第 11 章

Microsoft Intune によるアプリケーションおよびリソースへのアクセス

目次

概要

Microsoft Intune の最も強力で役立つ機能の 1 つは、組織内のデスクトップやモバイルベースのさまざまなオペレーティング システムを管理できるようになることです。大多数のアプリケーション ベンダーは、さまざまなプラットフォーム専用バージョンのソフトウェアを提供しています。例えば、Microsoft では Windows、iOS、および Android プラットフォームで動作する Office 製品を提供しています。管理環境の目標の 1 つは、さまざまなデバイスやコンピューターのプラットフォームでホストされる可能性のあるアプリケーションをサポートして、ユーザーの生産性を高められるようにすることです。

異なるデバイスやアプリを管理するようになると、リソース アクセスやアプリケーション機能の誤使用によるデータ損失から組織を保護することも必要になります。条件付きアクセスとモバイル アプリケーション管理 (MAM) ポリシーは、機能および組織のデータへのセキュリティで保護されたアクセスを提供するのに役立ちます。

この章では、Intune でのアプリケーション管理のプロセス、および組織のリソースやデータへのアクセスをセキュリティで保護するプロセスについて説明します。

目的

この章により、次のことを習得できます。

- Intune によるアプリケーション管理の要件を説明することができます。
- Intune によるアプリケーション展開プロセスを説明することができます。
- Intune により組織のリソースへのアクセスを管理する方法を説明することができます。

レッスン 1
Intune によるアプリケーション管理

他の管理ソリューションと同様に、Intune はアプリケーション管理のライフサイクル (ALM) プロセスに役立つ機能を備えています。Intune を使用してアプリケーションを準備、展開、監視、および更新または削除する方法を理解することが重要です。このレッスンでは、Intune クラウド サービスを使用してアプリケーションを適切に管理できるようにするためのライフサイクルと要件について説明します。

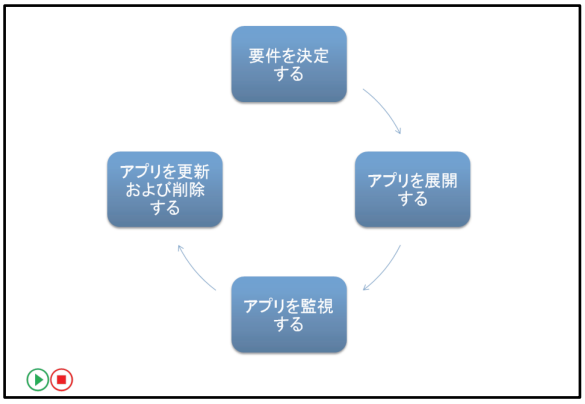
目的

このレッスンにより、次のことを習得できます。

- Intune による ALM を説明することができます。
- Intune によるアプリケーション管理の要件を説明することができます。
- Intune でサポートされるソフトウェア インストールの種類を説明することができます。

Intune による ALM の概要

Intune によるアプリ管理の主なメリットの 1 つは、既存の ALM プロセスを継続的にサポートできることです。アプリケーションを種類の異なるデバイスやコンピューターに展開する場合でも、ライフサイクルは通常、ネットワーク環境に展開されている他のアプリケーションと同じプロセスに従います。



Intune を使用してアプリケーションを管理するには、次のプロセスを使用します。

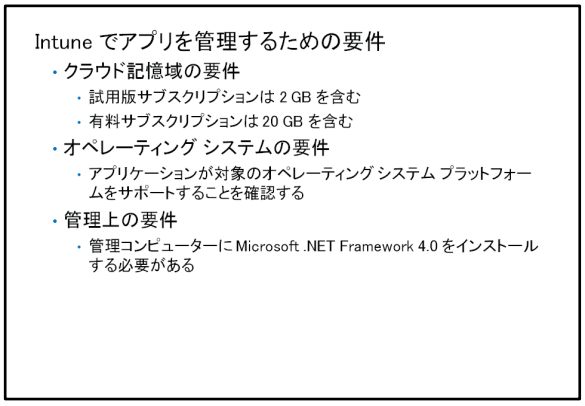
1. **要件を決定する :** 特定のアプリケーションで複数のプラットフォームをサポートしている場合があるため、アプリケーションを正常に展開するために対処する必要のある要件と前提条件を理解することが重要です。これには次の項目が含まれます。
    - クラウド記憶域の要件
    - オペレーティング システムの要件
    - 管理上の要件
2. **アプリを展開する :** 要件に応じて、特定のインストーラーをオペレーティング システム プラットフォームに展開できます。また、各プラットフォーム用のオンライン ストアで入手可能なアプリへのリンクを提供することもできます。もう 1 つのオプションは、管理対象のアプリケーションを展開して、MAM ポリシーを互換性のあるアプリと関連付けられるようにすることです。MAM ポリシーは管理対象のアプリの機能を制御する規則を提供します。
3. **アプリを監視する :** アプリの展開時に、Intune 管理コンソールを使用して、アプリ展開の進捗状況を確認できます。また、管理対象のコンピューターやデバイスにインストールされている、インベントリされたソフトウェアに関するレポートを確認することもできます。
4. **アプリを更新および削除する :** ALM の最終フェーズは、アプリケーションの更新または削除です。Intune を使用してアプリケーションを新しいバージョンに更新できます。そのアプリケーションが組織で不要になったと判断した場合は、管理対象のアプリをアンインストールするコマンドを構成することもできます。

Intune によるアプリケーション管理の要件

Intune によるアプリの展開を開始する前に、展開の成功に影響する可能性のあるサービスの要件、オペレーティング システムの要件、または管理上の要件を確認することが重要です。

Intune によるアプリケーション管理を準備する際は、次の点を考慮してください。

- クラウド記憶域の要件
- オペレーティング システムの要件
- 管理上の要件



クラウド記憶域の要件

Intune の試用版サブスクリプションに登録すると、2 GB のクラウドベースの記憶域が提供されます。この記憶域を使用して、管理対象のクライアントに展開するアプリケーション パッケージや更新プログラムを保存します。有料サブスクリプションでは、20 GB の記憶域が提供され、1 GB 単位で追加の記憶域を購入できます。展開するアプリケーションの数やサイズに基づいて、必要なクラウド記憶域を決定して、必要に応じて追加の記憶域を購入する必要があります。追加の記憶域は Intune アカウント ポータルから購入できます。

オペレーティング システムの要件

Windows ベースのコンピューターのほかに、多くの場合、さまざまなモバイル デバイスをサポートする必要があり、それぞれのオレーティング システムに特定の考慮事項があります。おおむね、Windows ベースのコンピューターやモバイル デバイスが Intune と互換性がある場合、プラットフォーム固有のストア アプリの展開もサポートされています。従来のアプリケーションのインストールでは、アプリケーションの要件を参照して、対象のコンピューターに搭載されているオペレーティング システムがサポートされていることを確認する必要があります。

管理上の要件

アプリを Intune にアップロードするには、管理コンピューターが Intune ソフトウェア パブリッシャーをサポートしている必要があります。このアプリケーションは、Intune 管理コンソール内でアプリを追加または変更したときに起動されます。このアプリケーションを使い始める前に、フル バージョンの .NET Framework 4.0 をインストールする必要があります。

ソフトウェア インストールの種類の概要

Intune を使用してアプリケーションを効果的に展開するには、管理できるソフトウェア インストーラーの種類を特定する必要があります。インストーラーの種類に応じて、次の方法を使用してアプリケーションを展開できます。

