第 8 章

エンタープライズ モビリティ ソリューションによる Windows 10 デバイスの管理

目次

概要

使用中のデバイスの管理が大きく変わりました。数年前は、ほとんどの作業がデスクトップ コンピューターとノート PC でおこなわれていましたが、今日のビジネス環境では、多くの作業がさまざまな種類のモバイル デバイスで実施されています。これを可能にするには、すべての種類のデバイス上でデータを保護することに加えて、適切なツールとテクノロジを使用して、これらのデバイスを管理することが必要です。

さらに、ますます多くのアプリケーションが、Software as a Service (SaaS) モデルに基づいて提供されるので、ユーザーを認証して必要なリソースへのアクセスを可能にする、グローバルにアクセス可能な ID 管理システムが必要になります。

エンタープライズ モビリティ戦略は、これらのニーズに対応するアプローチを定義します。この章では、Microsoft のエンタープライズ モビリティの実装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。

- Enterprise Mobility Suite について説明することができます。
- Microsoft Azure Active Directory (Azure AD) Premium を使用して、ディレクトリ サービスを管理することができます。
- Azure Rights Management (Azure RMS) を使用して、デバイスを保護することができます。
- Microsoft Intune のオプションについて説明することができます。

レッスン 1
Enterprise Mobility Suite の概要

Enterprise Mobility Suite は、現在の情報技術 (IT) 環境の課題とニーズに対応するために、Microsoft が提供する一連のテクノロジです。Azure AD Premium、Azure RMS、および Intune プラットフォームの機能を使用して、デバイス、アプリケーション、データを管理、展開、および保護するためのテクノロジを提供します。

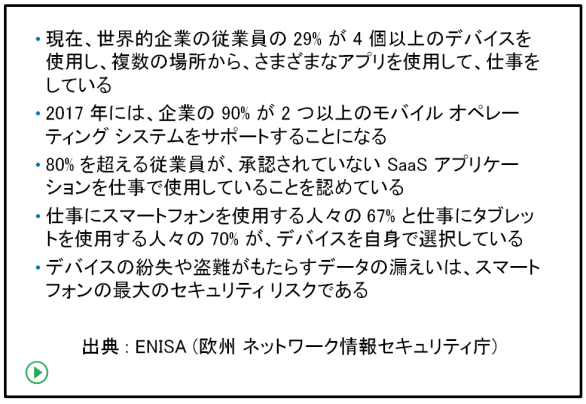
目的

このレッスンにより、次のことを習得できます。

- Enterprise Mobility Suite のコンポーネントについて説明することができます。
- Enterprise Mobility Suite の実用的な用途を識別することができます。
- Enterprise Mobility Suite の実装の要件について説明することができます。

Enterprise Mobility Suite とは

エンタープライズ モビリティは、新しいサービスとアプリケーション、さらにそれらを実行するデバイスを管理および操作する方法を定義する概念です。エンタープライズ モビリティは、組織の重要な要件になっています。また、エンタープライズ モビリティは、モバイル デバイス管理 (MDM) と誤解される場合がありますが、MDM 単独よりも多くの用途があります。



最近の調査では、現在、ますます多くの組織が、モバイル デバイスと SaaS アプリケーションの両方に関する同様の課題に直面しています。例えば、携帯電話、タブレット、ノート PC などのすべてのデバイスで稼働する 1 つの統合されたモバイル プラットフォームを保有する組織は、現在ほとんど見られません。通常は、少なくとも 2 つ (場合によっては 3 つ以上) の異なるプラットフォームが、従業員のデバイスで稼働しています。さらに、組織が Bring Your Own Device (BYOD) の概念をサポートする場合、使用するデバイスを従業員が選択します。ほとんどのサービスをオンラインで使用できるようにすることで、従業員はどこでも、どのデバイスでも作業できます。一般的に、適切なテクノロジを使用して対応しない限り、これらすべての新しい概念は、重大なデータ漏えいリスクとデータ セキュリティ リスクをもたらす可能性があります。

今日のデータとデバイスは、Active Directory ドメイン サービス (AD DS) でノート PC とデスクトップを管理するために使用されていたものと同じテクニックとテクノロジでは、適切に管理できません。それにもかかわらず、これらのデバイスには、保護する必要がある大量のビジネス データが保持されています。さらに、IT 部門は、これらのデバイスが業務用途で使用されている限り、デバイスを管理、制御できる必要があります。BYOD の概念では、IT 部門はユーザーのデバイスを完全な管理下に置くことができないので、組織には、デバイスのビジネス関連のアプリとデータのみを保護できるテクノロジが必要になります。

これらすべての要件により、デバイスとデータの新しい管理機能を備えた、新しいプラットフォームが必要になります。

Microsoft Enterprise Mobility Suite は、これらの要件のほとんどに対応しています。Enterprise Mobility Suite は、単体のソフトウェア、または単一のテクノロジではありません。ID 管理、データ保護、およびデバイスとソフトウェアの管理のために作成された、一連の製品およびテクノロジです。つまり、Enterprise Mobility Suite は、組織がエンタープライズ モビリティ戦略を定義、設計、および実装し、これらの新しいモビリティとクラウドのトレンドを積極的に活用するのに役立ちます。

Enterprise Mobility Suite には、次の 3 つの重要なコンポーネントがあります。

- **Azure AD Premium (ID とアクセスの管理) :** Microsoft クラウド プラットフォームの基本的なサービスの 1 つです。Office 365、Intune などのクラウド サービスをサポートする、クラウドベースの ID ソリューションを提供します。また、ローカルに展開された AD DS と同期することもできます。
- **Microsoft Intune (モバイル デバイス管理 (MDM) とアプリケーション管理) :** クラウドベース サービスを使用して、オンプレミスのデスクトップ コンピューターまたはノート PC の管理に加えて、従業員が使用するすべての種類のモバイル デバイスを管理できます。さらに、Intune により、モバイル デバイスおよびコンピューター向けのアプリケーションを管理し、展開することもできます。
- **Azure RMS (あらゆる場所とデバイスに対応したデータ保護) :** ローカルに展開された Active Directory Rights Management サービス (AD RMS) と同様の機能を、クラウドで提供します。これにより、一般的なドキュメントの種類に対する実装しやすい保護が可能になります。あらゆるデバイスで、Azure RMS が保護するドキュメントを利用することができます。ただし、ユーザーは承認される必要があります。

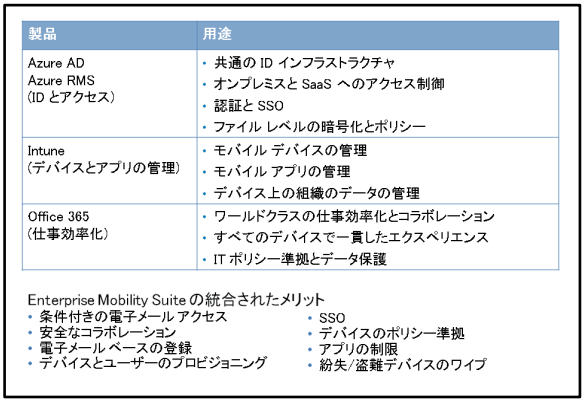
これらすべてのサービスについては、この章で後ほど詳しく説明します。

Enterprise Mobility Suite は、コスト効率の高いソリューションです。これは、Enterprise Mobility Suite のライセンスは、Enterprise Mobility Suite の各製品のライセンスを個別に購入するよりも大幅に安価なためです。さらに、ユーザーが使用するデバイスの数にかかわらず、ユーザー単位でライセンスされることもその理由です。

参考資料 : Microsoft エンタープライズ モビリティについては、次のサイトを参照してください。
Enterprise Mobility Suite
https://www.microsoft.com/ja-jp/server-cloud/products-Enterprise-Mobility-Suite.aspx

Enterprise Mobility Suite の用途

Enterprise Mobility Suite の 1 つまたは複数のコンポーネントを使用して、さまざまなシナリオで、デバイス管理機能とデータ保護要件を拡充することができます。



Azure AD Premium

一般的なシナリオでは、Azure AD Premium をローカルの AD DS の拡張機能として使用します。AD DS をクラウド内の Active Directory サービスと同期することにより、オンプレミスのアプリとサービス、およびクラウドのアプリとサービスに対して、シングル サインオン (SSO) 機能を使用できます。また、Azure AD Premium は、ローカルの AD DS のみでは実現できないセルフサービスのパスワード再設定や多要素認証などの追加機能も提供します。

Intune

Enterprise Mobility Suite の最も一般的な用途の 1 つは、コンピューターとモバイル デバイス (タブレットや携帯電話など) の両方に対する Intune を使用したデバイス管理です。Intune は、Windows、Android、および iOS の各プラットフォームにおけるすべての種類のデバイスを管理する効率的なメカニズムを提供するので、多くの組織は Intune を使用して、業務で使用するデバイスとアプリケーションの登録と制御をおこなっています。

Azure RMS

クラウドベースの Microsoft Rights Management サービス (RMS) であり、ローカルに展開された AD RMS と同様の機能を提供しますが、ネイティブな PDF 保護、保護されたドキュメントのさらに容易な共有、エクスプローラーや Microsoft Office アプリケーションとの統合などの機能が追加されています。Azure RMS を使用することで、ドキュメントが存在する場所に依存する、コンピューターに束縛されたファイル アクセス許可とは異なり、.docx、.xlsx、.pdf などの一般的な種類のドキュメントを恒久的に保護できます。さらに、Azure RMS は既定でグローバルに利用できるので、ローカルに実装された AD RMS と比較して、保護されたドキュメントの共有が大幅に容易になります。

