mobile Manager が Active Directory、LDAP あるいは会社のデータベースなどの内部サービスに接続することができます。 ■ 既存の企業インフラストラクチャをより簡単に活用します。一般的には多くの企業が、リバース プロキシ サーバを利用して内部のアプリケーション サーバをインターネットから隔離しており、これらの既存のプロキシ サーバを拡張して Horizon Mobile Manager と連動させることができます。	■ リバース プロキシ サーバの設定および Horizon Mobile Manager との通信のルールの設定は、綿密に計画する必要があります。 ■ 独自の SSL 証明書を使用する SSL 通信のためのリバース プロキシ サーバを構成する必要があります。 ■ リバース プロキシ サーバが、セカンダリ インターフェイス上の Horizon Mobile Manager に対するルートを確保できるよう、ネットワーク チームの関与が必要です。

3 つの構成のうち、DMZ に Horizon Mobile Manager をインストールするのが、最も手早く操作を開始して、VMware® Horizon Mobile™ ソリューションの機能を確認できる方法です。しかし、この構成では Horizon Mobile Manager のサービスがインターネット上に公開されるため、安全性は最も低くなります。DMZ 構成の使用は、概念実証のためのデモおよびテスト目的のみに限るべきです。DMZ 構成での Horizon Mobile Manager には可視性の問題があるため、この構成で Horizon Mobile Manager を内部ネットワークで動作している Active Directory やデータベース サーバに接続するのは避けてください。概念実証のためのデモの場合、Horizon Mobile Manager アプライアンスとともにインストールされた組み込み LDAP およびデータベース サーバを使用し、組み込み LDAP 内のテスト ユーザーを特定のモバイル デバイスに割り当てて、Horizon Mobile Manager の管理機能を実証します。

リバース プロキシ サーバの利用は最も設定が複雑な構成ですが、最も安全であり、本番環境にとって最適です。

Horizon Mobile Manager 仮想アプライアンスのインストール

2

Horizon Mobile Manager は仮想アプライアンスとして分配されます。インストール プロセスの最初の手順は、Horizon Mobile Manager 仮想アプライアンスのデプロイです。

どのような OVF 1.0 準拠の仮想化プラットフォームにも、Horizon Mobile Manager 仮想アプライアンスをインストールできます。手順では、VMware vSphere® 上でのデプロイについて説明します。

vSphere で仮想アプライアンスをデプロイするには、VMware vSphere® Client™ がインストールされた Microsoft Windows デスクトップが必要です。

開始する前に

製品のダウンロード ページから、Horizon Mobile Manager OVA ファイルをダウンロードします。

手順

1 vSphere Client にログインします。

2 [ファイル] - [OVF テンプレートのデプロイ] を選択します。

3 [参照] をクリックして、Horizon Mobile Manager OVA ファイルの場所を参照して選択します。

4 [次へ] をクリックします。

5 Horizon Mobile Manager テンプレートの詳細を確認し、[次へ] をクリックします。

6 エンド ユーザー使用許諾契約書を読んで同意し、[次へ] をクリックします。

7 Horizon Mobile Manager 仮想アプライアンスの分かるような名前を入力して、[次へ] をクリックします。

8 [シン プロビジョニング フォーマット] を選択して、[次へ] をクリックします。

9 選択したオプションを確認して、[完了] をクリックします。

Horizon Mobile Manager 仮想アプライアンスがデプロイされていることを示す進行状況メッセージが表示されます。導入が完了すると、成功メッセージが表示されます。

次に進む前に

Horizon Mobile Manager 仮想アプライアンスをパワーオンして構成します。第 3 章「Horizon Mobile Manager 仮想アプライアンスの構成 (P. 13)」を参照してください。

Horizon Mobile Manager 仮想アプライアンスの構成

3

仮想アプライアンスのネットワーク アダプタを構成し、パワーオンします。仮想アプライアンスのパワーオン後、デフォルトのパスワードを変更し、固定 IP アドレスを設定し、アプライアンスのネットワーク設定を構成することで、アプライアンス自体を構成します。

開始する前に

Horizon Mobile Manager 仮想アプライアンスをインストールします。第 2 章「Horizon Mobile Manager 仮想アプライアンスのインストール (P. 11)」を参照してください。

使用するデプロイの構成を決定します。第 1 章「デプロイの構成 (P. 7)」を参照してください。

手順

1 vSphere Client で、仮想アプライアンスの［はじめに］タブの［仮想マシン設定の編集］をクリックします。

2 ［ハードウェア］タブで、選択した構成に該当するオプションにしたがって、仮想アプライアンスのネットワーク アダプタを構成します。

デプロイの構成	説明
DMZ 内の Horizon Mobile Manager	DMZ 内でネットワーク インターフェイスに接続します。
NAT を使用してパブリック IP を内部 IP に変換する 内部ネットワーク内の Horizon Mobile Manager	内部ネットワーク内でネットワーク インターフェイスに接続します。
リバース プロキシ サーバを使用して外部要求を内部 IP へプロキシする内部ネットワーク内の Horizon Mobile Manager	内部ネットワーク内でネットワーク インターフェイスに接続します。

3 vSphere Client で Horizon Mobile Manager 仮想アプライアンスをパワーオンして、［コンソール］タブをクリックします。

仮想アプライアンスのパワーオン中に、仮想アプライアンスはメッセージを表示します。エンド ユーザー使用許諾契約書を読んで同意します。

4 仮想アプライアンスがパワーオンされ、メイン メニューが表示されたら、［ログイン］を選択します。

5 アプライアンスのデフォルト値：ユーザー名 **root**、パスワード **vmware** を使用して、仮想アプライアンスの Linux オペレーティング システムにログインします。

6 セキュリティ上の理由により、デフォルトの root パスワードを変更します。

7 **exit** と入力して、メイン メニューに戻ります。

8 ［ネットワークの構成］を選択します。

9 選択したデプロイの構成に適した設定に従い、ネットワーク設定を構成します。

デプロイの構成	説明
DMZ 内の Horizon Mobile Manager	固定 IP アドレスを使用するようにアプライアンスのネットワーク設定を構成します。プロンプトに応答して、IP アドレス、ネットマスク、ゲートウェイ、DNS サーバ、ホスト名を構成します。
NAT を使用してパブリック IP を内部 IP に変換する 内部ネットワーク内の Horizon Mobile Manager	a 固定の内部 IP アドレスを使用するようにアプライアンスのネットワーク設定を構成します。プロンプトに応答して、IP アドレス、ネットマスク、ゲートウェイ、DNS サーバ、ホスト名を構成します。内部ネットワークでフォワード プロキシ サーバの使用が求められる場合は、プロキシ サーバを構成します。 b ファイアウォール上で、TCP/IP ポート 443 をアプライアンスの内部 IP アドレスにマッピングする NAT ルールを作成します。
リバース プロキシ サーバを使用して外部要求を内部 IP へプロキシする内部ネットワーク内の Horizon Mobile Manager	a 固定 IP アドレスを使用するようにアプライアンスのネットワーク設定を構成します。プロンプトに応答して、IP アドレス、ネットマスク、ゲートウェイ、DNS サーバ、ホスト名を構成します。内部ネットワークでフォワード プロキシ サーバの使用が求められる場合は、プロキシ サーバを構成します。 b 次の 2 つのネットワーク インターフェイスでリバース プロキシ サーバを設定します： ■ DMZ 内に 1 つのインターフェイス ■ 内部ネットワーク内に 1 つのインターフェイス c HTTPS 接続を有効化するようリバース プロキシ サーバを構成し、SSL プロトコル接続を使用してインターネットとプロキシ サーバとの間のトラフィックを暗号化します。 d SSL 接続を要求し、次の URI を内部ネットワーク内の Horizon Mobile Manager にプロキシするよう、プロキシ ルールを構成します： ■ `https://<your_domain_name>/provision` ■ `https://<your_domain_name>/leasing` ■ `https://<your_domain_name>/download` Horizon Mobile Manager 内の組み込み Apache サーバは、指定された TCP/IP ポート上で特定の種類の要求を待機するよう構成されています。したがって、リバース プロキシ サーバが `mod_jk` あるいは `mod_proxy_ajp` モジュールを使用している場合は、TCP/IP ポート 8009 を使用して Horizon Mobile Manager に接続してください。リバース プロキシ サーバが `mod_proxy_http` モジュールを使用している場合は、TCP/IP ポート 8080 を使用して Horizon Mobile Manager に接続してください。

[コンソール] タブで仮想アプライアンスのネットワーク設定の構成を終了したら、メイン メニューに戻ります。

これで、Horizon Mobile Manager 仮想アプライアンスの構成が完了しました。

次に進む前に

Horizon Mobile Manager 構成インターフェイスに接続して、ライセンス キーを追加して設定を構成します。第 4 章「ライセンス キーの追加 (P. 15)」および第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」を参照してください。

ライセンス キーの追加

4

構成インターフェイスを使用して、Horizon Mobile Manager を使用してワークスペースを管理するための機能を有効化するライセンス キーを追加します。 各ライセンス キーは、Horizon Mobile Manager でワークスペースの特定の数を管理するライセンスを提供します。

開始する前に

- 1 つ以上の有効なライセンス キーを取得します。 ライセンス キーは、構成インターフェイス内でシリアル番号と呼ばれる場合もあります。
- Chrome、Firefox、Internet Explorer、Safari ブラウザの最新バージョンを使用していることを確認します。

手順

1 ブラウザで、**`https://<ip_address>:5480`** の形式で、Horizon Mobile Manager 構成インターフェイスの URL を入力します。ここでは、<ip_address> は、仮想アプライアンス自体の構成時に設定したものとなります。

Web インターフェイスは自己署名証明書を使用します。

2 **`root`** ユーザーとしてログインします。

Horizon Mobile Manager 仮想アプライアンスを構成したときに設定したパスワードを使用します。 デフォルトのパスワードを変更しなかった場合は、パスワードとして **`vmware`** を入力します。

3 [Horizon] タブをクリックして、[ライセンス] をクリックします。

4 [ワークスペースのライセンスの追加] をクリックします。

5 ライセンス キー （シリアル番号） を入力して [追加] をクリックします。

有効なライセンス キーを入力すると、ライセンスの有効期限やライセンスの管理対象となるワークスペースの数など、ライセンスに関連する情報がシステムに表示されます。

次に進む前に

まだしていない場合は、Horizon Mobile Manager 設定を構成します。 少なくとも 1 回は、[設定] タブの [保存して再起動] をクリックし、Horizon Mobile Manager のインストール プロセスを完了させる必要があります。第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」を参照してください。

Horizon Mobile Manager の設定の構成 5

Horizon Mobile Manager を初めて使用する前に、特定の設定をカスタマイズするか、デフォルト値を受け入れる必要があります。［設定］タブの［保存して再起動］をクリックし、基本となるワークスペースのイメージなど、Horizon Mobile Manager 内のユーザー ワークスペースの設定に必要な要素を初期化します。

開始する前に

- Chrome、Firefox、Internet Explorer、Safari ブラウザの最新バージョンを使用していることを確認します。
- ライセンス キーを追加します。第 4 章「ライセンス キーの追加 (P. 15)」を参照してください。
- NAT またはリバース プロキシ サーバのいずれかのデプロイの構成を使用している場合は、そのデプロイの構成で使用される外部に接続する URL または IP アドレスを取得します。第 3 章「Horizon Mobile Manager 仮想アプライアンスの構成 (P. 13)」を参照してください。
- SMTP 電子メール サーバを使用した電子メール送信のための、組織の電子メール関連情報、およびテスト構成の電子メールを受信できる電子メールアドレスを入手します。
- 次の項目について、デフォルト値を使用するかカスタム値を指定するかを決定します：