- アプリ パッケージをクラウド記憶域にアップロードし、Intune ポータル サイトからユーザーに対してアプリを使用可能にします。
- アプリ パッケージをクラウド記憶域にアップロードし、管理対象のコンピューターにアプリを直接展開します。

ソフトウェア インストールの種類	ファイル拡張子
Windows インストーラー	.exe、.msi
iOS 用アプリ パッケージ	.ipa
Android 用アプリ パッケージ	.apk
Windows Phone 用アプリ パッケージ	.xap、.appx、.appxbundle
Windows 用アプリ パッケージ	.appx、.appxbundle

- オンライン ストアに掲載されているアプリ、または Web ブラウザーから実行する Web ベースのアプリへの外部リンクをモバイル デバイスに提供します。ユーザーはこの種のリンクを Intune ポータルサイトから使用できます。

注 : オンライン アプリ ストアを介さずに、モバイル デバイスにアプリを直接インストールすることもできます。これはサイドローディングと呼ばれ、管理対象のモバイル デバイス プラットフォームに基づいた追加の要件があります。

次の表に、Intune がサポートしているソフトウェア インストールの種類を示します。

種類	説明
Windows インストーラー (.exe、.msi)	最も一般的な種類のアプリケーション インストーラーです。この種類のインストーラーを使用する場合は、無人インストールによる展開がサポートされていることを確認してください。これは通常、強制的にサイレント インストールする /q などのコマンドライン スイッチによって指定されます。サイレント モードでのアプリの展開については、アプリケーションのマニュアルを参照してください。 追加のサポート ファイルがある場合は、それらをアプリの展開の構成時に指定した場所から使用できるようにする必要があります。
iOS 用アプリ パッケージ (.ipa)	iOS オペレーティング システム用のアプリは、.ipa パッケージを使用してインストールされます。iOS アプリケーションを展開するには、.ipa パッケージが Apple によって署名されている必要があり、また自社が Apple Developer Enterprise Program に登録されている必要があります。
Android 用アプリ パッケージ (.apk)	モバイル デバイス管理機関を Intune に設定すると、.apk ファイルを Android デバイスに展開できるようになります。Android パッケージの展開には追加の要件はありません。
Windows Phone 用アプリ パッケージ (.xap、appx、.appxbundle)	Windows Phone のバージョンによっては、モバイル コード署名証明書が必要になる場合があります。Window Phone 8 では、デバイスと Intune の間に暗号化された IP 接続を確立するために、Symantec 証明書が必要です。Windows Phone 8.1 では、基幹業務アプリのサイドローディングを計画している場合のみ、証明書が必要です。
Windows 用アプリパッケージ (.appx、appxbundle)	Windows Phone アプリと同様に、Windows RT または登録された Windows 8.1 以降のコンピューター用の Windows .appx パッケージは、署名とサイドローディング製品のアクティベーション キーを取得する必要があります。

注 : モバイル デバイスのインストーラーの種類は、モバイル デバイス管理機関を Intune に設定した後でのみ使用可能になります。オンライン ストアにリンクされているアプリケーションを展開する場合、インストールはストアから管理されるため、他の証明書要件は不要です。

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
Intune を使用してアプリケーションを展開するには、最初にアプリケーションを Intune ベースの専用のインストール パッケージに変換する必要があります。	

活動の分類

どのインストールの種類が各オペレーティング システム プラットフォームに関連しているかを識別する必要があります。

各項目を適切なカテゴリに分類してください。各項目の右側にカテゴリの番号を記入して解答してください。

項目	
1	.appx
2	.msi
3	.ipa
4	.apk
5	.exe

カテゴリ 1		カテゴリ 2		カテゴリ 3
Windows 8.1 以降のコンピューター		iOS デバイス		Android デバイス

レッスン 2
アプリケーション展開プロセス

Intune によるアプリケーション展開処理では、展開ができるだけ効果的になるようにするために、多数の考慮事項と設定が必要です。このレッスンでは、コンピューターとモバイル デバイスの両方へのアプリの展開および展開の監視のためのプロセスと操作について説明します。

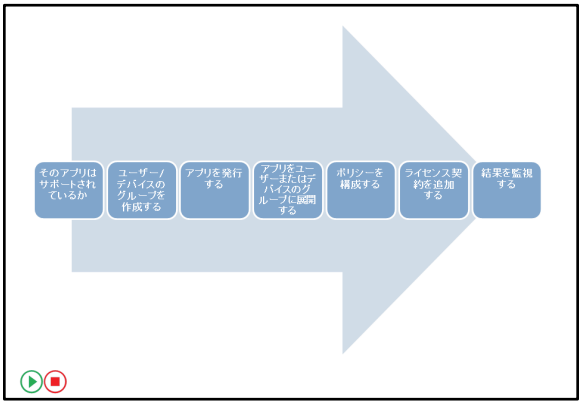
目的

このレッスンにより、次のことを習得できます。

- Intune のアプリケーション展開の全体的なプロセスを説明することができます。
- Intune ソフトウェア パブリッシャーを使用してアプリケーションを発行することができます。
- Intune によるアプリケーション展開の管理方法を説明することができます。
- Intune によりアプリケーションを展開することができます。
- Intune でのアプリケーション展開を監視することができます。
- Intune によるモバイル アプリケーション管理を説明することができます。

Intune のアプリケーション展開プロセスの概要

Intune によるアプリ展開の全体的なプロセスには、次の処理が含まれます。



1. **Intune がアプリをサポートしていることを確認する：**Intune がアプリケーションのインストールの種類をサポートしており、アプリケーションがユーザーの介入なしにインストールできることを確認します。
2. **ユーザーまたはデバイスのグループを作成する：**Intune でユーザーベースまたはデバイスベースのグループを作成して、特定のユーザーまたはデバイスを対象にソフトウェア管理タスクをおこなえるようにします。特定のグループのユーザーがアプリケーションを必要とする場合、アプリを展開するユーザーまたはデバイスのグループを作成します。利用可能なインストールの展開を計画している場合は、管理対象のユーザーをそのコンピューターにリンクして、外部リンクとポータル サイト アプリを使用できるようにする必要もあります。
3. **アプリを発行する：**Intune ソフトウェア パブリッシャーを使用して、アプリケーション ファイルを Intune のクラウド記憶域に追加するか、外部リンクの URL またはアプリ ストアから管理されるアプリを指定します。ウィザードを使用して、インストール要件、検出規則、コマンドライン引数を構成し、アプリに関する一般的な情報を提供します。アプリを発行すると、Intune 管理コンソールの [アプリ] でアプリを展開できるようになります。
4. **アプリをユーザーまたはデバイスのグループに展開する：**アプリケーションを発行すると、アプリの展開タスクを管理できます。アプリを展開するには、まずソフトウェアを展開するユーザーまたはデバイスのグループを選択します。次に、[必須のインストール]、[利用可能なインストール]、または [アンインストール] など、実行する特定の展開アクションを構成できます。選択したアクションに応じて、インストールの期限を構成することもできます。