注 : Azure RMS は、Office 365 RMS の機能を拡張するものとして使用できます。

Enterprise Mobility Suite は、Office 365 と連携して使用できます。Enterprise Mobility Suite サービスは、Office 365 テナントと容易に統合できるので、Office 365 サービスの機能を大幅に拡張できます。

Enterprise Mobility Suite の実装の要件

Enterprise Mobility Suite を実装するには、最初に、環境に必要なコンポーネントとテクノロジを決定する必要があります。Enterprise Mobility Suite の各コンポーネントは個別に展開されますが、いくつかの展開シナリオには共通の前提条件があります。

Enterprise Mobility Suite のすべてのコンポーネントはクラウドベース サービスなので、オンプレミスのシステムに対しては、ほとんど要件はありません。

- Azure AD Premium
  - Windows Server 2003 以降のフォレスト機能レベル
  - Windows Server 2008 SP1 以降
- Azure RMS
  - Windows 7 以降、Mac OS X 10.8 以降、Windows 8 RT
  - Windows Phone 8.1、Android 4.0.3、iOS 7
  - Office 2010 以降
- Intune
  - ポート 80 と 443 経由の通信を確保する

Azure AD Premium

ほとんどの組織で一般的におこなわれているように、ローカルに AD DS を展開している場合、AD DS オブジェクトを Azure AD と同期した後で、Enterprise Mobility Suite の他のコンポーネントを展開することをお勧めします。これは必須のタスクではありませんが、AD DS のユーザーとグループのオブジェクトを Azure AD と同期することで、ユーザーはクラウドベース サービスとローカルの AD DS で同じ資格情報を使用できるようになります。この方法を選択しない場合、Azure AD に別のユーザー アカウントを作成する必要があり、このシナリオでは、ユーザーはローカルの AD DS と Enterprise Mobility Suite サービスにサインインするために、複数の資格情報を保有することになります。このようなシナリオを維持するのは困難であり、エンド ユーザーの余分な関与が必要になるので、ほとんどの組織はこのシナリオを避けることになります。

ローカルの AD DS を Azure AD と同期することを決定した場合、同期を実行するコンピューターに Windows Server 2008 Service Pack 1 (SP1) 以降がインストールされていることを確認します。ローカルの AD DS ドメインは、Windows Server 2003 以降のフォレスト機能レベルである必要があります。

Azure RMS と Intune の両方のサービスは、ID 管理サービスを Azure AD に依存しています。したがって、Azure AD にユーザー オブジェクトを提供した後で、これらの Enterprise Mobility Suite サービスを使用する必要があります。

Azure RMS

Azure RMS を使用するには、Azure AD が稼働していることに加えて、サポート対象のクライアント デバイスを保有している必要があります。デスクトップとノート PC の場合は、Windows 7 および Mac OS X 10.8 の各オペレーティング システムがサポート対象です。
モバイル デバイスの場合は、Windows Phone 8.1、Android 4.0.3、iOS 7、および Windows 8 RT の各オペレーティング システムがサポートされます。これらよりも新しいプラットフォームも、すべてサポートされます。

Azure RMS はアプリケーションの内部で機能するので、保有するアプリケーションが Azure RMS をサポートすることを確認することも必要です。Windows オペレーティング システムでは Microsoft Office 2010 以降がサポートされ、Mac OS X オペレーティング システムでは Microsoft Office 2011 以降がサポートされます。PDF ドキュメントに対して RMS 保護を使用する場合、Microsoft の RMS 共有アプリ、または Foxit Reader、Nitro Reader、TITUS Docs などの Microsoft 以外のアプリを使用できます。

Intune

Intune の場合、管理対象のデバイスと、クラウドベース サービスが使用するインターネット上の Web サイトとが、ネットワーク インフラストラクチャ上で通信できる必要があります。ほとんどの通信は、ポート 80 と 443 を使用しておこなわれます。Intune を使用してデスクトップ コンピューターとノート PC を管理する場合、Windows Vista 以降が稼働していることを確認します。

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
Enterprise Mobility Suite は、サーバーにインストール可能な製品です。	

レッスン 2
Azure Active Directory Premium の概要

Azure AD は、ディレクトリ サービス、高度な ID 管理、およびアプリケーション アクセス管理を組み合わせて ID とアクセスを管理するための包括的なクラウド ソリューションであり、開発者にリッチな標準プラットフォームを提供します。クラウド内に Active Directory のインスタンスを提供し、それを使用することで、オンプレミスとクラウドのリソースにアクセスできます。

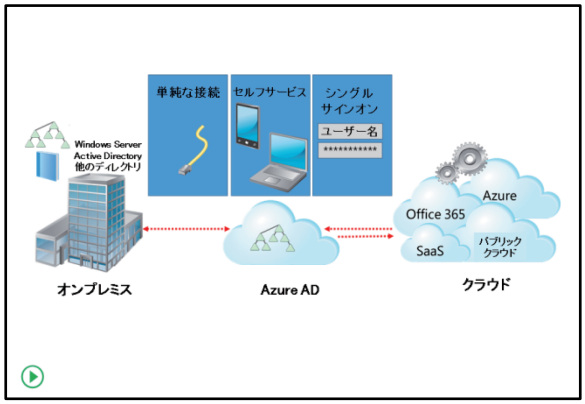
目的

このレッスンにより、次のことを習得できます。

- Azure AD Premium について説明することができます。
- オンプレミスの AD DS を Azure AD と統合するための考慮事項について説明することができます。
- Azure AD で、多要素認証とパスワードを管理することができます。
- Azure AD がサポートする SaaS アプリケーションについて説明することができます。
- SaaS アプリケーションへのアクセスを可能にすることができます。
- Windows 10 で Azure AD を使用する方法について説明することができます。

Azure Active Directory Premium とは

Azure AD は、多種多様なシナリオで使用できるオンライン ディレクトリ サービスです。これを使用することで、AD DS 実装をクラウドに拡張したり、クラウドベース アプリケーションをサポートしたりできます。Azure AD は、サポートするための物理インフラストラクチャを構築することなく、サービスとしての ID を提供します。



Azure AD は当初、Office 365 向けのディレクトリ サービスとして開発され、Intune などの他のアプリケーションをサポートするように拡張されました。現在は、独立したサービスとして利用できます。

Azure AD は、次のアプリケーションで使用できます。

- **内部ユーザー向けの独自のクラウドベース アプリケーション :** Azure AD は、クラウドベース アプリケーション向けの属性ストアとして使用できます。ユーザー認証は、Azure AD で実行できますが、Active Directory フェデレーション サービス (AD FS) とオンプレミスの AD DS を使用しておこなうこともできます。
- **外部ユーザー向けの独自のクラウドベース アプリケーションまたはオンプレミス アプリケーション :** Azure AD は、クラウドベース アプリケーション向けの属性ストアとして使用できます。ユーザー認証は、Azure AD で実行できますが、他の ID プロバイダーと統合したさまざまな認証メカニズムを使用することもできます。
- **Microsoft 以外のベンダーが提供するクラウドベース アプリケーション :** Azure AD を使用して、必要な情報のみを Microsoft 以外のクラウド アプリケーション プロバイダーに提供し、Microsoft 以外のアプリケーションに対してユーザーを認証することができます。

Azure AD の重要なメリットの 1 つは、プラットフォームに依存しないことです。Azure AD は、AD DS と AD FS を使用することで Windows ベースの環境と統合できますが、他のさまざまなプラットフォームをサポートすることもできます。

Azure AD は、3 つのエディション (Free、Basic、および Premium) で利用できます。Azure AD の Premium エディションは、Enterprise Mobility Suite に含まれています。Azure AD Premium には、Free および Basic のエディションで使用できるすべての機能が含まれています。さらに、ID 管理機能と SaaS アプリケーション アクセス機能が提供されます。

Basic および Free のエディションにはない、Azure AD Premium の重要なメリットとしては、次のものがあります。

- ユーザー管理だけではなく、グループ管理を提供します。
- オンプレミスへの書き戻しを含むセルフサービスのパスワード再設定機能を搭載しています。
- 2,000 以上の事前構成された SaaS アプリケーションに対応した SSO 機能を提供できます。
- 潜在的な脅威を容易に識別することを可能にする高度なセキュリティ レポート、および脅威を認識して防御するメカニズムを提供します。
- 多要素認証を提供します。

参考資料 : Azure AD については、次のサイトを参照してください。
Azure Active Directory とは
https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-whatis/

オンプレミスの AD DS を Azure AD と統合するための考慮事項

ほとんどの Microsoft クラウド サービスは、Azure AD に依存しています。ローカルに展開された Exchange Server、SharePoint、System Center などのサービスは、AD DS に大きく依存するのと同様に、Office 365、Intune などのクラウド サービスは、Azure AD に依存しています。

- 次のシナリオ向けにローカルの AD DS と Azure AD を統合できる
  - クラウドベース ユーザー
  - クラウドベース ユーザー (パスワード同期を実施)
  - フェデレーション ユーザー
- AD DS と Azure AD 間に Azure AD Connect を実装する場合は、次を考慮する
  - パスワード同期により、同期対象のすべてのユーザー アカウントでパスワードが同期される
  - パスワード同期エージェントは、2 分ごとに実行される
  - 同じパスワード ポリシーがクラウドベースのユーザーとオンプレミスのユーザーに適用される
  - Azure AD では、パスワードが期限切れになることはない