データベース

組み込み VMware® vFabric™ Postgres データベース（デフォルト）か、独自の外部データベースを使用できます。次の外部データベースがサポートされます。

- Microsoft SQL Server 2008
- Oracle 11g R2

たとえば、次のような場合は外部データベースを使用することもできます：

- 会社のデータベース標準に合わせるため
- 自社の標準データベース管理の実践事項を使用した管理およびバックアップを提供するため
- 大量のユーザーを管理するときにパフォーマンスの改善またはロード バランシングを行うため

クラスタ化された構成で Horizon Mobile Manager をインストールするには、外部データベースを使用する必要があります。

ネーム サービス

Horizon Mobile Manager にユーザー アカウント情報を提供するために使用するディレクトリ サービスを決定します。デフォルトでは、仮想アプライアンスには事前構成済みの組み込み OpenLDAP サービスが含まれています。この組み込み OpenLDAP サービスは、概念実証のためのデモまたはテスト環境での試験的使用に適しています。本番環境では、組織の LDAP またはシングル ドメインの Active Directory ネーム サービスを使用してください。複数の Active Directory ドメインの使用はサポートされていません。

デフォルトのシステム管理者　選択したネーム サービス内のどのユーザーアカウントを Horizon Mobile Manager のデフォルトのシステム管理者として使用するかを決定します。デフォルトのシステム管理者は Horizon Mobile Manager 管理インターフェイスにログインでき、すべての操作を実行できます。

このアカウントの使用は、適切なユーザーへの継続操作に関するロールを割り当てるなど、Horizon Mobile Manager の初期設定時のみに限定することをお勧めします。監査証跡の一貫性を確保するため、Horizon Mobile Manager の継続的な操作は、管理者またはフリート マネージャのロールが割り当てられた Horizon Mobile Manager ユーザーによって実行される必要があります。基本要素の構成手順と初期化が完了した後、デフォルトのシステム管理者を Horizon Mobile Manager 管理インターフェイスへログインさせ、[ロール & ジョブ] ページを使用してユーザーへ適切な Horizon Mobile Manager のロールを割り当てます。

リポジトリ　Horizon Mobile Manager リポジトリのデフォルトの場所を使用するか、別の場所を指定できます。リポジトリは、ワークスペースのイメージ、アプリケーション、システムファイルなど、Horizon Mobile Manager オブジェクトを保存します。デフォルトのリポジトリ パスは、Horizon Mobile Manager 仮想アプライアンスのファイル システム内の `/opt/vmware-mmp/repo` です。

クラスタ化された構成内で Horizon Mobile Manager を使用する場合、あるいはユーザーのワークスペース内に大容量のアプリケーションを多数デプロイする予定がある場合は、仮想アプライアンスの外部のリポジトリを使用することもできます。仮想アプライアンスの最大ディスク容量は 40 GB であるため、この容量を超えるような大容量のアプリケーションを多数デプロイする予定がある場合は、適切なストレージ容量のあるリポジトリの場所を選択します。

注意　既存の Horizon Mobile Manager インストールについては、[設定] タブからいつでも設定を更新できます。ただし、Horizon Mobile Manager を初めて使用した後にこれらの設定の一部を更新すると、最初に使用した後にシステム内で発生した変更を手動で適用するという追加の操作が必要となる場合があります。たとえば、最初に組み込み OpenLDAP ネーム サービスを選択してユーザー デバイスをプロビジョニングし、その後別のネーム サービスを使用するよう設定を更新した場合は、新しいネーム サービスに同じユーザー ID を追加するまで、既存のユーザーが機能しなくなります。

手順

1　ブラウザで、**`https://<ip_address>:5480`** の形式で、Horizon Mobile Manager 構成インターフェイスの URL を入力します。

2　**`root`** ユーザーとしてログインします。

Horizon Mobile Manager 仮想アプライアンスを構成したときに設定したパスワードを使用します。デフォルトのパスワードを変更しなかった場合は、パスワードとして **`vmware`** を入力します。

3　[Horizon] タブをクリックし、[設定] をクリックします。

4　[デフォルトの管理者名] フィールドで、あるユーザー名を Horizon Mobile Manager システム管理者に指定します。

指定する名前は、Horizon Mobile Manager で使用するために選択するネームサービス内に存在している必要があります。表示されたデフォルト値（**`admin`**）は、組み込み OpenLDAP ネーム サービス内のユーザー アカウントです。このデフォルトの **`admin`** アカウントのパスワードは、**`vmware`** です。

外部のネーム サービスの使用を選択している場合は、[デフォルトの管理者名] フィールドの値を、お使いのネーム サービス内に存在する名前に更新する必要があります。

5　Horizon Mobile Manager のファイル システム リポジトリの場所を指定します。

ローカルまたはネットワークのファイル システム パスを入力できます。デフォルトのリポジトリ パスは、仮想アプライアンスのファイル システム内の `/opt/vmware-mmp/repo` です。[保存して再起動] をクリックすると、Horizon Mobile Manager が提供するデフォルトのオブジェクト（基本のワークスペースのイメージなど）が指定された場所に書き込まれます。

6 ログイン サーバ、ダウンロード サーバ、リース サーバの外部と接している root（エントリ レベル）URL を入力します。

注意 管理対象のモバイル デバイス上のワークスペースは定期的に Horizon Mobile Manager と通信するため、ログイン、リース、およびダウンロードの各サーバの URL は、ワークスペースが存在する、あるいはワークスペースをこれからインストールするデバイスからアクセス可能なものである必要があります。NAT またはリバース プロキシ サーバのいずれかのデプロイの構成を使用している場合は、その構成で使用されている外部に接している URL を入力する必要があります。

URL の先頭に **`https://`** を含めます。**`http://`** と入力した場合でも、デバイス上のワークスペースは、サーバとの通信に安全な **443** ポートを使用します。

これらの 3 つの URL は同じものであっても構いません。たとえば、パブリック IP アドレスでデプロイされた 1 つの Horizon Mobile Manager 仮想アプライアンスの単純な構成では、その仮想アプライアンスが管理、ログイン、ダウンロード、およびリースを目的としたサーバを提供する場合があります。この場合、ログイン、ダウンロード、およびリースの各サーバに指定される URL は、**`https://<ip_address>`** となります。ここでは、<ip_address> がパブリック IP アドレスとなっています。

サーバ	使用可能な状況の例
ログイン サーバ	ワークスペース ユーザーが各自のモバイル デバイス上で、ワークスペースのインストールおよびダウンロードに使用します。
ダウンロード サーバ	ワークスペースにソフトウェアを提供します。
リース サーバ	ワークスペース リースを管理します。

7 (オプション) 組み込みデータベースではなく独自の Oracle または SQL Server データベースを使用するには、 [外部データベースを使用] を選択し、ドロップダウン メニューからデータベースのタイプを選択します。次に、Horizon Mobile Manager がそのデータベース内にデータを保存し、それらにアクセスするための情報を指定します。

[アドレス（URL）]	データベースへのアドレスです。
[ユーザー名]	データベース接続のためのデータベース ユーザーです。
[パスワード]	データベース接続のためのパスワードです。
[DBA ユーザー名]	Horizon Mobile Manager が使用するデータベース オブジェクトを作成するための、DDL 権限を持つ DBA レベルのデータベース ユーザーです。
[DBA パスワード]	DBA ユーザーのパスワードです。
[検証クエリ]	データベースへの接続を検証するために使用する SQL クエリです。

外部データベースの場合は、接続プールの初期サイズなど、追加の詳細設定を指定できます。

8 (オプション) 組み込み OpenLDAP サービスではなく、自分独自のネーム サービスを使用するには、 [外部サービスを使用] を選択し、タイプを選択します。

独自の Active Directory ネーム サービスを使用している場合、Active Directory ドメインを入力する必要があります。複数の Active Directory ドメインの使用はサポートされていません。

独自の LDAP ネーム サービスを使用している場合、LDAP サーバの URL、root DN、ユーザー検索クエリを入力する必要があります。また、manager DN ユーザー名およびパスワードを入力できます。

9 Horizon Mobile Manager が組織の電子メール サーバへ接続するよう、電子メール設定を構成します：

a お使いの電子メール サーバの SMTP ホスト アドレスとポート情報を入力します。

b (オプション) SSL 暗号化を使用するには、 [SSL の使用] チェック ボックスを選択します。

c (オプション) 認証を使用するには、 [認証の使用] チェック ボックスを選択し、SMTP 認証を実行するためのユーザー名とパスワードを指定します。

d 受信者の電子メールアドレスを指定し、[電子メールの送信] をクリックして確認電子メールを送信することで、構成のテストを行います。

システムがその SMTP 情報を使用して電子メールの送信に成功すると、確認電子メールに検証コードが記載されます。

e 確認電子メールからコードを取得し、そのコードを [テスト電子メールからのコード] フィールドに入力します。

10 [保存して再起動] をクリックし、構成設定を保存し、Horizon Mobile Manager を使用したワークスペースの設定と従業員のデバイスの管理に必要な基本要素を初期化します。

再起動が実行されていることを示すメッセージが表示されます。

再起動プロセスが完了すると、Horizon Mobile Manager が初期化され、デフォルトのシステム管理者に指定されたユーザー アカウントを使用して管理インターフェイスにログインできるようになります。

注意 管理インターフェイスにログインする前に、[保存して再起動] をクリックし、基本要素が初期化されていることを確認する必要があります。保存して再起動しないと、一部の必要な要素が使用できない場合があります。

次に進む前に

これで、Horizon Mobile Manager でワークスペース ユーザーを構成できます。ブラウザで、**https://<ip_address>** の形式で、Horizon Mobile Manager 管理者インターフェイスの URL を入力します。

組み込みネーム サービスを指定して、システム管理者名のデフォルト値を変更していない場合は、ユーザー名 **admin** とパスワード **vmware** で管理インターフェイスにログインできます。

Horizon Mobile Manager の使用方法の詳細については、ログイン後にオンライン ヘルプを参照してください。

Horizon Mobile Manager で使用する NDES 設定の構成

6

Horizon Mobile Manager には、Microsoft Network Device Enrollment Service （NDES） 用の Simple Certificate Enrollment Protocol （SCEP） コネクタ プラグインが含まれています。 この SCEP コネクタ プラグインは、Horizon Mobile Manager と会社の Microsoft NDES サーバとの間の接続をサポートし、管理対象のデバイスのデジタル証明書の作成プロセスを自動化します。

開始する前に

- Chrome、Firefox、Internet Explorer、Safari ブラウザの最新バージョンを使用していることを確認します。
- ライセンス キーを追加します。 第 4 章「ライセンス キーの追加 (P. 15)」を参照してください。
- Horizon Mobile Manager の設定を構成し、 [保存して再起動] をクリックしてシステムを初期化します。 第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」を参照してください。

手順

1 ブラウザで、**`https://<ip_address>:5480`** の形式で、Horizon Mobile Manager 構成インターフェイスの URL を入力します。

2 **`root`** ユーザーとしてログインします。

Horizon Mobile Manager 仮想アプライアンスを構成したときに設定したパスワードを使用します。 デフォルトのパスワードを変更しなかった場合は、パスワードとして **`vmware`** を入力します。