5. **ポリシーを構成する :** モバイル デバイスの管理対象アプリケーションを展開している場合、管理対象ブラウザーのポリシー設定または iOS および Android デバイス用の MAM ポリシーを構成することもできます。これらのポリシーでは、各管理対象アプリの特定の設定や機能を構成できます。
6. **ライセンス契約を追加する :** 発行するライセンスされた各ソフトウェアに対して、Intune にライセンス契約を追加して、ライセンスの購入およびインストール レポートを確認できるようにすることもできます。Intune 管理コンソールの [アプリ] で、Microsoft ボリューム ライセンス契約または Microsoft 以外のその他のソフトウェア契約を追加できます。
7. **アプリ展開の結果を監視する :** [アプリ] でアプリを選択すると、アプリケーションのプロパティを表示できます。プロパティには、アプリをインストールしたユーザーやデバイスの数を表す統計が示されます。

デモンストレーション : Intune ソフトウェア パブリッシャーによるアプリケーションの発行

講師は、次のデモンストレーションをおこないます。

- Intune ソフトウェア パブリッシャーを使用してアプリを発行する

デモンストレーションの手順

1. LON-DC1 で、http://manage.microsoft.com から Intune 管理コンソールにサインインします。
2. [アプリ] で、ノードを表示します。
3. [アプリ] ノードで [アプリの追加] をクリックし、Intune ソフトウェア パブリッシャーを起動します。
4. 次のように入力してウィザードを完了します。
   - デバイスに配布する方法 : ソフトウェアのインストーラー
   - ファイルの種類 : Windows インストーラー (*.exe、*.msi)
   - 場所 : E:¥Labfiles¥Mod11¥XmlNotepad.msi
   - 発行元 : Microsoft
5. 要件を次のように構成して、[アップロード] をクリックします。
   - アーキテクチャ : 64 ビット
   - オペレーティング システム : Windows 8.1 以降のすべてのオペレーティング システム

アプリ展開の管理

ソフトウェア インストール パッケージをアップロードして発行すると、ソフトウェアを目的のターゲット グループに展開できます。アプリの展開を管理するには、次の手順を実行します。

1. [アプリ] で [アプリ] ノードを選択し、管理するアプリケーションを選択して、[展開の管理] をクリックします。
2. [グループの選択] ページで、インストールの対象となるユーザーまたはデバイスのグループを選択します。

3. [展開アクション] ページで、次のオプションのいずれかを選択します。使用可能なオプションは、オペレーティング システム プラットフォーム、およびユーザー グループとデバイス グループのどちらを選択したかによって異なります。
    - 必須のインストール : 対象となるすべてのコンピューターにアプリを自動的にインストールします。Android および iOS デバイスの場合、ユーザーはインストールする前に確認を受け入れることが必要になる場合があります。
    - 利用可能なインストール : 対象となるすべてのユーザーに対してアプリを利用可能にします。ユーザーは Intune ポータル サイトからアプリケーションをインストールできます。
    - 該当なし : 対象グループに対してアプリケーションを使用不可にします。
    - アンインストール : アプリケーションがアンインストールをサポートしている場合、このオプションは対象となるすべてのコンピューターからアプリをアンインストールします。

必須のインストールまたはアンインストールを展開する場合、アプリの展開または削除の期限を指定することもできます。期限オプションには、次のものがあります。

- なし : アプリはエージェント ポリシー設定に基づいて展開されます。
- 直ちに : 次回のポリシー同期で、Intune は対象グループ内のクライアント コンピューターをスキャンして、アプリを展開します。
- 1 週間 : 現在日から 1 週間以内にアプリを展開します。
- 2 週間 : 現在日から 2 週間以内にアプリを展開します。
- 1 か月 : 現在日から 1 か月以内にアプリを展開します。
- カスタム : 独自の展開日時を設定できます。

参考資料 : プラットフォームごとの使用可能なアクションについては、次のサイトを参照してください。
Microsoft Intune でのアプリ展開の開始
https://technet.microsoft.com/ja-jp/dn646955.aspx

デモンストレーション : Intune によるアプリの展開

講師は、次のデモンストレーションをおこないます。

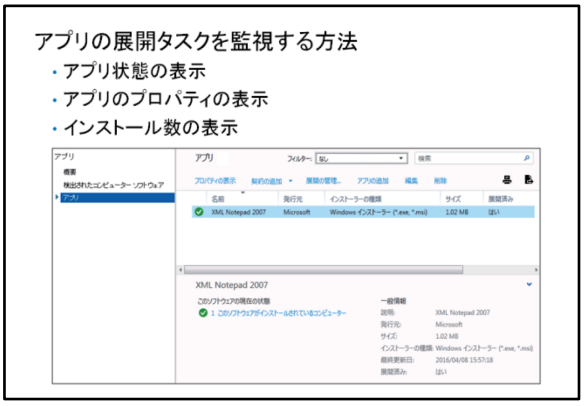
- Intune を使用して発行されたアプリを展開する

デモンストレーションの手順

1. LON-DC1 で、http://manage.microsoft.com から Intune 管理コンソールにサインインします。
2. [アプリ] で、[XML Notepad 2007] を右クリックし、[展開の管理] をクリックします。
3. 次のように入力してウィザードを完了します。
    - グループの選択 : すべてのコンピューター
    - 展開アクション : 必須のインストール
    - 期限 : 直ちに
4. [すべてのデバイス] ノードで、LON-CL1.Adatum.com のポリシーを更新します。

アプリ展開の監視

Intune では、アプリの展開タスクを監視する多数の方法を提供しています。次のような方法があります。

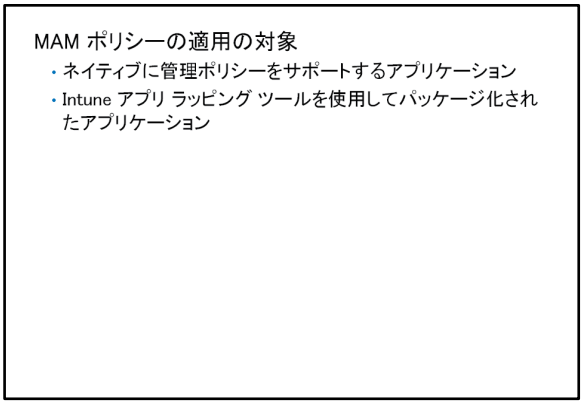


- **アプリ状態の表示 :** コンソールでアプリケーションを選択すると、プレビュー ウィンドウにアプリケーションの状態に関する詳細情報が表示されます。これには、アプリケーションをインストールしたコンピューターの合計数が含まれます。フィルターを使用して、次の状態をすばやく特定することもできます。
  - インストールの失敗
  - 要件を満たさない
  - インストール保留中

  モダン アプリの場合、ユーザーまたはデバイスの展開の概要、失敗したインストール、または期限が切れたまたは切れそうなアプリをフィルターして表示できます。
- **アプリのプロパティの表示 :** 展開したアプリのプロパティを表示すると、アプリをインストールしたコンピューターおよびユーザーの数に関する詳細情報、アプリに関する情報データ、およびインストールを承認されたグループの一覧が示されます。
- **インストール数の表示 :** インストールのカウント数をクリックすると、アプリケーションをインストールしたすべてのコンピューターの一覧を表示できます。これから、オペレーティング システムのバージョン、リンクされたユーザー、グループ メンバーシップなど、各クライアント コンピューターに関する情報を取得することもできます。