ただし、通常は同じユーザーがオンプレミスとクラウドの両方のサービスを使用しているので、認証と承認に関する問題が発生します。ローカルに展開された AD DS は、ローカルに展開されたリソースに対して、認証、承認、および SSO を提供します。この場合、Office 365 テナントのメールボックスなどのクラウドベース リソースにアクセスする際に、これらの同じユーザーを認証および承認する方法を検討する必要があります。ほとんどの組織とエンド ユーザーは、クラウド リソースにアクセスするために、ローカル リソースの場合と同じ方法でオンプレミスの AD DS 資格情報を使用することを期待しています。ある資格情報セットをローカルに展開されたサービスに使用し、別のセットをクラウド サービスに使用するなど、複数の資格情報を保有することを受け入れるユーザーはほとんどいません。

ローカルとクラウドの両方のリソースに対して SSO エクスペリエンスおよび単一の資格情報セットを保有するという共通的なニーズに対応するには、ローカルの AD DS を Azure AD インスタンスと同期する必要があります。

ローカルの AD DS を Azure AD と同期することにより、実際にユーザーとグループの各オブジェクトの一部が Azure AD にコピーされます。また、Azure AD が、ローカルに展開された AD DS に接続することなくユーザーを認証できるように、ユーザー オブジェクトのパスワード ハッシュを Azure AD と同期するように選択することもできます。パスワード自体は、Azure AD と同期されないことに留意してください。認証プロセスでユーザー アカウントを検証するには、パスワード ハッシュで十分であり、パスワード ハッシュを使用してユーザーのパスワードを明らかにすることはできません。パスワード ハッシュを Azure AD のユーザー アカウントと同期しないように選択した場合、Azure AD からの認証要求が、ローカルの AD DS ドメイン コントローラーに転送されるように、可用性の高いオンプレミスの AD FS を展開する必要があります。どちらも場合も、エンド ユーザーにとっては同じ結果になります。つまり、エンド ユーザーは、ローカルの AD DS 資格情報を使用してローカルとクラウドの両方のリソースにアクセスできます。

Microsoft クラウド サービスを実装する際におこなう必要性が高い、最初で最大の決定の 1 つは、ローカルの AD DS を Azure AD と同期するかどうかです。

ディレクトリ同期

Azure AD Connect は、オンプレミスの AD DS のユーザー アカウントを、Azure AD と自動的に同期するツールです。Azure AD Connect を使用すると、オンプレミスのユーザー情報が、Azure AD に自動的に反映されて使用できるようになります。ユーザー名は、同期プロセスの一環として同期されます。これにより、オンプレミスの認証と Azure AD でユーザー名が同じであることが保証されるので、サインインが簡略化されます。

Azure AD Connect は、次のシナリオで使用できます。

- **クラウドベース ユーザー :** このシナリオでは、Azure AD Connect はユーザーのアカウント情報を Azure AD と同期しますが、パスワードはクラウドベースのユーザー アカウント用として別に構成されます。オンプレミスでユーザー パスワードが変更された場合、パスワードを同期する方法がないので、ユーザーが混乱する場合があります。この場合は、Azure AD が認証を実行します。
- **クラウドベース ユーザー (パスワード同期を実施) :** このシナリオでは、Azure AD Connect はユーザーのアカウント情報とパスワードを Azure AD と同期します。この方法により、Azure AD とオンプレミスの AD DS でパスワードが同じになるので、ユーザーのサインイン時の混乱を避けられます。この場合も、Azure AD が認証をおこないます。
- **フェデレーション ユーザー :** このシナリオでは、Azure AD Connect はユーザーのアカウント情報を Azure AD と同期します。ただし、Azure AD は ID 情報を使用して、認証のためにユーザーを AD FS にリダイレクトします。Azure AD ではなく、AD FS が認証を実行します。AD FS はオンプレミスのユーザー アカウントを使用して認証を実行するので、複数のパスワードによりユーザーが混乱することはありません。

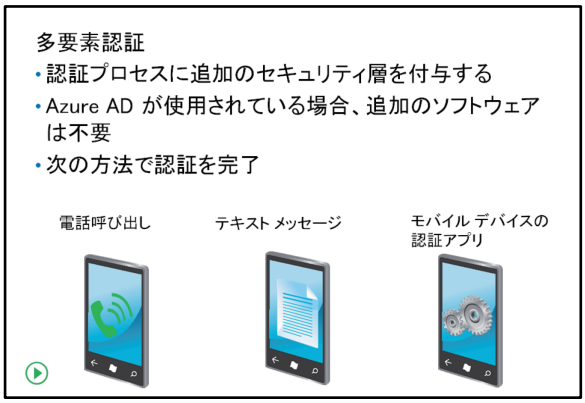
ローカルに展開された AD DS を Azure AD と統合することを選択した場合、次の考慮事項に留意する必要があります。

- パスワード同期を実装すると、同期されるすべてのユーザー アカウントでパスワードが同期されます。パスワード同期が適用されるユーザーの範囲を変更することはできません。
- パスワード同期エージェントは、オンプレミスの AD DS でパスワードが変更された際、パスワード変更の同期をおこないます。パスワード同期エージェントは、2 分ごとに実行されます。サイクル間隔を 2 分にすることで、オンプレミスの AD DS のパスワードと Azure AD のパスワードが一致しない期間を短時間にできます。ユーザーが Azure AD にサインインしているときにパスワードが変更された場合は、ユーザーが次回サインインするまで影響はありません。
- パスワード同期を使用すると、複雑性や有効期限などのパスワード ポリシーは、同じものがクラウドベースのユーザーとオンプレミスのユーザーに適用されます。パスワードはオンプレミスの AD DS でのみ設定され、Azure AD では設定されません。そのため、オンプレミスのパスワード ポリシーのみが適用されます。

- Azure AD では、ユーザー アカウントの同期されたパスワードが期限切れになることはありません。オンプレミスの AD DS でパスワードが期限切れになった場合でも、オンプレミスの AD DS でパスワードが変更されるまで、ユーザーは Azure AD で引き続き既存のパスワードを使用できます。ただし、ユーザーはオンプレミスの AD DS に次回サインインする際、パスワードを変更するように強制されます。

多要素認証とパスワード管理

Azure AD Premium は、多要素認証やセルフサービスのパスワード管理などの ID 管理機能を提供します。AD DS は、Microsoft Forefront Identity Manager などの追加ソフトウェアを実装しない限り、これらの機能をサポートしません。Azure AD Premium では、必要最小限の管理作業とエンドユーザーの操作だけで、これらの機能を有効にして使用できます。



多要素認証

多要素認証により、ユーザー アカウントのセキュリティが高まります。標準認証は、ユーザー名とパスワードに基づいています。認証に第 2 の要素を追加することで、承認されていない者がユーザーの資格情報を使用することがより困難になります。第 2 の要素は、ユーザーが知っているだけではなく所有しているものである必要があります。例えば、スマート カードは認証の第 2 の要素として使用できます。

クラウドベース アプリケーションはどこからでもアクセスできるので、セキュリティを強化することが重要です。未承認のユーザーが別のユーザーのアカウントを使用した場合、クラウドベース アプリケーションにアクセスするために、本来のユーザーのネットワークや物理的な場所にアクセスする必要はありません。さらに、多くのクラウドベース アプリケーションはスマートフォンなどのデバイスからアクセスされ、これらのデバイスはデスクトップ コンピューターよりもセキュリティが低くなります。それは、スマートフォンはデスクトップ コンピューターよりも、紛失または盗難の可能性が高いためです。スマートフォンが盗まれると、そのユーザーの資格情報を使用してクラウドベース アプリケーションにアクセスされる可能性があります。

Azure は、Azure AD のクラウドベース ユーザー アカウントに、多要素認証を追加します。特定のユーザー アカウントまたはすべてのユーザー アカウントに対して、多要素認証を有効にできます。

多要素認証が第 2 の要素として提供するコードは、サインイン プロセスの一環として入力する必要があります。次の方法を使用して、このコードを提供できます。

- 電話呼び出し
- テキスト メッセージ
- モバイル デバイスの認証アプリ

ユーザー アカウントが多要素認証を使用するように構成されると、次のサインイン時にユーザーに対して多要素認証の構成が求められます。この際、ユーザーは電話呼び出しとテキスト メッセージ用の電話番号、または Azure 認証アプリを構成します。Azure 認証アプリは、Windows Phone、iOS、および Android で使用できます。このアプリは、多要素認証メカニズムとしてスマート カードを導入するよりも、展開が容易で、コスト効率が高くなります。

Azure AD で多要素認証を構成するには、Azure ポータルにサインインし、Azure AD インスタンスのダッシュボードを開く必要があります。次に、[構成] タブで、[multi-factor authentication (多要素認証)] セクションを参照します。ここで、多要素認証設定を構成できます。Azure AD では、1 人または複数のユーザーに多要素認証を強制することができます。また、アプリのパスワード (多要素認証をサポートしないアプリケーション用)、信頼できる IP、デバイスの記憶などのサービス設定を構成することもできます。