3 [Horizon] タブをクリックし、次に [SCEP] をクリックします。

Horizon Mobile Manager が提供する NDES コネクタが、SCEP コネクタ リストに一覧表示されます。

4 [SCEP サーバの追加] をクリックします。

[SCEP サーバの追加] ウィンドウで、下記の情報を入力します。

サーバ名	会社で使用している Microsoft NDES サーバの名前。
外部 URL	NDES クライアントが会社の Microsoft NDES サーバに接続する際に使用する URL。
SCEP コネクタ	NDES サーバに接続するために使用される SCEP コネクタ プラグイン。 提供された NDES コネクタが表示されます。
管理者 URL	管理者が会社の Microsoft NDES サーバを管理するときに使用する URL。
管理者ユーザー名	会社の NDES 管理者のユーザー名。
管理者パスワード	会社の NDES 管理者のパスワード。
ドメイン	会社の NDES 管理者アカウントが作成された Windows ドメインの名前。

5 NDES サーバ情報を Horizon Mobile Manager に追加するには、 [追加] をクリックします。

デジタル証明書と Horizon Mobile Manager

7

Horizon Mobile Manager は、標準デジタル証明書を使用してセッション情報を暗号化し、SSL プロトコル接続を介して Horizon Mobile Manager とモバイル デバイスとの間の通信を行います。デプロイ環境において、Horizon Mobile Manager がデバイスに対して有効な証明書を示すことが可能で、さらにそれらのデバイスのワークスペースで使用されている署名付き証明書を伝達できる状況がサポートされている必要があります。

Horizon Mobile Manager とモバイル デバイスとの間の通信に使用されている証明書は次のとおりです：

SSL 証明書	サーバとクライアント（モバイル デバイス）間の安全なセッションを暗号化します。
署名証明書	サーバとクライアント間の通信にデジタル署名します。
ルートおよび中間の認証局（CA）証明書	特定の SSL または署名証明書が信頼できるかどうかを判断するための証明書の信頼チェーンを提供します。

初回の Horizon Mobile Manager のインストールと構成時に、自動生成された内部ルート認証局（CA）と、構成ユーザー インターフェイスに入力されたサーバの URL を使用して、自己署名 SSL 証明書と署名証明書が自動的に生成されます （第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」 を参照してください）。Horizon Mobile Manager の管理インターフェイスの [セキュリティ] ページには、自動的に生成された証明書のエイリアスが一覧表示されます。

デフォルトの構成の場合、Horizon Mobile Manager は、これらの自動的に生成された自己署名証明書を使用します。デフォルトの証明書を使用するか、それらを独自の証明書で置き換えるかを決めるには、次を考慮する必要があります。

- どちらの方法が選択したデプロイの構成により適しているか。
- デバイスの所有者にどのような要件を課すことが可能か。自己署名の SSL 証明書を使用することによって、デバイス所有者に対し、デバイスがサーバと確実に通信できるように各デバイスの認証設定の更新を要求することになります （「自己署名の SSL 証明書を使用する場合のモバイル デバイスの要件 (P. 24)」を参照してください）。

注意 Horizon Mobile Manager によって使用されているリース サーバの URL を変更すると、組み込み Apache サーバ内のデフォルトの証明書の置き換えによる変更は失われます。リース サーバの URL は、（第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」 に記載されているように） Horizon Mobile Manager の構成インターフェイス内で設定されます。構成インターフェイスの [保存して再起動] ボタンをクリックすると、そのリース サーバの URL をドメインとして使用した、内部 MVP ルート CA によって署名された新しいデフォルトの証明書がシステムによって自動的に生成されます。新しく生成された証明書は以前に使われていた証明書に置き換わります。このため、デフォルトの証明書を独自の証明書で置き換えて、その後にリース サーバの URL を変更する場合、証明書の置き換えプロセスを繰り返し行わなくてはなりません。

デプロイ構成による証明書のアプローチ方法

次の表は、各デプロイ構成に適したオプションの概要を示すものです。

表 7-1. Horizon Mobile Manager のデプロイ構成と適切な証明書のアプローチ方法

構成	証明書の選択
ご使用のネットワーク DMZ 内の Horizon Mobile Manager	■ 組み込み Apache サーバ内の、デフォルトの自己署名の証明書を使用します。 ■ 組み込み Apache サーバ内の、デフォルトの自己署名の証明書を独自の証明書と置き換えます。その証明書は、自己署名されたもの、または信頼性のある CA により署名されたものになります。デフォルトの証明書を置き換えるときに、ルートの CA 証明書および証明書の信頼チェーン内にあるすべてのすべての中間の CA 証明書をアップロードする必要があります。「デフォルトの証明書を信頼性のある署名付き証明書で置き換え (P. 25)」および「DMZ または NAT デプロイ構成でのデフォルトの SSL 証明書の置き換え (P. 25)」を参照してください。
企業の内部ネットワーク内にあり、NAT を使用している Horizon Mobile Manager	■ 組み込み Apache サーバ内の、デフォルトの自己署名の証明書を使用します。 ■ 組み込み Apache サーバ内の、デフォルトの自己署名の証明書を独自の証明書と置き換えます。その証明書は、自己署名されたもの、または信頼性のある CA により署名されたものになります。デフォルトの証明書を置き換えるときに、ルートの CA 証明書および証明書の信頼チェーン内にある中間の CA 証明書をアップロードする必要があります。「デフォルトの証明書を信頼性のある署名付き証明書で置き換え (P. 25)」および「DMZ または NAT デプロイ構成でのデフォルトの SSL 証明書の置き換え (P. 25)」を参照してください。
企業の内部ネットワーク内にあり、DMZ のリバース プロキシ サーバを使用している Horizon Mobile Manager	リバース プロキシ サーバを使用する場合、そのサーバが SSL 通信用として構成されていることが必要なため、ご使用のリバース プロキシ サーバでは独自の SSL 証明書を使います。この証明書は、自己署名されたもの、または信頼性のある CA により署名されたものになります。この構成では、ルートの CA 証明書および SSL 証明書の信頼チェーン内にあるすべての中間の CA 証明書をアップロードする必要があります。「デフォルトの証明書を信頼性のある署名付き証明書で置き換え (P. 25)」および「リバース プロキシ サーバのデプロイ構成での独自の信頼性のある署名付き SSL 証明書の使用 (P. 27)」を参照してください。

この章では次のトピックについて説明します。

自己署名の SSL 証明書を使用する場合のモバイル デバイスの要件

自動的に生成された証明書は一意であり、サーバの最初の利用あるいは概念実証による利用は可能ですが、信頼性が高いことで有名な CA によって署名されているものではありません。このため、デバイス所有者が VMware® Switch アプリケーションを起動して最初にビジネス ワークスペースをインストールする前に、Switch アプリケーションのデフォルトの認証設定を更新する必要があります。

Horizon Mobile Manager が自己署名の SSL 証明書を使用するとき、デバイス所有者は Switch アプリケーションの設定で [サーバの認証] チェック ボックスの選択を解除する必要があります。このチェック ボックスは、Switch アプリケーションのインストール時にデフォルトで選択されます。[サーバの認証] チェック ボックスが選択されていて、SSL 証明書が自己署名証明書である場合、デバイスは証明書の確認に有名な CA の Android トラスト ストアを使用しようとします。証明書が有名な CA によって署名されていないため、セッションの認証が失敗し、デバイスは Horizon Mobile Manager への接続を拒否します。

Horizon Mobile Manager のデプロイが自己署名の SSL 証明書（デフォルトで自動的に生成された証明書または独自の自己署名の証明書） を使用している場合、デバイス所有者に対して、ワークスペースの初回インストール時に Switch アプリケーションを開始する前に［サーバの認証］チェック ボックスが選択解除されているか確認するよう通知されます。このチェック ボックスの選択が解除されると、デバイスは SSL 証明書が自己署名されており Horizon Mobile Manager への接続が許可されているものであるという事実を無視します。Switch アプリケーションの［サーバの認証］設定をデバイス上に表示するには、デバイスの［アプリケーション設定］画面で、［VMware Switch］をタッチし、［スペースの管理］をタッチします。

注意 ［サーバの認証］チェック ボックスの選択が解除され、デバイス所有者が初回のインストールを開始すると、通信が SSL プロトコルによるセキュアな状態であっても、この状況についてユーザーに警告するメッセージが表示されます。

デフォルトの証明書を信頼性のある署名付き証明書で置き換え

デフォルトの自己署名 SSL 証明書を信頼性のある認証局 （CA） によって署名された証明書で置き換えると、デバイスの所有者が Switch アプリケーションの設定を変更する必要がなくなります。

注意 デフォルトの SSL 証明書を信頼性のある CA によって署名された証明書で置き換えることにメリットはありますが、一般的に自動的に生成された内部 CA ルート （internal-ca-root）の証明書に対するセキュリティ上の疑義がない限り、デフォルトの署名付き証明書を置き換えることに明確な理由はありません。

DMZ または NAT デプロイの場合、組み込み Apache サーバの自動生成された SSL 証明書を独自の署名付き SSL 証明書で置き換えます。リバース プロキシ サーバの構成では、独自の信頼性のある署名付き SSL 証明書をリバース プロキシ サーバで使用します。すべてのデプロイ構成において、独自の証明書 （SSL または署名付き） を使用する場合、Horizon Mobile Manager にルートの CA 証明書と、置換用証明書の信頼チェーン内にあるすべての中間の CA 証明書をアップロードする必要があります。

デフォルトの SSL 証明書または署名付き証明書を独自の信頼できる署名付き証明書に置き換えるための一般的な手順は次のとおりです。

1 プライベート キーおよび証明書署名要求 （CSR） を生成します。

2 自分の証明書に署名を付ける認証局 （CA） に CSR を送信します。

CA から、自分の証明書によって使用されるルート CA および中間 CA 証明書の信頼性のある証明書チェーンとともに、署名付き証明書が送られてきます。

3 署名付き証明書および自分の証明書に署名を付けた CA 証明書をロードして、Horizon Mobile Manager によって使用できるようにします。

DMZ または NAT 構成	信頼性のある SSL 証明書を仮想アプライアンスのコンソールから組み込み Apache サーバにロードします。管理インターフェイスを使用して置換用署名付き証明書をロードします。
リバース プロキシ サーバ構成	信頼性のある SSL 証明書をご使用のリバース プロキシ サーバにロードします。管理インターフェイスを使用して置換用署名付き証明書をロードします。
すべての構成	管理インターフェイスを使用して置換用証明書 （SSL または署名付き） に対応するルートおよび中間 CA 証明書をロードします。

DMZ または NAT デプロイ構成でのデフォルトの SSL 証明書の置き換え

DMZ または NAT のデプロイ構成で Horizon Mobile Manager を使用するときに、独自の信頼された署名付き SSL 証明書を使用するには、自動生成された証明書を独自の証明書に置き換えてください。

開始する前に

Horizon Mobile Manager 仮想アプライアンスをインストールし、構成します。

vSphere Client で仮想アプライアンスをパワーオンし、［コンソール］タブをクリックして、仮想アプライアンスの Linux オペレーティング システムに **root** ユーザーとしてログインします。仮想アプライアンスを構成したときに設定したパスワードを使用します。デフォルトのパスワードを変更しなかった場合は、パスワードとして **vmware** を入力します。

手順

1 仮想アプライアンスのコンソールで、次のコマンドを実行し、プライベート キーと CSR を生成します。

```
openssl req –out CSR.csr –new –newkey rsa:2048 –nodes –keyout privateKey.key
```

コマンドで、CSR に必要な情報が求められます。

2 プロンプトで、自分の組織に該当する情報を入力します。

Common Name には、デバイスの所有者が Switch アプリケーションに入り、サーバにログインして最初にワークスペースを設定するのに必要な完全修飾ドメイン名を入力します。このドメイン名は次の条件を満たす必要があります：