Intune によるモバイル アプリケーション管理

Intune は、モバイル アプリケーション管理 (MAM) ポリシーをサポートしています。これは、管理対象アプリの一部の機能を制限して、組織のコンプライアンスとセキュリティのポリシーに適合させるのに役立ちます。制限の例として、管理対象アプリ内での切り取り、コピー、または貼り付け機能の制限や、[名前を付けて保存] コマンドの無効化などがあります。MAM ポリシーは現在 Android 4 以降、および iOS 7 以降のデバイスをサポートしています。



アプリに制限を適用するには、次の方法を使用できます。

- **MAM ポリシーをネイティブ サポートしているアプリを展開する :** 最新のモバイル バージョンの Office の多くは、MAM ポリシーをサポートしています。このような種類のアプリケーションを使用することを計画している場合は、アプリケーションを展開して、管理対象アプリケーションに関連付ける MAM ポリシーを構成するだけで済みます。

参考資料： MAM ポリシーをサポートしているアプリとサービスの最新リストについては、次を参照してください。
Microsoft Intune のモバイル アプリケーション管理ポリシーと共に使用できる Microsoft アプリ
https://technet.microsoft.com/ja-jp/library/dn708489

- **Intune アプリ ラッピング ツールを使用する：** MAM ポリシーをネイティブ サポートしていないアプリの場合、Intune アプリ ラッピング ツールを使用してアプリを再パッケージ化することができます。組織内で作成されたアプリには通常、このツールを使用します。アプリ ストアに既に公開されているアプリにこのツールを使用することはできません。

参考資料： Intune アプリ ラッピング ツールの使用については、次のサイトを参照してください。

- iOS アプリの場合
  Microsoft Intune アプリ ラッピング ツールでモバイル アプリケーション管理のために iOS アプリを準備する
  https://technet.microsoft.com/ja-jp/library/dn878028.aspx
- Android アプリの場合は
  Microsoft Intune アプリ ラッピング ツールでモバイル アプリケーション管理のために Android アプリを準備する
  https://technet.microsoft.com/ja-jp/library/mt147413.aspx

アプリケーションをパッケージ化して発行すると、MAM ポリシーを作成できるようになります。アプリを構成しているデバイスの種類に基づいて、[ポリシー] にアクセスして次のポリシーを構成できます。

- モバイル アプリケーション管理ポリシー (Android 4 以降)
- モバイル アプリケーション管理ポリシー (iOS 7 以降)

知識の確認

質問	
アプリケーションを Intune クラウド記憶域にアップロードするには、次のどのツールを使用しますか。	
正しい解答を選択してください。	
	Intune アプリ ラッピング ツール
	Office アップロード センター
	Microsoft Intune ソフトウェア パブリッシャー
	Microsoft OneDrive 同期

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
MAM ポリシーを使用して iOS デバイスで作業フォルダーを制御できます。	

演習 A : Microsoft Intune によるアプリケーションの展開

シナリオ

A. Datum 社では、Research 部門のすべてのコンピューターに XML Notepad アプリケーションを展開する必要があります。あなたは、Intune ポータル サイトで、すべてのユーザーに Microsoft Word Mobile へのリンクを提供する必要があります。Intune のアプリケーション展開を使用し、これらのアプリケーションを提供します。

目的

この演習により、次のことを習得できます。

- Intune で展開用アプリケーションを発行することができます。
- Intune により、アプリケーションをターゲット グループに展開することができます。

演習のセットアップ

予定所要時間 : 30 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 MSL-TMG1
ユーザー名	Adatum¥Administrator Adatum¥Don
パスワード	Pa$$w0rd

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Don」、パスワード「Pa$$w0rd」を使用してサインインします。
6. インターネットへのアクセスのために、MSL-TMG1 を起動します。

注 : この演習を完了するためには、第 8 章から第 10 章のすべての前提条件を満たし、第 8 章から第 10 章の演習を完了する必要があります。

練習 1 : Intune での展開用アプリケーションの発行

シナリオ

XML Notepad と Word Mobile を提供するには、最初に、Intune でアプリケーションを追加して発行します。アプリケーションを発行してから、それらを正しいグループに展開します。

主な作業は次のとおりです。

1. Intune ソフトウェア パブリッシャーを使用して .msi インストーラーを発行する
2. アプリ ストアへの外部リンクを発行する

▶ 作業 1 : Intune ソフトウェア パブリッシャーを使用して .msi インストーラーを発行する

1. LON-DC1 に切り替え、Internet Explorer を開きます。
2. http://manage.microsoft.com を参照します。
3. Intune 管理コンソールにアクセスするための資格情報を入力します。
4. [グループ] で、[すべてのデバイス] ノードをクリックします。
5. [LON-CL1.Adatum.com] を右クリックし、[ユーザーの関連付け] をクリックします。[Don Funk] を [LON-CL1] にリンクします。
6. [アプリ] から [アプリ] ノードを参照します。
7. 次の情報を使用して新しいアプリを追加します。
   - このソフトウェアをデバイスに配布する方法 : ソフトウェアのインストーラー
   - ソフトウェアのインストーラー ファイルの種類 : Windows インストーラー
   - ソフトウェア セットアップ ファイルの場所の指定 : E:¥Labfiles¥Mod11¥XMLNotepad.msi
   - 発行元 : Microsoft
   - カテゴリ : 生産性
   - 要件
     - アーキテクチャ : 64 ビット
     - オペレーティング システム : Windows 8.1 からすべての新しいオペレーティング システム
8. 結果ウィンドウを更新し、XML Notepad が表示されることを確認します。

▶ 作業 2 : アプリ ストアへの外部リンクを発行する

1. LON-DC1 で、[アプリ] から [アプリ] ノードを参照します。
2. 次の情報を使用して新しいアプリを追加します。
   - このソフトウェアをデバイスに配布する方法 : 外部リンク
   - URL を指定 : https://www.microsoft.com/store/apps/9WZDNCRFJB9S
   - 発行元 : Microsoft
   - 名前 : Word Mobile
   - 説明 : Text Authoring Tool
   - カテゴリ : 生産性
   - おすすめアプリとして表示 : 選択済み

3. 結果ウィンドウを更新し、Word Mobile が表示されることを確認します。

結果 : この練習により、Intune でアプリを発行することができました。

練習 2 : アプリケーションの展開および展開の監視

シナリオ

アプリケーションが発行されたため、XML Notepad を Research グループに展開し、Word Mobile をすべてのユーザー グループに展開することができます。また、次の要件を満たす必要があります。

- XML Notepad には、直ちにインストールできるよう設定された期限付きの展開が必要である
- 発行されたストア アプリにアクセスするために、ユーザーはまず Web ベースの Intune ポータル サイトを使用すること

主な作業は次のとおりです。

1. XML Notepad を Research 部門に展開する
2. Word Mobile を Intune ポータルサイトに展開する
3. インストールを監視する

▶ 作業 1 : XML Notepad を Research 部門に展開する

1. LON-CL1 の Intune 管理コンソールで、[アプリ] を参照し、[XML Notepad 2007] アプリを選択し、[展開の管理] をクリックします。
2. 次の設定でアプリを展開します。
    - グループ : Research Computers
    - 展開 : 必須のインストール
    - 期限 : 直ちに

▶ 作業 2 : Word Mobile を Intune ポータルサイトに展開する

1. LON-CL1 で、Intune 管理コンソールから、[アプリ] を参照し、[Word Mobile] アプリを選択し、[展開の管理] をクリックします。
2. 次の設定でアプリを展開します。
    - グループ : すべてのユーザー
    - 承認 : 利用可能なインストール