セルフサービスのパスワード管理

ユーザーがパスワードを忘れた場合、ユーザーがパスワードを再設定できるようにすることで、IT サポート チームのタスクが非常に容易になります。通常の組織で IT サポート チームが受信する通話のほとんどは、ユーザー アカウントとパスワードに関連するものです。AD DS には、ネイティブなセルフサービスのパスワード管理機能はありません。ただし、この機能は Azure AD Premium で利用できます。

ユーザーは、携帯電話、代替メール アドレス、セキュリティの質問などの認証方法を登録できます。これらの代替方法を使用することで、パスワードを忘れた場合、ユーザーは Azure AD でパスワードを再設定できます。例えば、パスワードを再設定するために、ユーザーは 5 つのセキュリティの質問のうち少なくとも 4 つに答える必要がある、と構成できます。

代替方法を使用して実際にパスワードを再設定できるようにするには、この機能をユーザーは事前に登録しておく必要があります。ユーザーはこの登録をするために、http://aka.ms/ssprsetup にアクセスして、Azure AD の資格情報を使用してサインアップすることを選択できます。または、すべてのユーザーに対して、次回のサインインでセルフサービスのパスワード再設定に関する登録を求めることもできます。

最近、Azure AD Premium の新機能として、パスワードを AD DS に書き戻す機能が発表されました。つまり、ユーザーが Azure AD ポータルでパスワードを再設定または変更した場合、パスワードの変更がローカルの AD DS にも書き込まれるようにすることができます。

SaaS アプリケーションの概要

Azure AD Premium は、ローカルの AD DS からのユーザーを認証できることに加えて、さまざまな SaaS アプリケーションに関する追加機能を提供します。Azure AD Premium を使用すると、ユーザーに SaaS アプリケーションへのアクセスを割り当てることができます。つまり、ユーザーは、アプリケーション自体ではなく、Azure AD にサインインするだけで、これらのアプリケーションにアクセスできます。例えば、組織のユーザーが頻繁に LinkedIn サービスを使用する場合、Azure AD Premium インスタンスでこのアプリケーションへの SSO アクセスを有効にした後、この SSO アクセスを Azure AD のユーザーまたはグループに割り当てることができます。Azure AD をローカルの AD DS と同期すると、ユーザーはローカルの AD DS リソース、Azure AD、およびユーザーに割り当てられた各アプリケーションにアクセスする際に、1 セットの資格情報を使用するだけで済むようになります。

この機能を構成するには、Azure ポータルに管理者としてサインインし、アプリケーションを Azure AD に追加します。次のいずれかを選択して実行できます。

- 組織で開発したアプリケーションを追加する。
- ギャラリーからアプリケーションを追加する。

また、ネットワークの外部からアクセス可能なアプリケーションを公開することも選択できます。

ギャラリーから 1 つ以上のアプリケーションを使用することを選択した場合、Azure AD で現在アクセス可能なアプリケーションのリストがポータルに表示されます。2,000 を超えるアプリケーションがギャラリーに存在しています。アプリケーションの選択後、Azure アプリケーション ポータルを使用して、ユーザーまたはグループにアプリケーションへのアクセスを割り当てる必要があります。

また、アプリケーションをユーザーに割り当てる際は、特定のアプリケーション用に資格情報を事前設定するか、またはユーザーが最初にアプリケーションにアクセスする際に、資格情報をユーザーに設定させるかを選択できます。さらに、ユーザーがアプリケーションにアクセスする際に多要素認証の使用を求めるアクセス規則を、各アプリケーションに構成することもできます。

デモンストレーション : SaaS アプリケーションへのアクセス

講師は、次のデモンストレーションをおこないます。

- Azure AD を使用して SaaS アプリケーションにアクセスし構成する

デモンストレーションの手順

1. Azure AD インスタンス (https://manage.windowsazure.com/) を開きます。
2. アプリケーションを参照します。
3. 新しいアプリケーションを Azure AD に追加することを選択します。
4. アプリケーション ギャラリーから、1 つのソーシャル アプリケーションを選択します。
5. そのアプリケーションに対して、SSO が有効であることを確認します。
6. アプリケーションをユーザー アカウントに割り当て、選択したソーシャル アプリケーションに対して資格情報を事前設定します。
7. https://account.activedirectory.windowsazure.com/applications/ を参照し、Azure AD にサインインするだけで、アプリケーションにサインインできることを確認します。

Windows 10 における Azure Active Directory の使用

Windows 10 オペレーティング システムには、Azure AD のサポートが組み込まれています。Windows 8.1 など、Windows オペレーティング システムの以前のバージョンは、ローカルに展開された AD DS のみをサポートしていました。Windows 10 では、Azure AD のいくつかの機能と、Azure AD に依存するサービスを使用できます。

Windows 10 の Azure AD を使用する重要な機能強化としては、次のものがあります。

Windows 10 の Azure AD を使用する重要な機能
- Windows 10 コンピューターは Azure AD に参加できる
- オペレーティング システム状態のローミング
- Azure AD アカウントによる Windows 10 へのサインイン
- MDM ソリューションへの自動登録
- Windows 10 は、クラウドベースの SaaS に対して SSO を使用できる
- Azure AD に参加している Windows 10 デバイスは、オンプレミスのリソースに対して SSO を利用できる
- 新しい Windows ストアは、エンタープライズでの使用をサポートする

- **インストール プロセスの Out-of-Box Experience フェーズから、またはそれ以降に、Windows 10 コンピューターを Azure AD に参加させる機能 :** これによりユーザーは、AD DS の単一セットの資格情報を使用して、どこからでも組織のインフラストラクチャに参加できるようになり、さらに IT 部門が関与することなく、デバイスをユーザー自身で準備できるようになります。また、この機能は、Windows 10 が稼働するタブレットなど、AD DS ドメインにローカルに参加できない最新のフォーム ファクターを備えたデバイスでも動作します。

- **オペレーティング システム状態のローミング：**Windows 10 デバイスが Azure AD に参加することで、ユーザーは、壁紙、タイル構成、Web サイト、Wi-Fi 構成などのオペレーティング システム設定を、Azure AD で使用されるすべてのデバイスで同期することができます。
- **Azure AD アカウントによる Windows 10 へのサインイン：**組織が、Office 365 や Azure AD などのサービスを既に使用している場合、ユーザーはこれらのサービスの資格情報を使用して Windows 10 にサインインできます。
- コンピューターが Azure AD に参加することで、Intune や Microsoft 以外の MDM ソリューションなどのデバイス管理ソリューションに、コンピューターが自動的に登録されます。
- Windows 10 は、認証のために Azure AD を使用するクラウドベースの SaaS アプリケーションに対して、SSO を使用できます。
- Azure AD に参加している Windows 10 デバイスは、組織のネットワークに接続している場合、オンプレミスのリソースに対して SSO を利用できます。Azure AD のアプリケーション プロキシ サービスを使用することで、Azure AD に認証された外部ユーザーは、ローカルに展開されたサービスにアクセスできます。
- Windows 10 の新しい Windows ストアはエンタープライズでの使用をサポートし、Azure AD アカウントを使用したアプリケーションのライセンスをサポートしています。さらに、組織は Windows ストアからボリューム ライセンスされたアプリケーションを購入して、組織内のユーザーに提供できます。

知識の確認

質問	
多要素認証を実装するには、Azure AD のどのエディションが必要ですか。適合するものをすべて選択します。	
正しい解答を選択してください。	
	Basic
	Free
	Premium

レッスン 3
Azure RMS の概要

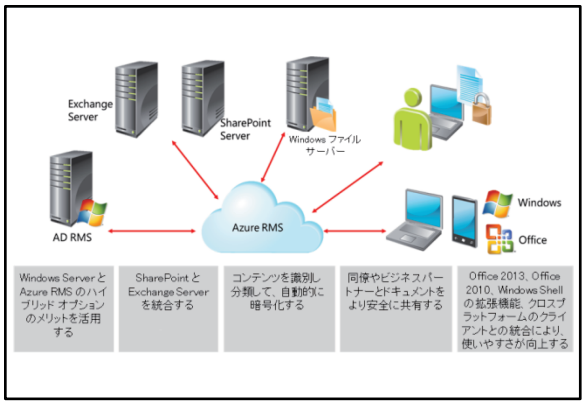
Microsoft は、コンピューターとモバイル デバイスの両方でデータを保護するためのクラウド サービスを、Enterprise Mobility Suite の一部として提供します。Azure RMS は、ローカルとクラウドの両方のリソース用に実装して使用できる、RMS テクノロジのクラウド バージョンです。このレッスンでは、このテクノロジを実装し使用する方法について説明します。

目的

このレッスンにより、次のことを習得できます。

- Azure RMS について説明することができます。
- Azure RMS を実装するプロセスについて説明することができます。
- Azure RMS で RMS テンプレートを使用する方法について説明することができます。
- Azure RMS をサポートするアプリケーションについて説明することができます。
- Microsoft Rights Management コネクタ (RMS コネクタ) が機能するしくみについて説明することができます。

Azure RMS とは



RMS は、データ漏えいの可能性を最小限に抑えるための情報保護テクノロジです。
データ漏えいとは、情報にアクセスしてはならない組織の内部または外部の人物に、承認されずに情報が伝達されることです。RMS は、Windows Server、Exchange Server、SharePoint Server、Office System など、Microsoft の既存の製品やオペレーティング システムに統合されています。