- この Horizon Mobile Manager デプロイで使用されるパブリック IP アドレスを外部的に解決できる完全修飾ドメイン名であること。
- 仮想アプライアンスの構成時に［ログイン サーバ URL］（URL の https:// を除いた部分）に入力したものと、同じ外部と接している URL であること。

たとえば、次のコード ブロックは、<our.domainname.com> のログイン サーバ URL のエントリを示します。

```
Generating a 2048 bit RSA private key
.............................................+
++.....+++
writing new private key to 'privateKey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Massachusetts
Locality Name (eg, city) [ ]:Cambridge
Organization Name (eg, company) [Internet Widgets Pty Ltd]:OurCompany
Organizational Unit Name (eg, section) [ ]:OurUnit
Common Name (eg, YOUR name) [ ]:our.domainname.com
Email Address [ ]:ourwebmaster@ourcompany.com
Please enter the following 'extra' attributes to be sent with your certificate
request
A challenge password [ ]:
An optional company name [ ]:
```

このコマンドでは、**CSR.csr** と **privateKey.key** という 2 つのファイルが生成されます。

3 **CSR.csr** ファイルを認証局に送信します。認証局から、署名付き証明書（**cert.pem** など）、証明書によって使用されるルートおよび中間 CA 証明書、およびその中で使用する証明書チェーン ファイル（**chain.pem** など）が送信されます。

4 Horizon Mobile Manager の管理インターフェイスに管理者としてログインします。ブラウザで、**https://<ip_address>** の形式で、Horizon Mobile Manager 管理 URL へ進みます。ここで、<ip_address> は、Horizon Mobile Manager のプライベート IP アドレスです。管理者ロールが割り当てられている Horizon Mobile Manager ユーザー アカウントを使用してログインします。デプロイが、組み込みネーム サービスを使用するよう構成されており、システム管理者名のデフォルト値を変更していない場合は、**admin** ユーザー名と **vmware** パスワードで管理インターフェイスにログインできます。

5 [セキュリティ] をクリックして [セキュリティ] ページを表示します。

6 [サーバ信頼証明書チェーン] セクションで、SSL 証明書に署名したルート CA 証明書および中間 CA 証明書をアップロードします。[新規証明書のアップロード] ボタンをクリックして各証明書をアップロードします。

この手順によって、モバイル デバイスのプロビジョニング時に、SSL 通信を信頼するために必要なルート CA 証明書と中間 CA 証明書がデバイス上のワークスペースのキーストアに確実に含まれるようになります。

注意 十分に管理された状況の場合を除き、[サーバ信頼証明書チェーン] リスト内の証明書、特にルート CA 証明書（デフォルトの MVP 内部 CA 証明書を含む）を削除しないでください。[サーバ信頼証明書チェーン] リストからルート CA 証明書を削除すると、次のリース更新操作でプロビジョニングされたすべてのデバイスからその証明書が削除されます。置換用のルート証明書を提供していない場合は、プロビジョニングされたこれらのデバイスをワイプし、再プロビジョニングする必要があります。リストから証明書を削除しなければならないケースは非常にまれです。このリストから証明書を削除する唯一の理由は、その証明書が侵害されていることが疑われる場合のみです。この場合は、特殊な手順に従って、ユーザー デバイスにすでにインストールされているワークスペースが機能し続けるようにしなければなりません（「プロビジョニングしたワークスペースのルート CA および中間 CA 証明書の変更 (P. 29)」 を参照）。

7 この Horizon Mobile Manager インスタンスによってすでにデバイスがプロビジョニングされている場合は、すべてのデバイスがリース呼び出しを行えるように、リース更新時間が経過するまで待機してください。リースが更新されたら、ルート CA 証明書と中間の CA 証明書がワークスペースに送信されます。リース更新時間が経過するまで待機すると、新しい SSL 証明書が組み込み Apache サーバで使用される前に、署証明書信頼チェーンがワークスペースのキーストアに確実にインストールされます。

注意 切断され、リース間隔よりも長い期間ネットワークにアクセスしていないデバイスは、この手順では新しい証明書を取得することができません。新しい証明書を取得していないなど、リース間隔を超過する期間切断されているデバイス上のワークスペースは、デバイスのネットワーク アクセスが回復しても、サーバとの SSL 通信を信頼しません。通信を有効化するためには、これらのワークスペースをワイプし、再プロビジョニングする必要があります。

8 `scp` コマンドを使用し、署名付き SSL 証明書を仮想アプライアンスのファイルシステムにセキュア コピーします。

9 仮想アプライアンスのファイル システムでは、`/etc/apache2/vhosts.d/mmp.conf` ファイルを編集し、SSL 証明書ファイルに関連する行がファイル内に存在することを確認し、パスが証明書および生成されたプライベート キーを指していることを確認します。

例：

```
SSLCertificateFile /path/to/the/signed/cert.pem
SSLCertificateKeyFile /path/to/your/generated/privateKey.key
SSLCertificateChainFile /path/to/the/cert/chain.pem
```

10 次のコマンドを使用して Apache サーバを再起動します：`/etc/init.d/apache2 graceful`

再起動後、組み込み Apache サーバで新しい SSL 証明書が使われるようになります。

リバース プロキシ サーバのデプロイ構成での独自の信頼性のある署名付き SSL 証明書の使用

リバース プロキシ サーバを使用する場合、そのサーバが SSL 通信用として構成されていることが必要なため、ご使用のリバース プロキシ サーバでは独自の SSL 証明書を使います。この証明書は、自己署名証明書でも、信頼できる CA の署名付きのものでも構いませんが、デフォルトの自己署名 SSL 証明書を信頼できる CA の署名付きのものに置き換えるメリットの 1 つとして、デバイスの所有者が Switch アプリケーションの [サーバの認証] チェック ボックスを選択解除する必要がないという点が挙げられます。

このデプロイ構成では、Horizon Mobile Manager にルート CA 証明書および SSL 証明書の信頼チェーンで使用されているすべての中間 CA 証明書をアップロードする必要があります。ワークスペースを最初にデバイスにインストールするときに、正しい信頼チェーンを持つよう、デバイスのプロビジョニングの前に信頼チェーンのアップロードを実行することをお勧めします。

開始する前に

Horizon Mobile Manager 仮想アプライアンスをパワーオンします。

手順

1 Horizon Mobile Manager の管理インターフェイスにログインします。ブラウザで、**`https://<ip_address>`** の形式で、Horizon Mobile Manager 管理 URL へ進みます。ここで、<ip_address> は、Horizon Mobile Manager のプライベート IP アドレスです。管理者ロールが割り当てられている Horizon Mobile Manager ユーザーを使用してログインします。デプロイが、組み込みネーム サービスを使用するよう構成されており、システム管理者名のデフォルト値を変更していない場合は、**`admin`** ユーザー名と **`vmware`** パスワードで管理インターフェイスにログインできます。

2 [セキュリティ] をクリックして [セキュリティ] ページを表示します。

3 [サーバ信頼証明書チェーン] セクションで、SSL 証明書に署名したルート CA 証明書および中間 CA 証明書をアップロードします。[新規証明書のアップロード] ボタンをクリックして各証明書をアップロードします。

この手順によって、モバイル デバイスのプロビジョニング時に、SSL 通信を信頼するために必要なルート CA 証明書と中間 CA 証明書がデバイス上のワークスペースのキーストアに確実に含まれるようになります。

注意 十分に管理された状況の場合を除き、[サーバ信頼証明書チェーン] リスト内の証明書、特にルート CA 証明書（デフォルトの MVP 内部 CA 証明書を含む）を削除しないでください。[サーバ信頼証明書チェーン] リストからルート CA 証明書を削除すると、次のリース更新操作でプロビジョニングされたすべてのデバイスからその証明書が削除されます。置換用のルート証明書を提供していない場合は、プロビジョニングされたこれらのデバイスをワイプし、再プロビジョニングする必要があります。リストから証明書を削除しなければならないケースは非常にまれです。このリストから証明書を削除する唯一の理由は、その証明書が侵害されていることが疑われる場合のみです。この場合は、特殊な手順に従って、ユーザー デバイスにすでにインストールされているワークスペースが機能し続けるようにしなければなりません（「プロビジョニングしたワークスペースのルート CA および中間 CA 証明書の変更 (P. 29)」 を参照）。

この時点で、リバース プロキシ サーバを使用したデバイスのプロビジョニングが可能になります。

デフォルトの署名付き証明書の置き換え

自動的に生成される内部 CA ルート証明書が侵害されたと考えられる場合を除いて、通常は、デフォルトの署名証明書を置き換える大きな理由はありません。

開始する前に

Horizon Mobile Manager 仮想アプライアンスをパワーオンします。

手順

1 管理インターフェイスに管理者としてログインし、[セキュリティ] をクリックして [セキュリティ] ページを表示させます。

2 [署名付きサーバ証明書] セクションの [証明書署名要求の生成] ボタンをクリックして、CA に送信する CSR を生成します。

3 E メールで CSR を CA に送信します。

4 CA から新しい署名付き証明書と、CA による署名付きのルート CA 証明書および中間の CA 証明書が返送されてきたら、[セキュリティ] ページの [サーバ信頼証明書チェーン] セクションを展開し、[新規証明書のアップロード] をクリックしてそれぞれのルート CA 証明書および中間の CA 証明書をアップロードします。

注意 手順 5 が完了し、リース更新時間が経過するまで、[サーバ信頼証明書チェーン] リスト内の証明書、特にルート CA 証明書（デフォルトの MVP 内部 CA 証明書を含む）を削除しないでください。

5 すべてのデバイスがリース呼び出しを行えるように、リース更新時間が経過するまで待機します。リースが更新されたら、ルート CA 証明書と中間の CA 証明書がワークスペースに送信されます。リース更新時間が経過するまで待機すると、新しい署名証明書を有効にする前に、署名証明書の置き換えのための証明書信頼チェーンがワークスペースのキーストアに確実にインストールされます。

注意 切断され、リース間隔よりも長い期間ネットワークにアクセスしていないデバイスは、この手順では新しい証明書を取得することができません。新しい証明書を取得していないなど、リース間隔を超過する期間切断されているデバイス上のワークスペースは、ネットワーク アクセスが回復しても正常に機能しません。これらのワークスペースはワイプし、再プロビジョニングする必要があります。

6 [セキュリティ] ページで、[サーバ署名証明書] セクションを展開し、[新規証明書のアップロード] をクリックして CA から送信された新しい署名証明書をアップロードします。

7 [署名証明書] ドロップダウン リストを使用して、新しい署名証明書を選択して有効化します。

注意 手順 8 が完了し、2 回目のリース更新時間が経過するまで、[署名付きサーバ証明書] リストから以前使用していた署名証明書を削除しないでください。

8 すべてのデバイスが別のリース呼び出しを行えるように、リース更新時間が経過するまで待機します。リースが更新されたら、有効な署名証明書として新しい署名証明書がワークスペースに送信されます。リース更新時間が経過するまで待機すると、古い署名証明書をリストから削除する前に、ワークスペースのメッセージへの署名に新しい証明書が使用されていることを確認することができます。

注意 切断され、リース間隔よりも長い期間ネットワークにアクセスしていないデバイスは、この手順にある新しい有効な署名証明書を使用することはできません。リース間隔を超過する期間切断されているデバイス上のワークスペースは、ネットワーク アクセスが回復しても正常に機能しません。これらのワークスペースはワイプし、再プロビジョニングする必要があります。

9 [セキュリティ] ページで、[サーバ署名証明書] リストを展開し、古い署名証明書を削除します。この時点で、古い署名証明書に関連付けられていたルート CA 証明書と中間の CA 証明書が新しい署名証明書で使用されていないのであれば、それらの CA 証明書を削除することもできます。