▶ 作業 3 : インストールを監視する

1. [グループ] で [すべてのデバイス] をクリックし、[LON-CL1.Adatum.com] を選択します。
2. LON-CL1.Adatum.com で、[ポリシーの更新] リモート タスクを実行します。
3. [リモート タスクの状態] を開き、タスクの状態を確認します。
4. [アプリ] で、[Word Mobile] アプリをクリックし、ソフトウェアの現在の状態を表示します。現在の状態では、このソフトウェアを使用できるユーザーの数が示されています。
5. Word Mobile アプリのプロパティを表示して、アプリへのリンクを受信するユーザーを決定します。
6. LON-CL1 に切り替え、Microsoft Intune Center を開きます。

7. Microsoft Intune Center で、パスワード「Pa$$w0rd」と「DonFunk@<ドメイン名>.onmicrosoft.com」を使用して、Intune ポータルサイトを開きます。
8. Microsoft Intune Center の [更新プログラム] で、[更新プログラムの確認]、[更新プログラムのインストール]、[インストール] の順にクリックします。ポリシーも更新されます。デスクトップに XML Notepad 2007 が表示されます。
9. 開いているウィンドウをすべて閉じます。

結果 : この練習により、Intune を使用して、アプリケーションを展開して監視することができました。

▶ 次の演習の準備をする

次の演習のために、仮想マシンを起動したままにします。

質問 : この演習で、アプリケーションを発行してグループに展開しました。アプリケーションがボリューム ライセンス契約の一部であった場合、次に何をする必要がありますか。

質問 : アプリケーションを Android または iOS デバイスに展開する前に、まず何をする必要がありますか。

レッスン 3
組織のリソースへのアクセスの管理

大多数の組織は、仮想プライベート ネットワーク (VPN) と Wi-Fi 接続を使用してネットワーク リソースにアクセスしています。多くの場合、これらのサービスの構成は複雑で、ヘルプ デスクや管理担当者からの追加のサポートが必要になります。Intune は、リソース アクセス プロファイルを提供して、VPN、Wi-Fi、および電子メール サービスを使用するために必要な設定をデバイスに事前設定できるようにします。このレッスンでは、Intune を使用したリソース アクセス プロファイルの実装に関する考慮事項と手順について説明します。

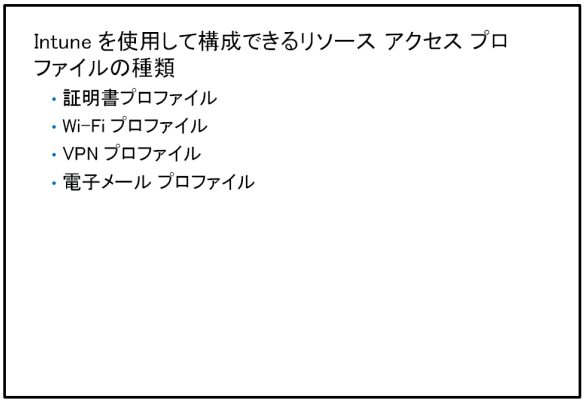
目的

このレッスンにより、次のことを習得できます。

- 組織のリソースへのアクセスを管理する方法を説明することができます。
- Intune により証明書プロファイルを展開する方法を説明することができます。
- Intune により Wi-Fi プロファイルを展開する方法を説明することができます。
- Intune により VPN プロファイルを展開する方法を説明することができます。
- Intune により電子メール プロファイルを展開する方法を説明することができます。
- 条件付きアクセス ポリシーを構成する方法を説明することができます。

組織のリソースへのアクセスを管理する方法

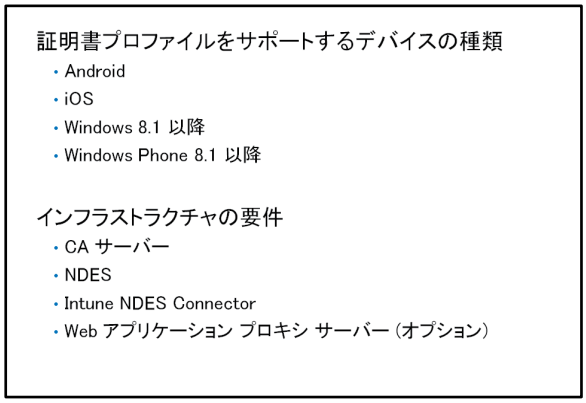
第 9 章では、Intune ポリシーの概念と、ポリシーを使用してクライアントに構成設定を提供する方法について説明しました。リソース アクセス プロファイルはこの概念を拡張し、ユーザーが組織の内部ネットワークに配置されているファイルやサービスにアクセスできるようにします。Intune は、次の種類のリソース アクセス プロファイルの展開をサポートするポリシー設定を提供します。



- **証明書プロファイル :** VPN や Wi-Fi 接続など、証明書を必要とする可能性のある接続方法をセキュリティで保護できるようにするためのサポートを提供します。
- **Wi-Fi プロファイル :** Wi-Fi を使用して組織ネットワークに接続するために必要なワイヤレス設定を展開して、エンドユーザーの構成作業を最小限に抑えます。
- **VPN プロファイル :** VPN テクノロジを使用して組織ネットワークに接続するために必要な VPN 設定を展開できるようにします。
- **電子メール プロファイル :** デバイスに Exchange ActiveSync 電子メール設定を展開して、組織の電子メールにアクセスできるようにします。

注 : すべてのコンピューターやデバイス プラットフォームがすべての種類のリソース アクセス プロファイルをサポートしているわけではないことに注意してください。最新のサポート情報については、http://aka.ms/x4penv を参照してください。

Intune による証明書プロファイルの展開



証明書プロファイルを使用して、オンプレミスの組織のリソースに接続するために必要な証明書を管理対象デバイスに提供します。通常、VPN や Wi-Fi などのサービスはこれらの証明書を使用します。証明書プロファイルの目的は、デバイスを自動的に構成して、証明書を手動でインストールする必要をなくすことです。証明書プロファイルは、次の処理の準備に役立ちます。

- 信頼されたルート証明書をデバイスに展開する。
- 信頼された公開キー基盤からのサービス固有の証明書を要求するようにデバイスを構成する。

次の種類のデバイスは、証明書の登録と更新をサポートしています。

- Android
- iOS
- Windows 8.1 以降
- Windows Phone 8.1 以降

Intune では、証明書の展開に使用する証明書プロファイルとして、次のものがあります。

- **信頼されたルート証明書プロファイル :** 信頼されたルート証明機関 (CA) 証明書または中間 CA 証明書を対象のデバイスに展開するために使用します。使用する各プラットフォーム用の信頼されたルート証明書プロファイルを作成する必要があります。この作成した各プロファイルを、各プラットフォーム用に作成する Simple Certificate Enrollment Protocol (SCEP) 設定プロファイルとペアにします。
- **Simple Certificate Enrollment Protocol (SCEP) 証明書プロファイル :** このプロファイルは、証明書要求のためのプラットフォーム固有の設定を展開するために使用します。各 SCEP 証明書プロファイルを、サポートされるデバイスの各オペレーティング システム プラットフォームに関連付けられた信頼された証明書プロファイルとペアにします。