RMS は、転送中および保管されている状態のデータを保護できます。例えば、RMS は、異なる受信者に誤ってメールを送信した場合でも、そのメッセージを開けないようにすることで、メールのドキュメントを保護できます。また、RMS を使用して、リムーバブル USB ドライブなどのデバイスに格納されたデータを保護することもできます。ファイルおよびフォルダーのアクセス許可のデメリットは、ファイルを別の場所にコピーすると、元のアクセス許可が適用されなくなることです。USB ドライブにコピーされたファイルは、コピー先のデバイスのアクセス許可を引き継ぎます。コピー後は、読み取り専用だったファイルが、ファイルおよびフォルダーのアクセス許可の変更により、編集される可能性があります。

RMS を使用すると、ファイルおよびフォルダーのアクセス許可に関係なく、ファイルをあらゆる場所で保護できます。また、ファイルを開くことを承認されているユーザーのみが、そのファイルのコンテンツを表示できます。

単一 AD DS フォレスト内のローカル ネットワーク インフラストラクチャでは、AD RMS を実装することで情報の保護能力を大幅に向上できます。ただし、AD RMS で保護されたコンテンツを、組織外の人物と共有するシナリオでは、保護が利用できない可能性があります。信頼の確立、または Microsoft アカウントの使用に加えて、Azure パブリック クラウド サービスを使用して、その著作権管理機能を活用できるようになりました。

Azure RMS により、ローカルの AD RMS インフラストラクチャを実装することなく、クラウドから RMS 保護を使用できるようになります。また、Azure RMS を使用することで、ポリシーと使用制約をドキュメントに割り当てて、これらのドキュメントを、Azure サービスをサブスクライブする別の組織と共有することもできます。Azure RMS は Office 365 のすべてのサービスおよびアプリと統合されているので、クラウドとオンプレミスの両方の環境から RMS のすべての機能を使用できます。

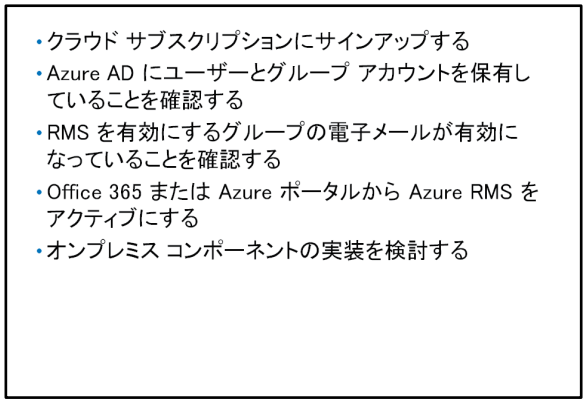
Azure RMS は、Office 365 Enterprise E3 および Microsoft Office 365 ProPlus のサブスクリプションで、または Enterprise Mobility Suite の一部として使用できます。また、独立したサービスとして購入することもできます。

Azure RMS には次の機能があります。

- **Microsoft Office と Information Rights Management (IRM) の統合 :** ローカルに展開された Microsoft Office のすべてのアプリは、Azure RMS を使用してコンテンツを保護できます。
- **Microsoft Exchange Online と IRM の統合 :** Azure RMS により、Microsoft Outlook Web App でメールメッセージを保護して利用できるようになります。また、Windows Phone 8 や iOS ベース デバイスなどの IRM をサポートするデバイスで、Exchange ActiveSync を通じて IRM 保護されたメッセージを利用することもできます。さらに、管理者は、保護と暗号化解除のために Outlook ルールと Exchange トランスポート ルールを使用して、コンテンツが組織外に不用意に漏えいしないようにすることができます。
- **Microsoft SharePoint Online と IRM の統合 :** Azure RMS を使用すると、管理者は SharePoint ライブラリのドキュメントに対して、自動的な IRM 保護を構成できます。
- **Windows ベース ファイル サーバーとの統合 :** RMS コネクタを介して、ファイル分類インフラストラクチャ (FCI) による自動的な保護をおこないます。

Azure RMS を実装するプロセス

Azure RMS の実装は、ローカルの AD RMS サービスを実装するよりも非常に簡単です。オンプレミスでの構成は、ほとんど必要ないか、またはまったく必要ありません。クラウドのサブスクリプションにサインアップし、Office 365 または Azure AD のテナントのアカウントを取得すると、RMS を有効にする準備が整います。



注 : 既定では、Office 365 または Azure AD のアカウントにサインアップした際、Rights Management は無効になっています。

組織の Azure RMS を有効にする前に、Azure AD にユーザー アカウントとグループ アカウントを保有していることを確認する必要があります。ほとんどの場合、これらのアカウントはローカルの AD DS と同期されます。さらに、Azure RMS を有効にするグループの電子メールが有効になっていることを確認する必要があります。

Azure RMS をアクティブにするには、次の手順を実行します。

1. Office 365 管理ダッシュボードで、[サービス設定] を展開し、[アクセス権管理] をクリックします。
2. [管理を行う]、[アクティブ化] の順にクリックします。

Office 365 を使用していないが、Azure RMS サブスクリプションを保有している場合、Azure ポータルを使用して Azure RMS をアクティブにできます。Azure ポータルで [Active Directory] を参照し、[Rights Management] をクリックして、[アクティブ化] を選択します。

Azure RMS をアクティブにした後で、オンプレミスのコンポーネントとアプリケーション構成の実装を検討する必要があります。さらに、Azure RMS を使用している場合、独自のカスタム RMS テンプレートの作成を検討することもできます。

オンプレミス側で、Azure RMS コネクタを実装して、Exchange、SharePoint、ファイル サーバーの役割サービスなどのオンプレミス サービスを有効にし、Azure RMS 機能を活用することを検討する必要があります。

RMS テンプレートの使用

RMS テンプレートを使用して、標準の RMS ポリシーを組織全体に構成することができます。例えば、表示のみのユーザー権利の割り当て、編集、保存、および印刷の各機能のブロック、または Exchange Server と連携する場合にメッセージの転送または返信の機能のブロックをおこなう、標準的なテンプレートを構成できます。

- Azure RMS で使用可能な 2 つの事前定義されたテンプレート
  - 保護されたコンテンツの読み取り専用
  - 保護されたコンテンツの読み取りと変更
- Azure ポータルを使用して、カスタム テンプレートを作成する
- カスタム テンプレートには、ユーザーの権利、スコープ、追加のオプションを構成できる
- テンプレートを使用する前に、発行する必要がある

次の 2 つのテンプレートは、Azure RMS と Office 365 RMS に既定で構成されます。

- 保護されたコンテンツの読み取り専用
  - **表示名 :** <組織名> - 社外秘 (閲覧のみ)
  - **特定の権限 :** コンテンツの表示
- 保護されたコンテンツの読み取りと変更
  - **表示名 :** <組織名> - 社外秘
  - **特定の権限 :** コンテンツの表示、ファイルの保存、コンテンツの編集、割り当てられた権限の表示、マクロの許可、転送、返信、全員に返信

ドキュメントの作成者は、既存のテンプレートを適用してコンテンツを保護することを選択できます。これをおこなうには、RMS 対応のアプリを使用します。例えば、Microsoft Word 2013 では、文書の保護機能を使用することにより、テンプレートを適用します。この機能を使用すると、Word 2013 は Azure RMS にクエリを発行して、RMS サーバーの場所を特定します。RMS サーバーの場所が特定されると、利用可能なテンプレートを使用したり、ドキュメントのカスタム アクセス許可を構成したりできます。

事前定義されたテンプレートを使用しない場合は、Azure ポータルを使用してカスタム テンプレートを作成できます。既存のテンプレートの管理、または新しいテンプレートの作成をおこなうには、Azure ポータルで Active Directory インスタンスを参照し、[Rights Management] をクリックします。

新しい Azure RMS テンプレートを作成する際は、最初にテンプレートの言語を選択して、テンプレートの名前と説明を入力する必要があります。次に、リストからテンプレートを選択し、そのダッシュボードを開きます。ここで、テンプレートで保護されるドキュメントに既定されるユーザー権利を構成できます。また、このテンプレートを適用できるユーザーまたはグループを指定して、テンプレートの範囲を定義することもできます。テンプレート ダッシュボードの [構成] タブで、コンテンツ有効期限やテンプレートのオフライン アクセスなどの設定を構成できます。