この時点で、置き換える署名証明書は、デバイスが使用する有効な証明書になります。

プロビジョニングしたワークスペースのルート CA および中間 CA 証明書の変更

プロビジョニングされたワークスペースでは、管理インターフェイスで指定された証明書信頼チェーンを使用して、サーバ側の SSL 証明書と Horizon Mobile Manager が使用する署名証明書の ID が確認されます。この証明書信頼チェーンは、ワークスペースがデバイスにプロビジョニングされるときに、ワークスペースにデプロイされます。証明書信頼チェーンの証明書が侵害されているおそれがある場合は、この一連の手順を実行して、侵害された証明書を置き換える必要があります。

この一連の手順を実行すれば、信頼チェーンから個々の証明書を削除する前に、新しい証明書信頼チェーンをプロビジョニングされたワークスペースに確実にデプロイできます。これらの手順を実行せずにデプロイされた信頼証明書チェーンが破損した場合（ワークスペースが置き換えるルート CA 証明書を取得可能になる前に、ルート CA 証明書を削除した場合など）、デバイスのワークスペースは正常に機能しなくなり、ワークスペースのワイプと再プロビジョニングが必要となります。

開始する前に

Horizon Mobile Manager 仮想アプライアンスをパワーオンします。

手順

1 Horizon Mobile Manager の管理インターフェイスに管理者としてログインし、[セキュリティ] をクリックして [セキュリティ] ページを表示させます。

2 [新規証明書のアップロード] をクリックして各証明書を追加し、新しいルート CA 証明書と中間の CA 証明書を [サーバ信頼証明書チェーン] セクションに追加します。

3 すべてのデバイスがサーバにリース呼び出しを行えるように、リース更新期間が経過するまで待機します。リースが更新されたら、指定したルート CA 証明書と中間の CA 証明書（新旧の証明書の両方を含む）のセットがワークスペースにデプロイされます。

4 リース更新期間が経過した後で、[サーバ信頼証明書チェーン] セクション内の侵害された証明書の横の [削除] ボタンをクリックできます。

次のリース更新時に、証明書信頼チェーンがプロビジョニングされたワークスペースに再度デプロイされますが、これに削除済みの侵害された証明書は含まれません。それ以降は、ワークスペースで更新された証明書信頼チェーンが使用されます。

注意 切断され、リース間隔よりも長い期間ネットワーク アクセスをしていないデバイスは新しい証明書を取得することができません。新しい証明書を取得していないなど、リース間隔を超過する期間切断されているデバイス上のワークスペースは、ネットワーク アクセスが回復しても正常に機能しません。これらのワークスペースはワイプし、再プロビジョニングする必要があります。

証明書の信頼チェーンから誤って削除されたルート CA 証明書のリカバリ

Horizon Mobile Manager 管理者が [サーバ信頼証明書チェーン] リストのルート CA 証明書の横の [削除] を誤ってクリックした場合、ルート CA 証明書を削除すると致命的な障害が発生する場合があることを示す警告が表示されます。ルート CA 証明書が削除されると、プロビジョニング済みのワークスペースはサーバと信頼性のある通信を行うことができなくなる場合があります。管理者が置き換え手順を実行せずにルート CA 証明書を削除する処理を選択し、その後、以前の構成への復元が必要となった場合、次の手順を使用することで、削除されたルート CA 証明書を証明書信頼チェーンに復元することができます。

開始する前に

vSphere Client で仮想アプライアンスをパワーオンし、[コンソール] タブをクリックして、仮想アプライアンスの Linux オペレーティング システムに **root** ユーザーとしてログインします。仮想アプライアンスを構成したときに設定したパスワードを使用します。デフォルトのパスワードを変更しなかった場合は、パスワードとして **vmware** を入力します。

手順

1 次のコマンドを実行します。

```
su tcserver
mkdir /opt/vmware-mmp/repo/security/certs-for-devices/internal-ca-root
cp /opt/vmware-mmp/repo/security/root/cert.pem /opt/vmware-mmp/repo/security/certs-for-devices/internal-ca-root/
```

2 管理インターフェイスで、[セキュリティ] ページを更新します。ルート CA 証明書が [サーバ信頼証明書チェーン] リストに復元されます。

次に進む前に

削除されたルート CA 証明書を復元した後、復元された証明書信頼チェーンがデバイスにデプロイされるように、ワークスペースのワイプと再プロビジョニングが必要となります。

8 手動での確認テスト

これらの手動でのテストを使用してご使用の Horizon Mobile Manager のインストールが VMware® Ready™ スマートフォン上でワークススペースのプロビジョニングおよび管理が可能か確認します。

これらのテストを開始する前に、次の項目があることを確認します。

- インストールされていて、構成済みおよびパワーオン状態の Horizon Mobile Manager インスタンス。
- 次を搭載している VMware Ready スマートフォン。
  - Horizon Mobile Manager インスタンスへのデータ アクセス（Wi-Fi、3G、LTE）。
  - アクティブな Wi-Fi 接続。
  - 装着済みの SIM カード。
  - インストールされている VMware Switch アプリケーション。VMware Switch アプリケーションは、Google Play から入手できます。

    信頼性のある署名付き SSL 証明書を使用するように Horizon Mobile Manager インスタンスを構成していない場合、Switch の設定で［サーバの認証］チェック ボックスが選択解除されていることを確認します。「自己署名の SSL 証明書を使用する場合のモバイル デバイスの要件 (P. 24)」を参照してください。
- Horizon Mobile Manager のデフォルトのシステム管理者の名前およびパスワード（第 5 章「Horizon Mobile Manager の設定の構成 (P. 17)」を参照してください）。
- 3 名のテスト ユーザー （その名前およびパスワード）。これらのユーザーはご使用の Horizon Mobile Manager インスタンスで使われる名前付けサービス内に存在している必要があります。名前付けサービスは Horizon Mobile Manager 仮想アプライアンスのインストールおよび構成の最中に指定されます。ご使用のインスタンスが事前構成された組み込み OpenLDAP サービスを使用している場合は、**user20**、**user21**、および **user22** のような事前構成されたユーザーを 3 つ使用します。3 つの事前構成されたユーザーのパスワードは **vmware** です。
- ブランディングおよび壁紙のテスト手順で使う 5 つの画像ファイル （JPG または PNG 形式）。使用可能な画像のサイズはそれぞれ次のようになります。
  - Horizon Mobile Manager サイトのロゴの画像： 80 ピクセル x 50 ピクセル。
  - ログイン画面イメージ： 600 ピクセル x 400 ピクセル。
  - デバイス上の会社ロゴの画像： 200 ピクセル x 200 ピクセル。
  - ワークスペースの壁紙の画像 （2 つのファイル）： 960 ピクセル x 640 ピクセル。
- この Horizon Mobile Manager インスタンス用のログイン サーバーの URL。
- ワークスペース上のショートカットで使う URL （所属する会社の Web サイトの URL など）。

VMware Email クライアント アプリケーションが関与するテストでは、（デバイス ユーザーによって使用される） 電子メール クライアントのアカウントおよび電子メール サーバー （Microsoft Exchange または VMware Zimbra のいずれか） への Wi-Fi アクセスが必要になります。

次の用語が確認テストで使用されます。

管理者	Horizon Mobile Manager で管理者ロールが割り当てられたユーザーのことを意味します。
オペレーション マネージャ	Horizon Mobile Manager でオペレーション マネージャ ロールが割り当てられたユーザーのことを意味します。
パーソナル フォン	個人使用の電話を意味します。ワークスペースのインストール後、電話にはパーソナル フォンとワークスペースという 2 つの側面が生じます。電話にインストールされたワークスペースがある場合、 [Switch] アイコンをタッチしてこの 2 つの側面を切り替えることが可能です。

この章では次のトピックについて説明します。

ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成

本番環境では、管理業務を実行するための各自の責任に応じて組織内の個人にロールを割り当てます。このテストでは、そのようなユーザーにロールを割り当てることができることを検証します。

Horizon Mobile Manager 仮想アプライアンスの初期構成中に、ユーザー アカウントがデフォルトのシステム管理者として指定されます。デフォルトのシステム管理者は管理インターフェイスにログインでき、すべての操作を実行できます。ただし、初期設定後、監査証跡の一貫性を確保するため、継続的な操作は、管理者またはオペレーション マネージャとしての特定のロールが割り当てられたユーザーによって実行される必要があります。システムは、ログインしているユーザーに対して、そのユーザーに割り当てられているロールが実行する権利を持つ操作の種類に対応した機能のみを表示します。標準のロールに関連する操作の説明については、Horizon Mobile Manager Administration のオンライン ヘルプを参照してください。

注意 組み込み OpenLDAP サービスを利用するインスタンスの場合は、このテストに **user20** および **user21** を使用できます。管理者ロールを **user20** に、オペレーション マネージャ ロールを **user21** に割り当てます。両方のユーザーのパスワードは **vmware** です。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

手順

1 Horizon Mobile Manager にデフォルトのシステム管理者（Horizon Mobile Manager のこのインスタンスの構成中に指定されたもの）としてログインします。構成プロセス中に組織でデフォルト値が保持されている場合は、ユーザー名が **admin**、パスワードが **vmware** となります。

2 左側のナビゲーションで［ロールとジョブ］をクリックし、［編集］をクリックします。

3 組織内で、これらの責任を持たせたいユーザーに対して、管理者またはオペレーション マネージャのロールを割り当てます。

   a ［ロールの追加］列で、ユーザーを検索します。システムがユーザー名を表示したら、［ロールの追加］をクリックします。そのユーザーに該当するロールを選択します。たとえば、このテストについて事前構成済みのユーザーを使用する場合は、**user20** に管理者ロールを割り当てます。

   b 手順 3a を繰り返し、追加のユーザーにロールを割り当てます。たとえば、このテストについて事前構成済みのユーザーを使用する場合は、**user21** にオペレーション マネージャ ロールを割り当てます。

4 ［保存］をクリックします。

次に進む前に

割り当てられたロールが有効であることを確認します：

1 オペレーション マネージャ ロールのみが割り当てられているユーザー（**user21** など）として管理インターフェイスにログインします。左側のナビゲーションに、次の名前が表示されていることを確認します：［ダッシュボード］、［ユーザー］、［グループ］、［ポリシー設定］、［テンプレート］、［ワークスペース イメージ］、［アプリケーション］。［ロールとジョブ］、［ブランディング］、［セキュリティ］については、それらに関連付けられている操作を実行する権利が管理者ロールのものであるため、左側のナビゲーションには表示されません。

2 管理者ロールのみが割り当てられているユーザー（**user20** など）として管理インターフェイスにログインします。左側のナビゲーションに、次のページ名が表示されていることを確認します。［ダッシュボード］、［ロールとジョブ］、［ブランディング］、［セキュリティ］。管理者ロールには、表示された選択肢に関連する操作を実行する権利しかないため、その他の選択肢は表示されません。

テンプレートの作成

このテストでは、テンプレートを作成します。テンプレートでは、ユーザーのモバイル デバイスにデプロイできるビジネス ワークスペースを定義します。テンプレートは、ワークスペースに含まれるソフトウェア、およびワークスペースのホーム画面の壁紙の背景とショートカットを決定します。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の手順を完了させます。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左側のナビゲーションで［テンプレート］をクリックし、［新規テンプレートの作成］をクリックします。

3 次のような、名前と説明を入力します：

- ［名前：］**Sales Template**
- ［説明：］**Template for employees in the Sales organization**