インフラストラクチャ要件

Intune を使用して証明書の展開をサポートするには、多数のインフラストラクチャ要件が伴います。これには次のような要件があります。

- **CA サーバー :** ネットワーク環境でエンタープライズ CA を使用可能にする必要があります。
- **ネットワーク デバイス登録サービス (NDES) :** 自動デバイス登録をサポートするには、NDES をセットアップする必要があります。このサービスは、証明書の要求と更新をサポートします。
- **Intune NDES Connector :** Intune 管理コンソールから NDES Connector のインストーラー (Ndesconnectorssetup.exe) をダウンロードできます。NDES をインストールしたコンピューターでこのファイルを実行します。
- **Web アプリケーション プロキシ サーバー (オプション) :** デバイスがインターネットを介して証明書を要求および登録できるようにする場合は、Web アプリケーション プロキシ サーバーを構成する必要があります。

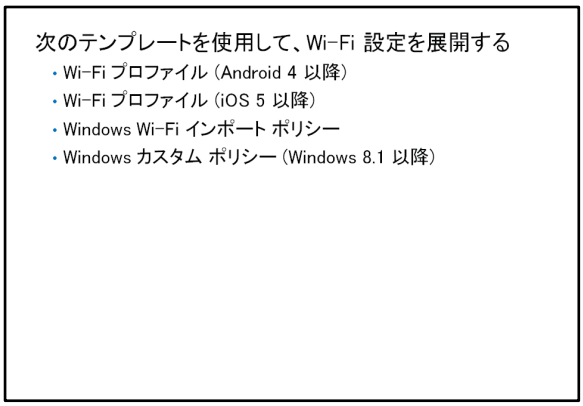
参考資料 : 証明書プロファイルをサポートするインフラストラクチャの詳細については、次を参照してください。
Microsoft Intune で証明書ポリシーを使用して会社のリソースへのアクセスを有効にする
https://technet.microsoft.com/library/dn818904.aspx

Intune による Wi-Fi プロファイルの展開

ネットワーク環境内の管理対象デバイスにワイヤレス ネットワーク設定を展開するには、Wi-Fi プロファイルを使用します。これにより、通常は手動でおこなうワイヤレス セキュリティや接続情報の構成が自動化され、簡単になります。

次の種類のデバイスは、Wi-Fi の自動構成をサポートしています。

- Android 4.0 以降
- iOS 5 以降



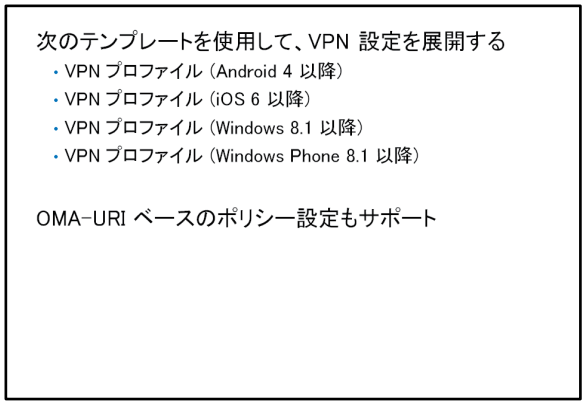
注 : Windows 8.1 以降では、構成済みデバイスから XML 設定ファイルをエクスポートし、Wi-Fi 構成プロファイルにインポートします。

管理対象デバイスで Wi-Fi プロファイルを作成するには、次のポリシー テンプレートを使用します。

- **Wi-Fi プロファイル (Android 4 以降) :** このポリシー設定には、Android デバイス固有のネットワーク接続設定が含まれます。セキュリティの種類、認証方法、サービス セット識別子 (SSID)、および Wi-Fi 接続に関連するその他多数の設定を指定できます。
- **Wi-Fi プロファイル (iOS 5 以降) :** このポリシー設定は、iOS デバイス固有のワイヤレス ネットワーク設定を構成します。これには、SSID、セキュリティ、認証、証明書情報など、多数の設定も含まれます。
- **Windows Wi-Fi インポート ポリシー :** このポリシーでは、既存の Windows 8.1 以降の構成済みコンピューターからエクスポートされた XML 構成プロファイル ファイルを指定してインポートできます。

注 : Wi-Fi 接続を既存のコンピューターからエクスポートするには、netsh wlan ユーティリティを使用します。例えば、コマンド「netsh wlan export profile Wi-Fi < 接続名>」を実行します。Windows 10 デバイスの場合、Windows カスタム ポリシーを構成して、Wi-Fi 接続設定に関連する Open Mobile Alliance Uniform Resource Identifier (OMA-URI) 設定を指定することもできます。

Intune による VPN プロファイルの展開



VPN 接続設定を管理対象のコンピューターおよびデバイスに展開するには、VPN プロファイルを使用します。これらの接続設定は、VPN に接続するために必要な接続とセキュリティの情報を提供し、内部ネットワーク リソースにアクセスできるようにします。

次の種類のデバイスは、VPN プロファイルによる展開をサポートしています。

- Android 4.0 以降
- iOS 6 以降
- Windows 8.1 以降 (Windows RT 8.1 を含む)
- Windows Phone 8.1 以降

次のポリシー テンプレートを使用して、管理対象デバイスに次の VPN プロファイルを作成します。

- VPN プロファイル (Android 4 以降)
- VPN プロファイル (iOS 6 以降)
- VPN プロファイル (Windows 8.1 以降)
- VPN プロファイル (Windows Phone 8.1 以降)

これらの各プロファイル テンプレートは、VPN サーバー アドレス、認証方法、プロキシ設定、および使用している VPN 接続の種類に関連する特定の設定などの設定を提供します。

VPN 接続の種類

Intune は、次の表に一覧する VPN 接続の種類をサポートしています。

接続の種類	サポートされるプラットフォーム (以降のすべてのバージョンを含む)
Cisco AnyConnect	iOS、Android
Juniper Pulse	iOS、Android、Windows Phone 8.1、Windows 8.1/Windows RT 8.1
F5 Edge Client	iOS、Android、Windows Phone 8.1、Windows 8.1/Windows RT 8.1
Dell SonicWALL Mobile Connect	iOS、Android、Windows Phone 8.1、Windows 8.1/Windows RT 8.1
Check Point Mobile VPN	iOS、Android、Windows Phone 8.1、Windows 8.1/Windows RT 8.1

注 : Windows カスタム ポリシーまたは Windows Phone OMA-URI ポリシーを作成し、OMA-URI 設定を使用して VPN 接続設定を指定できます。これは、Windows Phone 8.1 デバイス、Windows 10、および Windows 10 モバイル デバイスを使用してサポートされます。詳細については、http://aka.ms/pgaoa9 を参照してください。

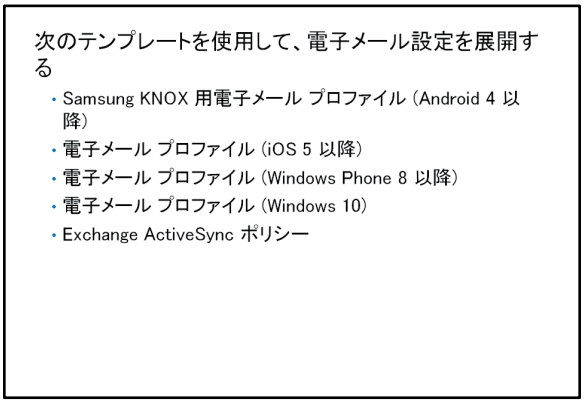
証明書の要件

VPN 接続の認証要件によっては、以前に Intune で作成した SCEP 証明書プロファイルも必要になる場合があります。SCEP プロファイルは、セキュリティで保護された VPN 接続を確立するために必要な証明書の要求に使用されます。