Azure RMS で構成できる RMS テンプレートは、次のユーザー権利をサポートします。

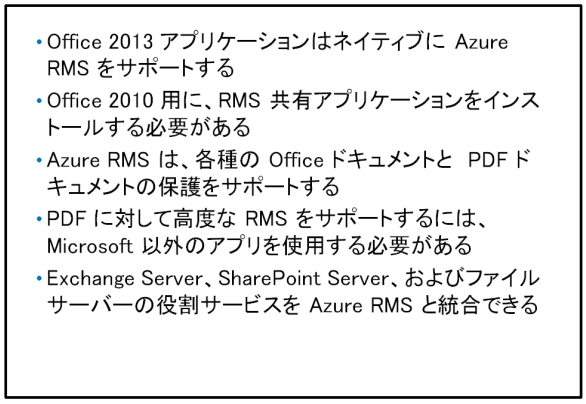
- **フル コントロール :** RMS で保護されたドキュメントに対するフル コントロールをユーザーに付与します。
- **コンテンツの表示 :** RMS で保護されたドキュメントの表示をユーザーに許可します。
- **コンテンツの編集 :** RMS で保護されたドキュメントの変更をユーザーに許可します。
- **ファイルの保存 :** RMS で保護されたドキュメントの保存機能をユーザーに許可します。
- **コンテンツのエクスポート (名前を付けて保存) :** RMS で保護されたドキュメントに名前を付けて保存する機能の使用をユーザーに許可します。
- **印刷 :** RMS で保護されたドキュメントの印刷を許可します。
- **転送 :** Exchange Server と連携して使用されます。RMS で保護されたメッセージの受信者に、そのメッセージの転送を許可します。
- **返信 :** Exchange Server と連携して使用されます。RMS で保護されたメッセージの受信者に、そのメッセージの返信を許可します。
- **全員に返信 :** Exchange Server と連携して使用されます。RMS で保護されたメッセージの受信者に、全員に返信する機能を使用してそのメッセージに返信することを許可します。
- **コンテンツのコピーと抽出 :** ファイルからデータをコピーすることを、ユーザーに許可します。この権利が割り当てられない場合、ユーザーはファイルからデータをコピーできません。
- **マクロの許可 :** マクロの使用をユーザーに許可します。
- **割り当てられた権利の表示 :** 割り当てられたユーザー権利の表示をユーザーに許可します。
- **権利の変更 :** 割り当てられたユーザー権利を変更することを、ユーザーに許可します。

ユーザー権利は割り当てのみが可能であり、拒否を明示的に指定することはできません。例えば、ユーザーがドキュメントを印刷できないようするには、ドキュメントに関連するテンプレートに印刷のユーザー権利を含めないようにします。

カスタム テンプレートを構成した後は、RMS 対応のアプリケーションでそのテンプレートにアクセスできるように、テンプレートを公開する必要があります。

Azure RMS をサポートするアプリケーション

Azure RMS と AD RMS は、すべての種類のドキュメントまたはファイルに対して使用できるわけではありません。RMS 保護を使用できるようにするには、RMS 対応のアプリケーションとサポート対象のファイルの種類が必要になります。ほとんどの場合、RMS 保護は、Word と Excel のドキュメントやメール メッセージなどの Office ファイルに適用されます。そのため、RMS を実装する前に、ユーザーが RMS で保護するファイルの種類を調べ、RMS 保護がこれらのファイルの種類をサポートすることを確認する必要があります。



Office 2013 以降のアプリケーションは、ネイティブに RMS をサポートするので、これらのアプリケーションのユーザーは RMS を使用するために構成をおこなう必要はありません。ユーザーが必要なことは、RMS が構成された Azure AD の資格情報を使用して、アプリケーションにサインインするだけです。

Office 2010 で Azure RMS を使用する場合は、Windows 用の RMS 共有アプリケーションをインストールする必要があります。

RMS 共有アプリケーションは、Office アプリケーションと Windows オペレーティング システム向けの無料のアドインです。このアドインは、Azure RMS を使用する Office 2010 のクライアントで必要になるので、Azure RMS をサポートするすべてのコンピューターとモバイル デバイスに実装することをお勧めします。

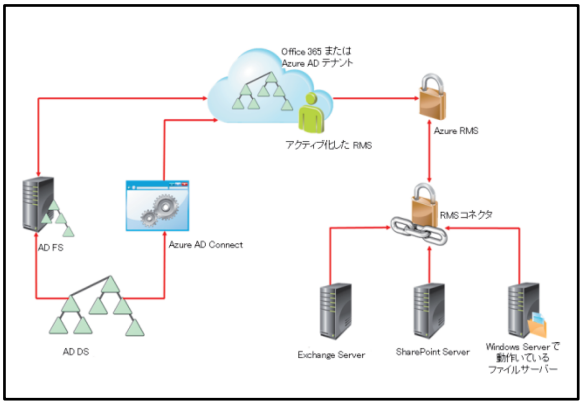
このアプリケーションは、Office アプリケーションと統合されます。ユーザーが、Office アプリケーションのリボンから直接ファイルとメールを保護できるように、Office のアドインとして提供されます。また、Azure RMS がネイティブにサポートしていないファイルの種類に対しても汎用的な保護をおこない、ユーザーが保護しているファイルを追跡したり失効させたりするための、ドキュメント追跡サイトを提供します。

Azure RMS は、PDF ファイルの保護も限定的にサポートします。PDF ファイルを保護するには、RMS 共有アプリを使用するか、Azure RMS で Azure RMS テンプレートにアクセスできる、サポート対象の Microsoft 以外の PDF ビューアーまたはエディターを使用する必要があります。Office アプリケーションとは異なり、Microsoft PDF ビューアーから直接 Azure RMS テンプレートにアクセスすることはできません。

また、一部のサーバー アプリケーションに Azure RMS のサポートを構成することもできます。Azure RMS は、Exchange Server (オンプレミスと Exchange Online の両方)、SharePoint (オンプレミスと SharePoint Online の両方)、および FCI と統合できます。この統合は、Azure RMS コネクタを実装することで実現できます。

参考資料 : Azure RMS の要件については、次のサイトを参照してください。
Azure Rights Management の要件
https://technet.microsoft.com/ja-jp/library/dn655136.aspx

RMS コネクタの概要



オンプレミスのサーバーを Azure RMS に接続して、このクラウド サービスをローカルで使用できるようにするには、最初にこれらのリソースを接続する必要があります。

RMS コネクタにより、オンプレミスのサーバーを Azure RMS に接続できます。このコネクタにより、既存のサーバーが Azure RMS の機能を使用できるようになります。つまり、RMS コネクタ以外の RMS コンポーネントをローカルにインストールすることなく、Azure RMS を使用してローカル リソースを保護できます。さらに、ローカル リソースで Azure RMS を使用することにより、リソースの共有が容易になり、リソースをクラウドとローカルの両方に展開するハイブリッド シナリオがサポートされます。

RMS コネクタは小さいサイズのソフトウェアで、ローカル ネットワーク上でサービスとして稼働します。Windows Server 2012 R2、Windows Server 2012、または Windows Server 2008 R2 にインストールする必要があります。Microsoft は、Azure RMS を使用するサーバーへのコネクタのインストールをサポートしていません。Azure RMS コネクタは、サーバーに、ローカルに展開された仮想マシンに、または Azure 仮想マシンに、安全にインストールできます。コネクタを構成するには、Azure AD の管理資格情報が必要になります。Azure RMS を使用するサーバーのコンピューター アカウントを、コネクタの構成に手動で追加する必要があります。コネクタが稼働すると、ローカル サーバーと Azure RMS の間で、通信エージェントとして機能します。

このコースの作成時点では、RMS コネクタは、ローカルに展開された Exchange Server、SharePoint Server、およびファイル サーバーをサポートしています。これらの各サービスから、Azure RMS テンプレートに直接アクセスし、それらを特定のリソースで使用できます。

例えば、ファイル分類のルールとタスクをローカルのファイル サーバーに実装し、ドキュメント内で検出された分類値に基づいて、Azure RMS テンプレートを使用してドキュメントを自動的に保護することができます。また、管理者から社内スタッフに送信されるすべてのメッセージに、RMS テンプレートの「転送不可」を自動的に実装することもできます。

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
Azure RMS は、Windows Server 2012 R2 にローカル サービスとして展開できます。	

レッスン 4
Intune の概要

Intune はスタンドアロンのクラウド サービスであり、コンピューター、ノート PC、タブレット、およびその他すべてのモバイル デバイスを管理するのに役立ちます。Azure AD をディレクトリ ストアとして使用し、ローカルの管理インフラストラクチャと統合できます。このレッスンでは、Intune を使用するメリット、およびいくつかの重要な機能について説明します。

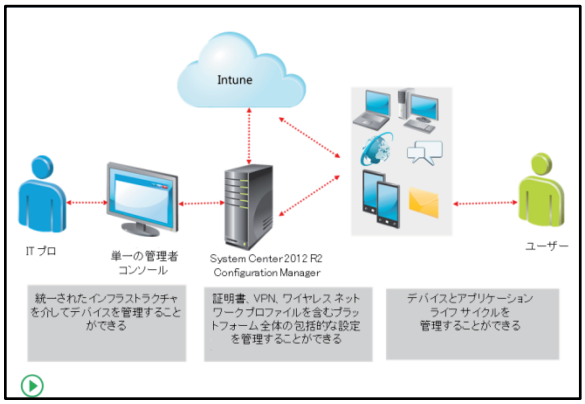
目的

このレッスンにより、次のことを習得できます。

- Intune の重要なメリットについて説明することができます。
- Intune を実装するためのオプションについて説明することができます。
- Intune クラウド サービスにサインアップする方法を説明することができます。
- Intune ポータルの使用について説明することができます。

Intune を使用するメリット

Intune は、Microsoft のクラウド プラットフォーム製品です。Intune を使用することで、Windows ベースのコンピューターと、Mac iOS、Android、Windows RT、および Windows Phone を搭載したモバイル デバイスを管理できます。Intune は、スタンドアロン、またはクラウド専用モードで実装するか、オンプレミスの System Center 2012 R2 Configuration Manager ソリューションと統合できます。