4 [すべてのアプリケーション] セクションで、緑色の [+] のアイコンをクリックし、ワークスペースに VMware View アプリケーションを含めます。[デプロイされたアプリケーション] のセクションに VMware Email と VMware View の 2 つのアプリケーションが表示されていることを確認します。

5 [カスタマイズ] セクションで次を行います。

a [新規アップロード] をクリックして壁紙を変更します。壁紙の名前（**Our Wallpaper** など）を入力し、960 x 640 ピクセルのイメージ ファイルのいずれかを参照します。[保存] をクリックし、ドロップダウン メニューを使用して壁紙を選択します。

b [ショートカットの追加] をクリックし、名前と URL（会社のメインの Web サイトなど）を入力します。

6 [保存] をクリックします。

次に進む前に

テンプレートが作成されたことを確認します：

1 左側のナビゲーションで、[テンプレート] の下に自分のテンプレート名が表示されていることを確認します。

2 そのテンプレート名をクリックし、2 つのアプリケーション（VMware Email と VMware View）および指定したショートカットが表示されることを確認します。

ポリシー設定の作成

このテストでは、ポリシー設定を作成します。ポリシー設定は、デバイス ユーザーがビジネス ワークスペースで実行できる操作、およびパスワードの強度や有効期限などのセキュリティ設定を制御します。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の手順を完了させます。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左側のナビゲーションで [ポリシー設定] をクリックし、[新規ポリシー設定の作成] をクリックします。

3 次のような、名前と説明を入力します：

- [名前：] **Sales Group Policies**
- [説明：] **Policy settings for employees in the Sales organization**

4 [ワークスペース リースの更新] セクションで、20 分間隔を選択します。自動無効化または自動ワイプの設定は変更しないでください。

5 [パスワード] のセクションを展開します。[パスワードの必要性] が選択されており、[パスワードの強度] が [PIN] に設定されていることを確認します。

6 [保存] をクリックします。

次に進む前に

ポリシー設定が作成されたことを確認します：

1 左側のナビゲーションで、[ポリシー設定] の下に自分のポリシー設定名が表示されていることを確認します。

2 そのポリシー設定をクリックし、指定した説明とワークスペース リースの更新間隔が表示されていることを確認します。

グループの作成とユーザーのグループへの追加

このテストでは、デバイス ユーザーをビジネス ワークスペースに関連付けるために使用するグループを作成します。ユーザーのデバイスにビジネス ワークスペースをプロビジョニングする前に、モバイル デバイス ユーザーがグループに属している必要があります。ユーザーのグループによって、インストールされるソフトウェアや、そのデバイスにデプロイされているビジネス ワークスペースに適用されるポリシーが決まります。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されているユーザーがあることを確認します。

「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」、「テンプレートの作成 (P. 33)」、および 「ポリシー設定の作成 (P. 34)」 の手順を完了させます。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左側のナビゲーションで［グループ］をクリックし、［新規グループの作成］をクリックします。

3 次のような、名前と説明を入力します：

- ［名前：］**Sales Group**
- ［説明：］**Employees in the Sales organization**

4 「テンプレートの作成 (P. 33)」 および 「ポリシー設定の作成 (P. 34)」 で作成したテンプレートとポリシー設定を選択します。

5 ［ユーザーの追加］列の検索フィールドに、これらの検証テストで使用するよう特定したデバイス ユーザーの名前を入力します。使用可能なユーザーは、Horizon Mobile Manager インスタンスの構成で指定したネーム サービス内にあります。このインスタンスが組み込み OpenLDAP サービスを使用している場合は、**user23** と入力します。

6 システムがリストにユーザー名を表示したら、そのユーザーの行の［追加］をクリックします。ユーザー名は、［グループ ユーザー］の列に表示されます。これは、そのユーザーがこのグループに割り当てられていることを示しています。

7 ［保存］をクリックします。

次に進む前に

グループが作成され、選択したユーザーがそれに割り当てられていることを確認します：

1 左側のナビゲーションで、［グループ］の下に自分のグループ名が表示されていることを確認します。

2 そのグループをクリックし、選択したユーザーがリストされていること、およびワークスペースの状態が［インストール保留中］と表示されていることを確認します。状態が［インストール保留中］となっているのは、そのユーザーのデバイスにまだワークスペースがプロビジョニングされていないためです。

ワークスペースと Horizon Mobile Manager のブランディング要素の構成

このテストでは、モバイル デバイスと管理インターフェイスに表示されるブランディング要素を構成します。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されているイメージ ファイルがあることを確認します。

「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の手順を完了させます。

手順

1 管理インターフェイスに管理者（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user20** など）としてログインします。

2 左側のナビゲーションで［ブランディング］をクリックし、［編集］をクリックします。

3 ［サイト ブランディング］のセクションで次の項目を更新します：

a サイトのタイトルを **Our Site** に、ログイン画面のタイトルを **Our Horizon Mobile Manager** に変更します。

b 対応する［参照］ボタンをクリックし、600 x 400 ピクセルのイメージ ファイルを選択して、サイトのロゴを変更します。

c 対応する［参照］ボタンをクリックし、80 x 50 ピクセルのイメージ ファイルを選択して、ログイン画面のイメージを変更します。

4 ［ワークスペース ブランディング］のセクションで次の項目を更新します：

a 会社名を変更します（**Our Company** など）。この名前は、ユーザーが最初にワークスペースをプロビジョニングするときにデバイスに表示されます。

b ビジネス ワークスペースを使用するための使用条件のテキストを変更します。このテキストは、ユーザーが最初にワークスペースをプロビジョニングするときにデバイスに表示されます。たとえば、**Your use of Our Company's corporate workspace is governed by the terms of this agreement.** のように入力することができます。

c 対応する［参照］ボタンをクリックし、200 x 200 ピクセルのイメージ ファイルを選択して、会社のロゴのイメージを変更します。このイメージは、ユーザーが Switch アイコンをタッチし、ワークスペースに入ったときにデバイスに表示されます。

5 ［保存］をクリックします。

次に進む前に

サイトのブランディング要素を確認します：

1 トップ バナーに表示されているタイトルが、［サイト タイトル］フィールドで指定したタイトルであることを確認します。

2 ログアウトし、ブラウザを更新します。ログイン画面に、自分のサイト ロゴとログイン画面のイメージが表示されていることを確認します。

ワークスペースのブランディング要素は、「モバイルデバイスへのワークスペースのインストール(P.36)」 で検証されます。

モバイル デバイスへのワークスペースのインストール

このテストでは、デバイスにワークスペースをプロビジョニングします。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」、「テンプレートの作成 (P. 33)」、「ポリシー設定の作成 (P. 34)」、「グループの作成とユーザーのグループへの追加 (P. 35)」 および 「ワークスペースと Horizon Mobile Manager のブランディング要素の構成 (P. 35)」 の手順を完了させます。

手順

1 モバイル デバイスで、［Switch］アイコンをタッチします。

［VMware Switch の設定フォーム］が表示されます。

2 「グループの作成とユーザーのグループへの追加 (P. 35)」 でグループに追加したユーザーに対応するユーザー アカウントのユーザー名とパスワードを入力します。

指定したユーザーが、Horizon Mobile Manager で定義済みのどのグループにも属していない場合、そのユーザーはログインすることができず、ワークスペースをデバイスにプロビジョニングできません。

3 お使いの Horizon Mobile Manager インスタンスのログイン サーバに使用されている完全修飾ドメイン アドレスを入力します。

このアドレスは、仮想アプライアンスの構成時に、[ログイン サーバ URL] フィールドで指定されます。アドレスの **https://** の部分は入力する必要がありません。

4 [移動] をタッチします。接続が確立されたら、「ワークスペースと Horizon Mobile Manager のブランディング要素の構成 (P. 35)」 で指定した会社のブランディング要素がデバイスに表示されることを確認します。

5 [次へ] をタッチします。

ワークスペースのダウンロードおよびインストールのプロセスが始まります。デバイス上の通知を表示することで、進捗を確認できます。インストールが完了したら、次のような通知がデバイスに送信されます：`VMware Switch is ready.Touch for your workspace`

6 通知をタッチしてワークスペースを開き、パスワードの作成など、画面上の指示にしたがってください。

パスワード要件は、「ポリシー設定の作成 (P. 34)」 で指定されます。

7 (オプション) E メール アプリケーションのテスト用のアクセスを設定する E メールの認証情報を入力します。これらのテストで使用するよう指定した E メール アカウントを使用します。

[手動セットアップ] をタッチしてから [破棄] をタッチすると E メール設定プロセスを保留できます。

デバイスには、ワークスペースのホームが表示されます。

次に進む前に

「ワークスペースと Horizon Mobile Manager のブランディング要素の構成 (P. 35)」 で指定した壁紙とショートカットが表示されていることを確認します。アプリケーション表示アイコンをタッチし、「テンプレートの作成 (P. 33)」 でテンプレートに追加したアプリケーションがあることを確認します。

ワークスペースの [Switch] アイコンをタッチし、パーソナル フォンへ切り替えます。

管理対象デバイスとの相互作用に関する詳細の表示

このテストでは、オペレーション マネージャとして、Horizon Mobile Manager と管理対象デバイスとの相互作用に関する詳細を表示します。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左側のナビゲーションで、[ユーザー] をクリックします。

3 プロビジョニングされたモバイル デバイスに対応するユーザーをクリックします。

たとえば、「モバイル デバイスへのワークスペースのインストール (P. 36)」 で **user23** を使用した場合は、そのユーザーを選択します。

システムは、デバイスの更新履歴、プロビジョニング ステータス、および関連付けられているグループ、ポリシー設定、テンプレートなど、モバイル デバイスと Horizon Mobile Manager との間の相互作用に関する詳細情報を表示します。

注意 デバイスのグラフィック イメージには、ワークスペースを最初にプロビジョニングしたときからの情報が表示されます。この情報は、今後のデバイスに対する変更によるデータで更新されることはありません。

次に進む前に

「モバイル デバイスへのワークスペースのインストール (P. 36)」 で実行したプロビジョニングの相互作用が相互作用の履歴に表示されていることを確認します。

ユーザーのワークスペースの無効化及び再有効化

このテストでは、オペレーション マネージャとしてユーザーのワークスペースを無効化し、その後再度有効化します。ワークスペースが無効化されると、デバイス ユーザーはワークスペースにアクセスできなくなります。再度有効化されると、ユーザーがワークスペースにアクセスすることができます。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左側のナビゲーションで、 [ユーザー] をクリックし、プロビジョニングされたデバイスに対応するユーザーを選択します。

システムは、そのユーザーの詳細ページを表示します。

3 詳細ページで、 [無効化] をクリックしてユーザーを無効化し、確認メッセージで [OK] をクリックします。

4 パーソナル フォンで、 [設定] > [アカウントおよび同期] をタッチし、Switch アプリケーションに関連付けられているユーザー（**Switch** アイコンが付いているユーザー アカウント）をタッチします。

5 [設定] > [すぐに同期] をタッチし、Horizon Mobile Manager との同期を開始します。

デバイスが Horizon Mobile Manager サーバと通信し、ワークスペースを無効化するコマンドを受信します。

6 モバイル デバイス上の通知を開き、Switch が無効化されたという通知を表示します。

7 パーソナル フォンのアプリケーション リストで、 [Switch] アイコンをタッチします。Switch が無効であることを示すメッセージが表示されます。

8 Horizon Mobile Manager 管理インターフェイスで、トップ バナーの更新アイコンを使用し、ユーザーの詳細ページを更新します。ページには、そのユーザーの無効化されたステータスが表示されます。

9 [有効化] をクリックし、ユーザーのワークスペース アクセスを再度有効化します。

10 パーソナル フォンで、手順 4 と 手順 5 を繰り返し、モバイル デバイスをサーバと同期します。アクセスがリストアされたことを示す通知が表示されたら、 [Switch] アイコンをタッチし、デバイス上でワークスペースを開けることを確認します。