Intune による電子メール プロファイルの展開

Intune には主に 2 種類のポリシー テンプレートが用意されており、これを使用してデバイスで Exchange ActiveSync 電子メール設定を展開して構成します。次の種類のデバイスは、電子メール プロファイルの構成をサポートしています。

- Samsung KNOX Standard (Android 4.0 以降)
- iOS 5 以降
- Windows Phone 8 以降
- Windows 10



管理対象デバイスで電子メール プロファイルを管理するには、次のポリシー テンプレートを使用します。

- Samsung KNOX 用電子メール プロファイル (Android 4 以降)
- 電子メール プロファイル (iOS 5 以降)
- 電子メール プロファイル (Windows Phone 8 以降)
- 電子メール プロファイル (Windows 10)

これらの各プロファイル テンプレートは、Exchange ActiveSync のホスト名やアカウント名などの設定を提供します。また、電子メール プロファイルは、Exchange Server と同期する電子メールの日数を指定する同期設定も提供します。

電子メール プロファイルと共に構成するもう 1 つのポリシーとして、Exchange ActiveSync ポリシーがあります。このポリシー テンプレートは、パスワード設定、暗号化設定、電子メール設定、デバイス機能などの一般的な設定を提供します。このポリシーはすべてのプラットフォームに適用され、各プラットフォームのオペレーティング システムでサポートされている設定のみに反映されます。

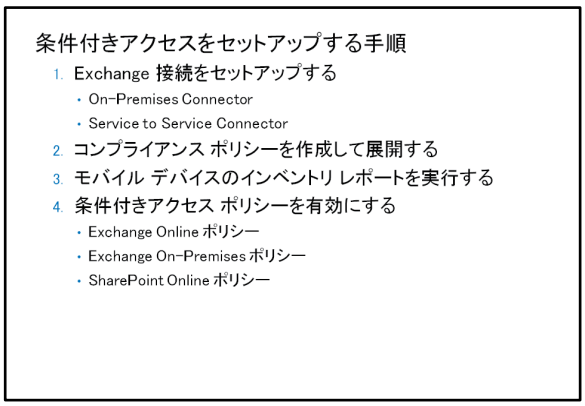
認証の要件

Exchange 接続の認証の要件によっては、Intune で以前作成した SCEP 証明書プロファイルも必要になる場合があります。SCEP プロファイルは、セキュリティで保護された電子メール接続を確立するために必要な証明書の要求に使用されます。代わりに、ユーザーのユーザー名とパスワードによる認証を必要とするように選択することもできます。電子メール プロファイルにはパスワードは含まれていないため、ユーザーは、Exchange サーバーに接続する際、パスワード情報を提供する必要があります。

ネットワーク リソースへの条件付きアクセスの構成

条件付きアクセスでは、構成されたポリシー設定に従って、特定のデバイスによる Exchange サービスまたは SharePoint サービスへのアクセスを許可またはブロックできます。条件付きアクセスは、特に次のサービスへのアクセスを管理するために使用できます。

- Exchange Online
- Exchange Online Dedicated
- オンプレミスの Exchange
- SharePoint Online



管理対象デバイスで条件付きアクセスを管理するには、次のポリシー テンプレートを使用します。

- **コンプライアンス ポリシー :** これを使用して、Exchange サービスまたは SharePoint サービスへのアクセスを判断する際の規則を指定します。規則には、パスワード設定、暗号化設定、および Intune が電子メール アカウントを管理する必要があるかどうかの設定が含まれます。
- **Exchange Online ポリシー :** このポリシーのオプションは、「デバイスがポリシーに準拠していない場合に、電子メール アプリから Exchange Online へのアクセスをブロックします。」を含みます。このオプションが選択されている場合、デバイスはコンプライアンス ポリシーで指定されたすべての規則に適合する必要があります。
- **Exchange On-Premises ポリシー :** このポリシーでは、ポリシーを適用する Intune のユーザー グループを構成できます。また、Exchange ActiveSync の詳細設定や適用するカスタム規則、およびコンプライアンス ポリシー設定も構成できます。
- **SharePoint Online ポリシー :** このポリシーのオプションは、「デバイスがポリシーに準拠していない場合に、アプリから SharePoint Online へのアクセスをブロックします。」を含みます。このオプションが選択されている場合、デバイスはコンプライアンス ポリシーで指定されたすべての規則に適合する必要があります。

条件付きアクセス ポリシーをセットアップするには、次の手順を実行します。

1. **Exchange 接続をセットアップする :** Intune では次の 2 種類のコネクタをセットアップできます。
    - **On-Premises Connector :** 使用環境でホストされている Exchange 環境への接続をセットアップするには、このコネクタを使用します。このオプションにより、On-Premises Connector ソフトウェアをダウンロードして、それをネットワーク環境内のコンピューターにインストールできます。
    - **Service to Service Connector :** ホストされる Exchange 環境への接続をセットアップするには、このコネクタを使用します。このコネクタを使用するには、Exchange 2013 テナントが構成されている Office 365 アカウントが必要です。

    Exchange コネクタは、Intune 管理コンソールで [管理] からダウンロードまたはセットアップできます。
2. **コンプライアンス ポリシーを作成して展開する :** コンプライアンス ポリシーの作成により、各デバイスで評価する必要がある規則を指定できます。また、対応する Exchange ポリシーまたは SharePoint ポリシーを指定しない場合、コンプライアンス結果はレポートに記録されるだけで、ユーザー アクセスは制限されません。
3. **モバイル デバイスのインベントリ レポートを実行する :** このレポートは、各デバイスの結果を提供して、管理者がユーザーに対する影響を判断できるようにします。ユーザーがコンプライアンス ポリシー規則に準拠するようにデバイスを構成していない場合、管理者は、まもなくブロックされることをユーザーに通知できます。
4. **条件付きアクセス ポリシーを有効にする :** 非準拠のデバイスを制限する準備が整ったら、Exchange Online、Exchange On-Premises、または SharePoint Online の条件付きアクセス ポリシー設定を有効にすることができます。

知識の確認

質問	
証明書の自動要求と更新を提供するには、次のどのサービスを使用しますか。	
正しい解答を選択してください。	
	ネットワーク アクセス保護
	Web アプリケーション プロキシ サーバー
	Active Directory ドメイン サービス
	NDES

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
Intune の条件付きのアクセスは、VPN プロファイルを使用して組織のネットワークへ接続するデバイスを制御します。	

演習 B : Intune によるリソースへのアクセスの管理

シナリオ

VPN の管理を簡素化するために、Intune を使用し、必要な証明書と VPN 接続設定を管理対象のデバイスに展開することに決めました。Intune には、ActiveSync 経由で Office 365 Exchange 環境を接続するすべてのデバイスを管理するための要件があります。Intune がすべての ActiveSync 接続を管理できるよう、Intune と Office 365 を統合し、ポリシー設定を適用することにしました。

目的

この演習により、次のことを習得できます。

- Intune での証明書の展開を構成することができます。
- 条件付きアクセス ポリシーを構成することができます。

演習のセットアップ

予定所要時間 : 30 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 MSL-TMG1
ユーザー名	Adatum¥Administrator Adatum¥Don
パスワード	Pa$$w0rd