Intune はクラウド専用サービスとして、BYOD シナリオでデバイスを管理できます。デバイス管理には、次の領域が含まれます。

- **ポリシー設定 :** Intune ポリシーの作成を支援するために、複数のポリシー テンプレートを使用できます。
- **アプリケーション展開とソフトウェア更新 :** Intune により、アプリを Windows モバイル デバイスにサイドロードしたり、アプリケーションを別のデバイスに展開したり、ストア アプリへのリンクを直接展開したりできします。
- **インベントリとレポート :** Intune に登録されたデバイスに関する情報を表示できます。
- **リモート ワイプ、リモート ロック、およびパスコードのリセット :** Intune は、紛失または盗難にあったデバイスのデータを未承認のユーザーが表示することを防ぎます。

また、Intune は、Windows オペレーティング システムを搭載したデバイス向けのアプリケーション ポータルを提供します。このポータルには、Windows 10、Windows 8.x、および Windows RT の各デバイス向けの Intune ポータル サイト アプリを通じてアクセスできます。Windows Phone 向けの Intune ポータル サイトを使用して、Intune ポータル サイトと Configuration Manager ポータル サイトにアクセスできます。

Intune を System Center 2012 R2 Configuration Manager と統合することで、次のことが可能になります。

- コンピューターおよびデバイスがドメイン メンバーかどうかにかかわらず、単一の管理エクスペリエンスを維持する。

- 登録されたモバイル デバイスを、Intune および System Center 2012 R2 を使用して管理する。

Configuration Manager と Intune を一緒に使用すると、次の領域のデバイス管理が可能になります。

- **アプリケーション展開とソフトウェア更新 :** Windows ストア、Windows Phone ストア、アプリ ストア、または Google Play を通じて、アプリを展開できます。
- **インベントリとレポート :** 組み込みのレポートを通じて、収集されたインベントリに関する情報を表示できます。
- **リモート ワイプ、リモート ロック、およびパスコードのリセット :** Intune は、紛失または盗難にあったデバイスのデータを未承認のユーザーが表示するのを防ぐのに役立ちます。

モバイル デバイスは Intune サービスに接続しますが、管理タスクは Configuration Manager コンソールで実行されます。管理タスクによる設定は、Intune Connector サイト システムの役割を通じて、Intune に接続されたデバイスに適用されます。ただし、Intune コネクタは、ドメイン メンバーではない Intune の管理対象コンピューターを、Configuration Manager コンソールに表示することを許可しません。これらのコンピューターに関する情報を表示するには、Intune 管理コンソールを使用します。

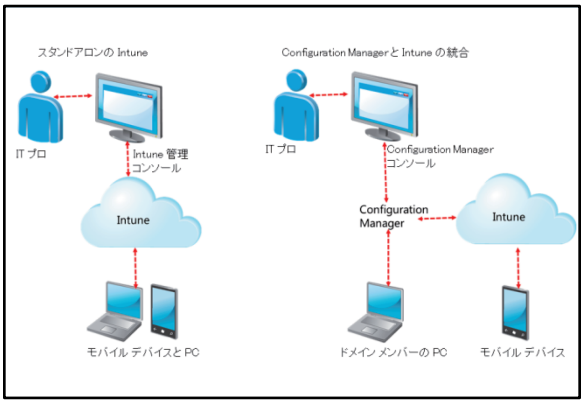
Intune と Exchange ActiveSync および Office 365 との比較

次の機能は Intune では使用できますが、Exchange ActiveSync および MDM for Office 365 では使用できません。

- セルフサービス ポータル サイトを使用して、ユーザーがデバイスを登録し、組織のアプリをインストールする。
- 証明書、仮想プライベート ネットワーク (VPN) プロファイル (アプリ固有のプロファイルを含む)、および Wi-Fi プロファイルを展開する。
- 組織用アプリから個人用アプリへの切り取り/コピー/貼り付け/名前を付けて保存を禁止する (モバイル アプリケーション管理)。
- 管理対象のブラウザー、PDF ビューアー、スキャナー ビューアー、および Intune 向けオーディオ/ビデオ プレーヤー アプリを使用することにより、コンテンツの表示をセキュリティで保護する。
- セルフサービス ポータル サイト、および Intune 管理コンソールを使用して、リモートでデバイスをロックする。
- PC の管理 (インベントリ、マルウェア対策、パッチ、ポリシーなど)
- Configuration Manager との統合による PC およびモバイル デバイス向けの単一の管理コンソール

Intune を実装するためのオプション

既定では、Intune はスタンドアロンのクラウド サービスとして展開されます。認証のために Azure AD を使用するので、Intune は間接的にローカルの AD DS とも統合されています。したがって、ユーザーとユーザーが使用するデバイスを管理できます。Intune は特に、ドメイン メンバーではないデバイス、携帯電話、または Azure AD に参加している Windows 10 デバイスなど、グループ ポリシーの管理スコープを超えたデバイスに対して役立ちます。Intune がスタンドアロンのクラウド サービスとして展開される場合、オンプレミス側で最小限の操作が必要になります。



なお、System Center 2012 R2 Configuration Manager を Intune および Azure と統合することを選択することもできます。Configuration Manager を Intune と統合することで、広範な MDM 機能が有効になります。また、Configuration Manager を Azure と統合することで、クラウドベースの配布ポイントが有効になります。Azure ベースの配布ポイントを使用するメリットの 1 つは、Azure に組み込まれた冗長性のメリットをフル活用できることです。Azure ベースの配布ポイントを作成し構成する際は、クライアントのトラフィックをセキュリティで保護するために Secure Sockets Layer (SSL) を使用します。

クラウドベースの配布ポイントの機能は、次のとおりです。

- イントラネットベースとインターネットベースの両方のクライアントをサポートする。
- コンテンツをフォールバックする場所として機能できる。
- クライアントを適切に構成することで、BranchCache の使用をサポートできる。
- 個別に管理することも、配布ポイント グループのメンバーとして管理することもできる。
- さらなる配布ポイントを割り当てることなく、組織の現在のニーズを満たすためにクラウド サービスを拡張するオプションを提供する。

クラウドベースの配布ポイントを展開することを選択した場合、次の制限に留意する必要もあります。

- Preboot Execution Environment (PXE) またはマルチキャスト対応の展開はサポートされない。
- ソフトウェア更新プログラム パッケージをホストすることはできない。
- 配布ポイントから実行するパッケージはサポートされない。クライアントはコンテンツをダウンロードし、ローカルに実行する必要がある。
- Microsoft Application Virtualization (App-V) アプリケーションのストリーミングはサポートされない。
- 事前設定されたコンテンツはサポートされない。
- [実行中のタスク シーケンスで必要になったときに、ローカルでコンテンツをダウンロードする] 展開オプションを使用するタスク シーケンスで、コンテンツの場所として使用できない。
- [タスク シーケンスを開始する前にすべてのコンテンツをローカルにダウンロードする] 展開オプションを使用するタスク シーケンスは、使用できる。
- プル配布ポイントとしては構成できない。

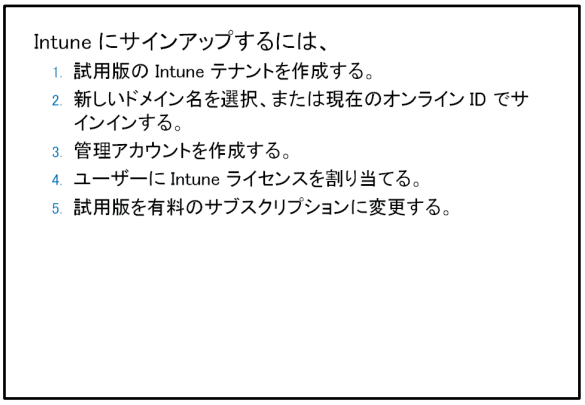
セキュリティに関しては、他のインターネット トラフィックと同様に、SSL を使用してクライアントのトラフィックを保護します。ただし、証明書の要件は、サポートされるクライアントのオペレーティング システムに応じて異なります。Intune コネクタ サイト システムの役割を使用して、管理タスクを実行できます。この役割には、Configuration Manager コンソールを通じてアクセスできます。Intune コネクタ サイト システムの役割は、中央管理サイトまたはスタンドアロンのプライマリ サイトにのみインストールできます。

Intune コネクタ サイト システムの役割を使用して Intune を構成すると、さまざまなデバイス クラスに対して、次の機能がサポートされます。

管理タスク	Windows RT、Windows 8.1、Windows 10	Windows Phone 8、Windows Mobile 10	iOS	Android
インベントリからの削除、ワイプ、リモート ワイプ、削除、およびデバイス ブロック	はい	はい	はい	はい
パスワード設定用のコンプライアンス設定、メール管理、暗号化、ワイヤレス通信、ローミング、およびセキュリティ	はい	はい	はい	はい

管理タスク	Windows RT、Windows 8.1、Windows 10	Windows Phone 8、Windows Mobile 10	iOS	Android
デバイス ストアからのアプリのインストール	はい	はい	はい	はい
ハードウェア インベントリ	はい	はい	はい	はい
基幹業務アプリの管理	はい	はい	はい	はい

Intune クラウド サービスへのサインアップ



Intune は、Enterprise Mobility Suite の一部として、またはスタンドアロンのクラウド サービスとして使用できます。どちらのライセンス モデルを選択しても、最初に試用版で Intune テナントを作成する必要があります。そのためには、Intune 製品ホーム ページに移動して、[無料で試す] をクリックする必要があります。これにより、サインアップ ページが開き、試用版の Intune テナントを作成するためのデータを入力できます。試用版のテナントは、30 日間の 100 ユーザー ライセンスを提供するので、実際にライセンスの購入を決定する前に、サービスを試用できます。試用版の Intune テナントは本番バージョンに容易に変換できるので、試用版のサインアップ時には、適切なデータを入力するようにします。