次に進む前に

ワークスペースの [Switch] アイコンをタッチし、パーソナル フォンへ切り替えます。

プロビジョニングしたワークスペースでのアプリケーションの更新

このテストでは、プロビジョニングされたワークスペースでのアプリケーションの追加および削除と、管理対象デバイスの更新を行います。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左のナビゲーションで、プロビジョニングされたワークスペースを定義するテンプレートをクリックし、[編集] をクリックします。

3 [デプロイしたアプリケーション] セクションで、アプリケーションのアイコンにある赤色の [X] をクリックし、「テンプレートの作成 (P. 33)」で追加したアプリケーション（VMware View アプリケーション）を削除します。

4 [すべてのアプリケーション] セクションから [デプロイしたアプリケーション] セクションにアプリケーションのアイコンをドラッグして、[デプロイしたアプリケーション] セクションに別のアプリケーションを追加します。手順 3 で削除したアプリケーションとは異なるアプリケーションを追加します。

5 [デプロイ] をクリックします。変更によりテンプレートに関連付けられているユーザーが影響を受けることを警告するメッセージが表示されます。[OK] をクリックします。

6 パーソナル フォンで、次の手順で電話と Horizon Mobile Manager を同期します：

   a [設定] > [アカウントおよび同期] をタッチします。

   b Switch アプリケーションに関連付けられているユーザーをタッチします。

   c [設定] > [今すぐ同期] をタッチします。

   デバイスが Horizon Mobile Manager サーバと通信を行い、更新されたテンプレートに応じてワークスペースを更新します。

7 ワークスペースに切り替え、アプリケーション セットが 手順 3 および 手順 4 で選択したものになっていることを確認します。

次に進む前に

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

プロビジョニングしたワークスペースの壁紙およびショートカットの更新

このテストでは、ワークスペースのホーム画面で使用する壁紙とショートカットを更新し、管理対象デバイスを更新します。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左のナビゲーションで、プロビジョニングされたワークスペースを定義するテンプレートをクリックし、[編集] をクリックします。

3 [カスタマイズ] セクションで、[新規のアップロード] をクリックして他の 960 x 640 ピクセルの壁紙イメージ（第 8 章「手動での確認テスト (P. 31)」 を参照）をアップロードし、ドロップダウン コントロールを使用して現在の壁紙に選択します。

4 [ショートカットの追加] をクリックし、別のショートカット（**communities.vmware.com** など）をリストに追加します。

5 [デプロイ] をクリックします。

6 「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 に記載されている方法で、パーソナル フォンで、デバイスとサーバを同期します。

7 ワークスペースに切り替え、ホーム画面の壁紙とショートカットが選択したものになっていることを確認します。

次に進む前に

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

ワークスペースのパスワード ポリシーの更新

このテストでは、プロビジョニングされたワークスペースのパスワード ポリシーを更新し、新しいポリシーを管理対象デバイスにデプロイします。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 左のナビゲーションで、プロビジョニングされたワークスペースで使用されているポリシー設定（「ポリシー設定の作成 (P. 34)」 で作成したポリシー設定）をクリックし、 [編集] をクリックします。

3 [パスワードの強度] をクリックしてセクションを展開し、パスワードの強度に [手動] を選択します。パスワードの長さを [6] 、最小桁数を [1] 、最小特殊文字数を [1] に設定します。

4 [デプロイ] をクリックし、メッセージ警告で [OK] をクリックします。

5 「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 に記載されている方法で、パーソナル フォンで、デバイスとサーバを同期します。

6 [Switch] アイコンをタッチし、ワークスペースへ切り替えます。パスワードの検証フォームに、ワークスペースの最初のプロビジョニング時に設定したパスワードを入力します（「モバイル デバイスへのワークスペースのインストール (P. 36)」）。

7 パスワードの作成フォームで、新しいパスワードを作成します。テストとして、**1234** と入力します。新しいポリシーを説明するメッセージが表示されます。

8 手順 3 で設定したポリシーと一致するパスワードを入力し、新しいパスワードを確認します。

次に進む前に

ワークスペースが表示されることを確認します。

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

位置特定サービスのポリシーの更新

このテストでは、ワークスペースの位置特定サービスに関するポリシー設定を変更し、新しい設定を管理対象デバイスにデプロイします。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 パーソナル フォンで、位置特定サービスを無効にします。

[設定] > [位置特定サービス] をタッチし、対応するチェック ボックスの選択を解除します。

2 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

3 プロビジョニングされたワークスペースで使用されているポリシー設定をクリックし、[編集] をクリックします。

4 [機能] セクションで、まだ選択されていない場合は [位置情報サービスの有効化] 選択ボックスを選択します。位置特定サービスが [高精度] に設定されていることを確認します。

5 [デプロイ] をクリックし、警告メッセージで [OK] をクリックします。

6 「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 に記載されている方法で、パーソナル フォンで、デバイスとサーバを同期します。[Switch] アイコンをタッチしてワークスペースに入るときに、ポリシー違反が発生したことを示す警告が表示されることを確認します。

   オペレーション マネージャが位置特定サービスが必要であると指定し、デバイス ユーザーがデバイスの位置特定サービスを無効にする場合はポリシー違反となり、Horizon Mobile Manager によってワークスペースが無効となります。

7 デバイスの位置特定サービスを再度有効化し、ワークスペースに切り替えます。ワークスペースに入れることを確認します。

8 パーソナル フォンに切り替え、次の手順を使用して、位置特定サービスへのアクセスをオフにするよう Switch アプリケーション設定を変更します：

   a [設定] > [アカウントおよび同期] をタッチし、Switch ユーザー アカウントをタッチします。

   b [Switch 設定の管理] をタッチします。[VMware Switch 設定の管理] 画面で、[場所] をタッチします。

   c [非表示] を選択し、Switch アプリケーションで位置特定サービスが表示されないようにします。

9 デバイスとサーバを同期します。[Switch] アイコンをタッチしてワークスペースに入るときに、ポリシー違反が発生したことを示す警告が表示されることを確認します。

   オペレーション マネージャが位置特定サービスが必要であると指定し、デバイス ユーザーが Switch 設定の位置特定サービスを無効にする場合はポリシー違反となり、Horizon Mobile Manager によってワークスペースが無効となります。

10 手順 8a と 手順 8b を繰り返し、Switch アプリケーションの位置設定を開きます。[詳細] 設定をタッチし、Horizon Mobile Manage の [高精度] 設定に合わせます（手順 4 を参照）。

11 [Switch] アイコンをタッチしてワークスペースへ切り替え、ワークスペースに切り替えることができることを確認します。

次に進む前に

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

カット/コピー/ペーストおよびカメラ機能のポリシー設定の更新

このテストでは、ワークスペースでのカット/コピー/ペーストおよびカメラ機能のポリシー設定を変更し、新しいポリシーを管理対象デバイスにデプロイします。

ポリシー設定でカット/コピー/ペースト機能が有効になっていないと、ユーザーはワークスペースからデバイスのパーソナル側にテキストをコピーできません。ポリシー設定でカメラ機能が有効になっていないと、ユーザーはワークスペースでカメラを使用できません。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 パーソナル フォンで、ワークスペースに切り替えて、カメラが使用できることを確認します。具体的には、アプリケーションを表示して、[カメラ] アイコンをタッチし、写真を撮ります。

2 ワークスペースのアプリケーションでテキストの一部をコピーし、パーソナル フォンに切り替えて、アプリケーションにテキストをペーストできることを確認します。

3 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

4 プロビジョニングされたワークスペースで使用されているポリシー設定をクリックし、[編集] をクリックします。

5 [機能] セクションで、それぞれのチェック ボックスの選択を解除して、カット/ペースト/コピー機能とカメラ機能を無効にします。[デプロイ] をクリックして、警告メッセージで [OK] をクリックします。

6 パーソナル フォンで、デバイスとサーバを同期します（「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 を参照）。手順 1 と 手順 2 を繰り返し、ワークスペースでカメラが使用できないこと、ワークスペースからパーソナル フォンにテキストをコピーおよびペーストできないことを確認します。

次に進む前に

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

プロビジョニングしたワークスペースに対するパスワード リセットの開始

このテストでは、プロビジョニングされたワークスペースのパスワードを強制的にリセットします。通常、この操作は、デバイス ユーザーがワークスペースのパスワードを忘れてしまった場合に使用します。パスワードをリセットすると、ユーザーは、新しいパスワードを設定するよう要求されます。それまでのパスワードの検証は必要ありません。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 プロビジョニングされたワークスペースに対応するユーザーのユーザー詳細ページを開きます（詳細は 「ユーザーのワークスペースの無効化及び再有効化 (P. 38)」 を参照）。

3 [パスワードのリセット] をクリックします。確認メッセージで、[OK] をクリックします。

4 「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 に記載されている方法で、パーソナル フォンで、デバイスとサーバを同期します。

5 ワークスペースに切り替えます。以前のパスワードの検証なしで、新しいパスワードを設定するよう要求されていることを確認します。

6 新しいパスワードを作成します。

次に進む前に

新しいパスワードの作成後に、デバイスにワークスペースが表示されることを確認します。

ワークスペースの [Switch] アイコンをタッチして、パーソナル フォンに切り替えます。

デバイスからプロビジョニングしたワークスペースのワイプ

このテストでは、プロビジョニングされたワークスペースをデバイスからワイプします。通常、この操作は、デバイスの紛失または盗難がユーザーから報告された際に実行します。プロビジョニングされたワークスペースをワイプすると、デバイス上のすべてのワークスペース データが削除され、デバイスからリカバリできなくなります。

開始する前に

第 8 章「手動での確認テスト (P. 31)」 に記載されている項目があることを確認します。

ワークスペースがスマートフォンに正しくプロビジョニングされたことを確認します。

手順

1 管理インターフェイスにオペレーション マネージャ（「ユーザーへのロールの割り当てによる管理者およびオペレーション マネージャの作成 (P. 32)」 の **user21** など）としてログインします。

2 プロビジョニングされたワークスペースに対応するユーザーのユーザー詳細ページを開きます（詳細は 「ユーザーのワークスペースの無効化及び再有効化 (P. 38)」 を参照）。

3 [ワイプ] をクリックします。確認メッセージで、 [OK] をクリックします。

4 パーソナル フォンで、デバイスとサーバを同期します（「プロビジョニングしたワークスペースでのアプリケーションの更新 (P. 38)」 を参照）。管理者によってワークスペースがワイプされたことを示す通知がデバイスに送信されます。

5 [Switch] アイコンをタッチし、ワークスペースへ切り替えます。

6 ［VMware Switch のセットアップ］ フォームが表示されていることを確認します。

ワークスペースは削除されているため、プロビジョニング プロセスを開始するために ［VMware Switch のセットアップ］ フォームが表示されます。

次に進む前に

この時点で、手順 「モバイル デバイスへのワークスペースのインストール (P. 36)」 を繰り返すことでワークスペースを再プロビジョニングすることができます。あるいは、プロビジョニング プロセスをキャンセルすることもできます。

組み込み OpenLDAP サービスの使用 9

組み込み OpenLDAP サービスは、一般的にデモンストレーションおよびテスト構成で使用されます。組み込み OpenLDAP サービスを使用する場合に実行する可能性がある操作は、新規ユーザーの追加、既存のユーザーの削除、ユーザー パスワードの削除などの一般的な LDAP 操作です。