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Don」、パスワード「Pa$$w0rd」を使用してサインインします。
6. インターネットへのアクセスのために、MSL-TMG1 を起動します。

注 : この演習を完了するためには、第 8 章から第 10 章のすべての前提条件を満たし、第 8 章から第 10 章の演習を完了する必要があります。また、第 5 章で構成した Office 365 アカウントも使用します。

練習 1 : Intune での証明書の展開の構成

シナリオ

コンピューターやモバイル デバイスへの VPN の構成を簡素化するために、Intune を使用して、証明書と VPN 接続設定を展開することに決めました。

主な作業は次のとおりです。

1. 信頼済み証明書プロファイルを構成して展開する
2. Simple Certificate Enrollment Protocol (SCEP) 証明書プロファイルを構成して展開する
3. 仮想プライベート ネットワーク (VPN) プロファイルを構成して展開する

▶ 作業 1 : 信頼済み証明書プロファイルを構成して展開する

1. LON-DC1 に切り替え、Internet Explorer を開きます。
2. http://manage.microsoft.com を参照します。
3. Intune 管理コンソールにアクセスするための資格情報を入力します。
4. [ポリシー] で、[構成ポリシー] ノードを参照します。
5. 次の設定を使用して新しい構成ポリシーを追加します。
   - テンプレート : 信頼済み証明書プロファイル (Windows 8.1 以降)
   - 名前 : Windows RootCert Policy
   - 説明 : Certificate for the Adatum Root CA
   - 証明書ファイル : RootCert.cer (E:¥Labfiles¥Mod11¥RootCert.cer)
6. 新しいポリシーを [すべてのコンピューター] デバイス グループに展開します。

▶ 作業 2 : Simple Certificate Enrollment Protocol (SCEP) 証明書プロファイルを構成して展開する

1. [ポリシー] で、[構成ポリシー] ノードを参照します。
2. 次の設定を使用して新しい構成ポリシーを追加します。
   - テンプレート : SCEP 証明書プロファイル (Windows 8.1 以降)
   - 名前 : Windows SCEP Policy
   - 説明 : SCEP policy for Windows computers
   - SCEP サーバー URL : http://lon-dc1/certsrv/mscep
   - サブジェクトの別名 : ユーザー プリンシパル名 (UPN)
   - 証明書の有効期間 : 2 年
   - キー使用法
     - キーの暗号化
     - デジタル署名
   - ハッシュ アルゴリズム : SHA-1
   - 拡張キー使用法 : 任意の目的
   - ルート証明書の選択 : Windows RootCert Policy
3. 新しいポリシーを [すべてのコンピューター] デバイス グループに展開します。

▶ 作業 3 : 仮想プライベート ネットワーク (VPN) プロファイルを構成して展開する

1. [ポリシー] から [構成ポリシー] ノードを参照します。
2. 次の設定を使用して新しい構成ポリシーを追加します。
   - テンプレート : VPN プロファイル (Windows 10 Desktop および Mobile 以降)
   - 名前 : Windows VPN Policy
   - 説明 : VPN policy for Windows computers
   - VPN 接続名 : Adatum VPN
   - 接続の種類 : Check Point Capsule VPN
   - VPN サーバーの説明 : Adatum VPN
   - サーバーの IP アドレスまたは FQDN : Checkpoint.adatum.com
3. 新しいポリシーを [すべてのコンピューター] デバイス グループに展開します。

結果 : この練習により、Intune で証明書の展開を構成することができました。

練習 2 : 条件付きアクセス ポリシーの構成

シナリオ

すべてのモバイル デバイスのセキュリティを保護し、またそれらのデバイスを Intune で管理できるようになってから、Exchange ActiveSync を使用して Exchange へのアクセスを可能にする必要があります。Microsoft Exchange コネクタを使用して、Intune を Office 365 を統合する必要があります。必要に応じて、コンプライアンスと Exchange Online ポリシーを構成します。

主な作業は次のとおりです。

1. Microsoft Exchange コネクタを構成する
2. コンプライアンス ポリシーを構成する
3. Microsoft Exchange Online ポリシーを構成する

▶ 作業 1 : Microsoft Exchange コネクタを構成する

1. LON-DC1 の Intune 管理コンソールで、[管理者] を参照し、[Microsoft Exchange] ノードを展開して、[Exchange 接続のセットアップ] をクリックします。
2. Office 365 の Service to Service Connector のセットアップをおこない、クイック同期を実行します。

▶ 作業 2 : コンプライアンス ポリシーを構成する

1. [ポリシー] で、[コンプライアンス ポリシー] ノードを参照します。
2. 次の設定を使用して新しいコンプライアンス ポリシーを追加します。
   - 名前 : Exchange Compliance Policy
   - モバイル デバイスのロック解除にパスワードを必要とする : はい
   - 必要なパスワードの種類 : 有効化し、[数値] を選択
   - 他の値は既定値のまま
3. 新しいポリシーを [すべてのユーザー] グループに展開します。

▶ 作業 3 : Microsoft Exchange Online ポリシーを構成する

1. [ポリシー] で、[条件付きアクセス] ノードを参照します。
2. 次の設定を使用して新しい Exchange Online ポリシーを追加します。
   - Exchange Online の条件付きアクセス ポリシーを有効にする : 選択済み
   - デバイス プラットフォーム : iOS、Android、および Windows 10 Mobile
   - Windows デバイスは次の要件を満たしている必要があります
   - [デバイスは準拠デバイスである必要があります] と [Microsoft Intune でサポートされていないデバイスから電子メールへのアクセスをブロックする]
   - [対象グループ] : Helpdesk Administrator

注 : この演習では、既定の Helpdesk Administrator グループのみを選択します。運用環境で、1 つ以上の Active Directory セキュリティ グループを選択することになります。

3. 新しいポリシーを保存します。

結果 : この練習により、Intune を使用して、条件付きアクセス ポリシーを構成することができました。

▶ 次の章の準備をする

演習が完了したら、仮想マシンを初期状態に戻します。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. [仮想マシン] リストで、[23697-2B-LON-DC1] を右クリックし、[戻す] をクリックします。
3. [仮想マシンを戻す] ダイアログ ボックスで、[戻す] をクリックします。
4. 起動中のすべての仮想マシンに対して、手順 2 ～ 3 を繰り返します。

質問 : この演習により、信頼済み証明書プロファイルと Simple Certificate Enrollment Protocol (SCEP) 証明書プロファイルを構成することができました。ネットワーク デバイス登録サービス (NDES) が Intune クライアントからの要求に応答するためには、他に何をおこなう必要がありますか。

質問 : この演習では、コンプライアンス ポリシーが有効化された直後に Microsoft Exchange Online ポリシーを構成しました。運用環境で、Exchange Online ポリシーを有効化する前に、まず何をおこなう必要がありますか。

復習とまとめ

復習問題

質問 : あなたは、Windows 10 ワークステーションに VPN 接続設定を展開する必要があります。ポリシー設定に一覧表示されていない組み込みの VPN 接続ソリューションは使用しないでください。Windows 10 コンピューターをサポートするためにできることは何ですか。

質問 : あなたの組織では、Intune を使用して展開する最新のアプリケーションが開発されました。あなたは、さまざまな部門に基づいて、アプリケーション内で、特定の機能を制御する方法を提案する必要があります。この場合、何をする必要がありますか。