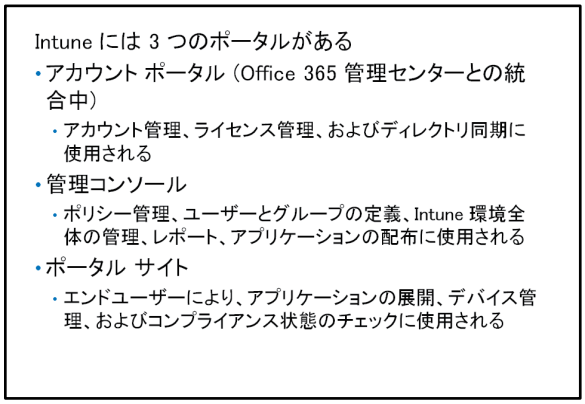
重要なことは、既に Office 365 または Azure AD のサブスクリプションを保有している場合、新しいデータを使用して試用版の Intune テナントを作成しないことです。つまり、Office 365 または Azure AD の Microsoft オンライン ID を使用してサインインし、試用版の Intune サブスクリプションを作成します。このサブスクリプションは Azure AD の現在のインスタンスに関連付けられるので、Intune ライセンスを現在のユーザーに割り当てることができます。

試用版テナントの作成時、登録済みの Azure AD ドメインをまだ保有していない場合は、既定のテナント ドメイン名を選択する必要があります。この名前には常に onmicrosoft.com というサフィックスが付いており、独自のドメインを追加するまで、既定のドメイン名になります。この既定のドメイン名を作成する際は、テナント管理者のユーザー ID とパスワードも入力する必要があります。この管理者は全体管理者であるため、この資格情報を安全に保持する必要があります。

テナントを作成すると、Intune 管理ダッシュボードが開きます。Intune サブスクリプションを既存の Azure AD と関連付けている場合、Intune ライセンスをユーザーに割り当てることができます。関連付けていない場合は、Intune 管理コンソールから新しいクラウド専用ユーザーを作成できます。

Intune ポータルの概要

Intune には、管理用に次の 3 つの異なるポータルがあります。



- **アカウント ポータル :** Intune サブスクリプションを作成した後ですぐにアクセスできる既定のポータルです。https://account.manage.microsoft.com/ からアクセスできます。このポータルで、ユーザーの管理、ディレクトリ同期の構成、およびグループとドメインのセットアップを実行できます。また、このポータルで、ライセンスと Intune サブスクリプションを管理することもできます。さらに、Intune のサービス正常性の監視に加えて、管理者の委任、およびサポートの検索も実行できます。一般的に、Intune の構成が完了した後で、このポータルに頻繁にアクセスすることはありません。

注 : このコースの作成時点では、このポータルは運用されています。しかし、Microsoft では、Intune アカウント ポータルと Office 365 管理センターの統合を進めています。これが完了すると、すべてのユーザーを Office 365 管理センターで管理することになります。

- **管理コンソール :** クライアント ユーザーとデバイスを管理するためのメイン ポータルです。https://manage.microsoft.com/ からアクセスできます。このポータルで、Intune 環境全体を管理します。このポータルを使用して、ユーザーとデバイスのグループの定義 (Intune では、これらは Azure AD のグループではありません)、アラートの構成、および Intune テナントの全体的な状態の確認をおこないます。さらに、Intune を使用して管理するすべてのデバイスに対して、ポリシーの構成、展開、およびアプリケーションの配布をおこないます。また、このポータルには、さまざまなインベントリ レポートを生成できるレポート セクションがあります。ナビゲーション ウィンドウの最後には管理者領域があり、Exchange Online、Apple Push Notification サービス、多要素認証など、他のサービスと Intune との統合を構成できます。
- **ポータル サイト :** Web アプリケーションとして、およびデスクトップとモバイル デバイスのアプリケーションとして、すべてのプラットフォームで使用できます。エンド ユーザーは、ほとんどこのポータルを使用します。https://portal.manage.microsoft.com/ からアクセスするか、または Windows、iOS、または Android の各デバイスにポータル サイト アプリをインストールすることでアクセスできます。ユーザーは、ポータル サイト アプリを使用して Intune にデバイスを登録し、組織がポータル サイトから公開したアプリケーションをインストールします。さらに、ユーザーはこのポータルにアクセスして、登録されたデバイスの表示、コンプライアンス状態のチェック、および新しいデバイスの追加や古いデバイスの削除をおこなうことができます。

演習 : Microsoft Intune サブスクリプションの実装

シナリオ

あなたは、デスクトップとモバイルの管理について、Intune を評価することに決めました。まず、試用版サブスクリプションにサインアップする必要があります。次に、Intune にユーザーを追加し、ユーザーがポータル サイトにアクセスできるかどうかを確認することができます。

目的

この演習により、次のことを習得できます。

- Intune 評価版サブスクリプションにサインアップすることができます。
- Intune ユーザーを追加することができます。

演習のセットアップ

予定所要時間 : 40 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 MSL-TMG1
ユーザー名	Adatum¥Administrator
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 : Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Aidan」、パスワード「Pa$$w0rd」を使用してサインインします。
6. インターネットにアクセスするために、MSL-TMG1 も起動する必要があります。

練習 1 : Intune 試用版サブスクリプションへのサインアップ

シナリオ

Intune サービスを評価するために、試用版にサインアップする必要があります。

主な作業は次のとおりです。

1. 新しいサブスクリプションへサインアップする
2. ポータルを確認する
3. Enterprise Mobility Suite の評価版を起動する

▶ 作業 1 : 新しいサブスクリプションへサインアップする

1. LON-CL1 で、[検索] ボックスに「iexplore」と入力します。[Internet Explorer] を右クリックし、[タスク バーにピン留めする] をクリックします。
2. LON-CL1 で、タスク バーの [Internet Explorer] を開き、https://www.microsoft.com/ja-jp/server-cloud/products-Microsoft-Intune.aspx に移動して、[無料で試す] をクリックします。
3. 第 5 章で Office 365 評価版サブスクリプション用に作成した資格情報を使用して、Intune 試用版ライセンスの認証をおこないます。

▶ 作業 2 : ポータルを確認する

1. Office 365 管理センターで、ユーザーとライセンスを参照します。
2. [管理者] セクションから、[Intune] を開きます。Intune 管理コンソールで、使用可能なオプションを参照します。

▶ 作業 3 : Enterprise Mobility Suite の評価版を起動する

1. https://www.microsoft.com/en-us/server-cloud/enterprise-mobility/ems-trial.aspx を参照して、Enterprise Mobility Suite の評価版を起動します。

結果 : この練習により、Intune 評価版サブスクリプションにサインアップすることができました。

練習 2 : Intune ユーザーの追加

シナリオ

Intune 試用版の起動後、Intune サービスにユーザーを追加します。

主な作業は次のとおりです。

1. Intune ユーザーを追加する
2. ユーザーがポータル サイトにアクセスできることを確認する

▶ 作業 1 : Intune ユーザーを追加する

1. Office 365 管理センターのダッシュボードで、新しいユーザーを作成します。
2. 「Test User」という名前を付けます。
3. そのユーザーに Office 365、Intune、および Enterprise Mobility Suite のライセンスを割り当てます。
4. 次の情報を使用して、さらに 2 名のユーザーを作成します。
   - Don Funk
   - Allie Bellew
5. ブラウザーを閉じます。

注 : 作成した各ユーザーのユーザー名とパスワードを書き留めます。また、以降の章でこれらのアカウントが使用できるように、あなたの有効な電子メール アドレスに作成の結果を送信することもできます。

▶ 作業 2 : ユーザーがポータル サイトにアクセスできることを確認する

1. LON-CL1 で Internet Explorer を開き、http://portal.manage.microsoft.com を参照します。
2. ユーザー ID「testuser@<ドメイン サフィックス>」と前の作業で書き留めた一時パスワードを使用して、サインインします。
3. 表示されるメッセージに従って、パスワードを変更します。新しいパスワードとして、「Pa$$w0rd!」と入力します。
4. ポータル サイトが開くことを確認します。

注 : [このデバイスは登録されていません] というメッセージが表示されます。

5. 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、ユーザーを Intune に追加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. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。

復習とまとめ

ベスト プラクティス

- Enterprise Mobility Suite に含まれる 2 つ以上の製品が必要な場合は、個別の製品の購入ではなく、Enterprise Mobility Suite の購入を検討します。
- 組織の AD DS と Azure AD を同期して、SSO を実現します。
- RMS 共有アプリをコンピューターとモバイル デバイスに実装して、追加の機能を実現します。
- セルフサービスのパスワード管理を実装します。
- 多要素認証を使用して、組織の AD DS 内のセキュリティ上で極めて重要なアカウントを保護します。

一般的な問題とトラブルシューティングのヒント

一般的な問題	トラブルシューティングのヒント
PDF ドキュメントに対してカスタムの RMS アクセス許可を設定できない。	

復習問題

質問 : Enterprise Mobility Suite を購入することの主な利点は何ですか。

質問 : クラウドベースおよびオンプレミスのアプリケーションの両方で SSO をおこなえるようにする必要がある場合、まず何をする必要がありますか。