この情報は、システム管理者としての経験があり、標準的な LDAP 操作とコマンドに詳しい方を対象としています。

組み込み OpenLDAP サーバは TCP ポート 389 上で実行されます。OpenLDAP サーバーには、Horizon Mobile Manager 仮想アプライアンスの Linux コンソールからローカルでのみアクセス可能です。標準的な LDAP コマンドを使用して組み込み OpenLDAP サーバの操作を実行できます。必要なバイナリ （**ldapadd**、**ldapsearch**、**ldapdelete**、および **ldapmodify**） は仮想アプライアンスにインストールされています。

デフォルトで、仮想アプライアンスがインストールされ構成されると、組み込み OpenLDAP サービスは、**Enterprise User 1**、**Enterprise User 2** などのパターンに追随する共通名 （**cn**） を持つエントリで事前構成されます。ユーザーは次の属性で事前構成されます。

- userPassword: **vmware**
- sn: **User**
- uid: **user1**、**user2** などのパターンに追随します。
- ou: **people**

たとえば、**Enterprise User 1** の事前構成されたエントリは次の属性値を持っています。

```
cn: Enterprise User 1
sn: User
mail: user1@mvp.org
uid: user1
```

仮想アプライアンスの構成を行う最中に、デフォルトのシステム管理者として使用するユーザー アカウントを指定します。このアカウントは、Horizon Mobile Manager 管理インターフェイスへのログインとすべての操作の実行が可能です。仮想アプライアンスの構成を行っている最中に、デフォルトの値を使用した場合、ユーザー アカウントは、**cn** 属性が **Admin User** に設定され、**uid** 属性が **admin** に設定され、userPassword 属性が **vmware** に設定されている組み込み LDAP サービスの事前構成されたエントリになります。

ベース識別名 （DN)、バインド DN、およびバインド PW

組み込みの OpenLDAP サーバー用のベース識別名 （DN） は **dc=mvp, dc=org** です。

bind DN は **admin** で、bind PW は **vmware** です。

デフォルトのシステム管理者エントリ用パスワードの変更

事前構成された管理者エントリ （**uid: admin**） のパスワードを変更するには、属性が適切に設定された LDAP データ交換フォーマット （LDIF） ファイルを作成し、**ldapmodify** コマンドを実行して既存の値を LDIF ファイルの値に変更します。

1 コンソールから仮想アプライアンスにログインします。

2 テキスト エディタを使用して、ファイル システム内に新規の LDIF ファイルを作成します。例：
`vi /home/tcserver/changepass.ldif`

3 LDIF ファイルに適切な行を入力してファイルを保存します。この例では、**admin** uid のパスワードが **classic*CD** に変更されます。

```
dn: uid=admin,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: classic*CD
```

4 **ldapmodify** コマンドを実行します。

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w
vmware –f /home/tcserver/changepass.ldif
```

ご使用の Horizon Mobile Manager インスタンスが事前構成のユーザー アカウントをデフォルトのシステム管理者として使用する場合、Horizon Mobile Manager 管理インターフェイスへの次回ログイン時に、ユーザー名 **admin** と新しいパスワードを使用することになります。

組み込み OpenLDAP へのユーザーの追加

デモ環境において、所属する組織やチームのメンバーに対応するユーザー アカウントまたは事前構成されたものではないユーザー名が必要になる場合があります。LDIF ファイルを使用して、標準の **ldapadd** 操作を実行して新規エントリを OpenLDAP サービスに追加できます。この例では、addentry.ldif という名前が付けられた LDIF ファイルによって、個別の Stacy Barr のエントリが **uid:sbarr** および **userPassword:stacy*b** で定義されます。

```
dn: uid=sbarr,ou=people,dc=mvp,dc=org
objectclass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Stacy Barr
sn: Barr
uid:sbarr
mail: s.barr@mvp.org
userPassword: stacy*b
```

エントリを組み込みの OpenLDAP に追加するには、仮想アプライアンス コンソールで **ldapadd** コマンドを実行します。

```
/usr/bin/ldapadd –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/addentry.ldif
```

組み込み OpenLDAP からのユーザーの削除

組み込み OpenLDAP サービスからエントリを削除するには、仮想アプライアンス コンソールで **ldapdelete** コマンドを使用します。

たとえば、事前構成された **user50** エントリを削除するには、次を実行します。

```
/usr/bin/ldapdelete –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware
"uid=user50,ou=people,dc=mvp,dc=org"
```

ユーザー パスワードの変更

デフォルトの admin アカウントのパスワードを変更する手順と同じように、ユーザーのパスワードを変更するには、LDIF ファイルを使用して標準の **ldapmodify** 操作を実行します。単一の LDIF ファイルを 1 つの **ldapmodify** 操作で使用して複数のユーザーのパスワードを変更するには、ファイルに 4 行のブロックを各ユーザー用に作成します。ブロックはそれぞれ空白行で区切られます。

たとえば、事前構成された **user21**、**user22**、**user23**、および **user24** のパスワードを変更するには、次の行を含む **changeuserpwd.ldif** という名前が付けられた LDIF ファイルを作成します。

```
dn: uid=user21,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*21

dn: uid=user22,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*22

dn: uid=user23,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*23

dn: uid=user24,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*24
```

ldapmodify コマンドを LDIF ファイルで実行することにより、1 つの操作で複数のパスワードを変更できます。

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/changeuserpwds.ldif
```

その他の OpenLDAP コマンドの使用

組み込みの OpenLDAP サービスで標準の OpenLDAP コマンドを使用できます。

Horizon Mobile コンポーネントのバージョンの決定 10

サポート要求を提出しているとき、ご使用の Horizon Mobile 環境の主要コンポーネントのバージョン、ビルド、またはモデル番号は問題の発生源を診断するのに役立ちます。

Horizon Mobile 環境の主要コンポーネントは次のとおりです：

- VMware Ready モバイル デバイス
- VMware Ready コンポーネント
- VMware Switch アプリケーション
- ベース ワークスペースのイメージ
- VMware Horizon Mobile Manager 仮想アプライアンス

各コンポーネントには関連した識別子があります。

表 10-1. Horizon Mobile コンポーネントの識別子

コンポーネント	識別子
モバイル デバイス	モバイル番号 （モバイル デバイス上）
VMware Ready コンポーネント	ソフトウェアのバージョン番号 （モバイル デバイス上）
Vmware Switch コンポーネント	ソフトウェアのバージョン番号 （モバイル デバイス上）
ベース ワークスペースのイメージ	■ ソフトウェアのバージョン番号 （モバイル デバイス上） ■ ビルド ID とイメージの名前 （管理インターフェイス内）
Horizon Mobile Manager	ソフトウェア バージョンおよびビルド番号 （仮想アプライアンスのコンソール内および構成インターフェイス内）

モバイル デバイス上のバージョン情報

注意 バージョン情報を取得する手順は、ご使用の特定のモバイル デバイスによって、異なることがあります。

モバイル デバイス上では、デバイスのモデル番号と、VMware Ready、VMware Switch、およびベース ワークスペース イメージのコンポーネントのソフトウェア バージョン情報を取得できます。

デバイスのモデル番号

デバイス上でモデル番号を取得します。モデル番号は通常、デバイスの［端末について］の情報で確認できます。

VMware Ready、VMware Switch、ベース ワークスペース イメージのソフトウェアのバージョン

これらのコンポーネントのバージョン番号は、すべてのアプリケーションのリストを表示し、そのリスト内で VMware Switch を見つけ、その設定を開くことによって取得できます。例：

1 ［設定］ > ［Apps］ > ［すべて］を開きます。

2 すべてのアプリケーションのリストで、[VMware Switch] をタッチします。

3 [スペースの管理] をタッチします。[VMware Switch の設定] が表示されます。

4 [診断] をタッチします。VMware Ready、VMware Switch のソフトウェアのバージョン番号と、プロビジョニングされたワークスペースが表示されます。ワークスペースがデバイス上でプロビジョニングされていない場合は、ワークスペース情報は表示されません。

Horizon Mobile Manager 仮想アプライアンスで取得可能な情報

モバイル デバイス自体で入手できる情報に加えて、Horizon Mobile Manager の管理インターフェイスを使用することによってユーザーのモバイル デバイス上にプロビジョニングされたワークスペースに関する追加情報を取得できます。

1 オペレーション マネージャとして管理インターフェイスにログインします。

2 [ユーザー] をクリックして対象ユーザーのユーザー詳細ページを開き、表示されたユーザー リスト内のユーザーの名前をクリックします。

3 [ワークスペース コンテナ] セクションが展開されていない場合、それを展開します。名前の行には、ベース ワークスペース イメージの名前が表示されます。名前の注記を作成します。

4 名前とビルド ID とを関連付けるには、[ワークスペース イメージ] をクリックして Horizon Mobile Manager のこのインスタンスで使用できるワークスペース イメージのリストを表示します。

5 リストのエントリをクリックすると、ベース ワークスペース イメージの名前が表示されます。[ワークスペース イメージ詳細] ウィンドウで、ビルド ID 行にワークスペース イメージのビルド番号が表示されます。

Horizon Mobile Manager 仮想アプライアンスに関する情報

ご使用の Horizon Mobile Manager のインストールの識別情報を、次の場所で確認できます。

vSphere Client の使用 Horizon Mobile Manager 仮想アプライアンスを選択し、[コンソール] をクリックしてコンソールを表示します。Horizon Mobile Manager 仮想アプライアンスのバージョンおよびビルド番号が表示されます。

構成インターフェイスの使用 第 4 章「ライセンス キーの追加 (P. 15)」 に記載されているとおりに、構成インターフェイスにログインします。バージョンおよびビルドの情報が [システム] タブに表示されます。

管理インターフェイスの使用 オペレーション マネージャまたは管理者として管理インターフェイスにログインします。ハッシュおよびブランチ情報の識別を表示するには、[バージョン情報] をクリックします。

11 診断ログの収集

サポート要求を行うと、VMware テクニカル サポートから仮想アプライアンスの組み込みコンポーネントのログを要求されることがあります。サポート要求に合わせて、これらのログを収集して zip ファイルで提供することができます。

次の組み込みコンポーネントのログを収集できます。

- Apache サーバ
- vFabric Postgres データベース
- Linux オペレーティング システム

開始する前に

vSphere Client で仮想アプライアンスをパワーオンし、[コンソール] タブをクリックして、仮想アプライアンスの Linux オペレーティング システムに **root** ユーザーとしてログインします。仮想アプライアンスを構成したときに設定したパスワードを使用します。デフォルトのパスワードを変更しなかった場合は、パスワードとして **vmware** を入力します。

手順

1 Apache サーバのログ ファイルを zip 形式で圧縮します：

   a 次のコマンドを実行します：`tar czf apachelog1.tgz /home/tcserver/tcserver-current/mmp/logs/`

   b 次のコマンドを実行します：`tar czf apachelog2.tgz /home/tcserver/tcserver-current/mmp-config/logs/`

2 次のコマンドを実行して、vFabric Postgres データベースのログ ファイルを zip 形式で圧縮します：`tar czf postgreslog.tgz /opt/vmware/vpostgres/1.0/data/pg_log/`

3 次のコマンドを実行して、Linux オペレーティング システムのログ ファイルを zip 形式で圧縮します：`tar czf suselog.tgz /var/log/`

次に進む前に

作成された zip（.tgz）ファイルを、VMware テクニカル サポートに提供できる場所にコピーします。

インデックス

る

ろ

わ