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

Horizon Mobile Manager 1.2

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-000994-00

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 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。 エンタープライズ内の Horizon Mobile Manager のデプロイの構成は、デバイスが Horizon Mobile Manager との通信に会社のネットワークを使用しているか、インターネットを使用しているかに関わらず、一切の制約なく、デバイス上のワークスペースの管理をサポートする必要があります。

Horizon Mobile Manager 仮想アプライアンスには、サーバ側の管理機能を提供する組み込み Apache 2.2 が含まれています。 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となります。 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。 ■ 企業のファイアウォールを通じてポートを開かずに、Horizon Mobile Manager が Active Directory 、LDAP あるいは会社のデータベースなどの企業内サービスに接続するように構成することができません。
Horizon Mobile Manager は企業の内部ネットワーク内にあり、Horizon Mobile Manager の内部 IP アドレスをネットワーク アドレス変換（NAT）を使用して外部で利用できる 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。 これらの、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る必要があります。	■ 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 サーバがデバイスからの SSL 要求を終了し、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 がサポートする固有の 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。 ■ 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。 ■ この構成は、最も拡張性が高く、本番環境で Horizon Mobile Manager をデプロイするための安全なアーキテクチャです。	■ リバース プロキシ サーバおよび Horizon Mobile Manager との 通信のルールの設定には慎重な計画が必要です。 ■ 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、Horizon Mobile Manager を開始し、その機能を確認するための最も早い方法です。 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、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、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、Secure Sockets Layer（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 vPostgres 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

組み込み OpenLDAP ネーム サービス（デフォルト）か、独自のネーム サービスを使用できます。 テストおよび最初の導入の場合を除き、通常は独自の LDAP または Active Directory サービスを使用することになります。

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。

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 のデジタル証明書の要件

6

Horizon Mobile Manager では、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ます。 デフォルトの構成の場合、Horizon Mobile Manager は、自動的に生成された自己署名証明書を使用します。 お使いのデプロイ構成に適した証明書のアプローチ方法を使用する必要があります。

Horizon Mobile Manager とモバイル デバイスとの通信は、Secure Sockets Layer（SSL）プロトコル接続を介して送信されます。 Horizon Mobile Manager は、デバイスに対して有効な証明書を示し、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する必要があります。 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。

最初に Horizon Mobile Manager をインストールし構成するときに、自動的に生成された内部ルート認証局（CA）証明書とリース サーバに指定された 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。

注意 Horizon Mobile Manager の [セキュリティ] ページの [サーバ信頼証明書チェーン] リストの `internal-ca-root` エントリを削除しないでください。 証明書は、自動的に生成された内部ルート CA であり、制御された状況下で特定の順序の手順にしたがって行う場合を除き、削除しないでください。 詳細については、当社のナレッジ ベース記事（http://kb.vmware.com/kb/2035492）を参照してください。

これらの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。 自動的に生成された証明書を独自の自己証明書か、商業認証局が署名した証明書のいずれに置き換えるかを決定します。 デプロイの構成および独自の SSL および署名証明書を使用するタイミングや方法については、当社のナレッジ ベース記事（http://kb.vmware.com/kb/2035492）を参照してください。

注意 SSL 証明書が自己署名証明書（独自のものか、Horizon Mobile Manager で自動的に生成されたもの）の場合は、デバイス ユーザーが VMware® Switch アプリケーションを起動し、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、ユーザーが VMware® Switch アプリケーション設定の［サーバの認証］チェック ボックスを選択解除する必要があります。 チェック ボックスは、デフォルトで選択されています。［サーバの認証］チェック ボックスが選択解除されておらず、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。

VMware® Switch アプリケーションの［サーバの認証］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。 自己署名 SSL 証明書を使用している場合は、［サーバの認証］チェック ボックスを選択解除します。

ビジネス ワークスペースをデバイスにインストールした後、ユーザーは VMware® Switch アプリケーション 設定の［サーバの認証］チェック ボックスを選択することができます。 ワークスペースの最初のインストール後、通信ではワークスペースに含まれる証明書が使用されます。 その後、ワークスペースがワイプされた場合、SSL 証明書が自己証明書の場合は、ワークスペースを再インストールするために［サーバの認証］チェック ボックスを選択解除する必要があります。

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

7

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。

インデックス