!nventit

Windows 8.1向けMobiConnect Active Directory併用時のガイドライン

2015年7月3日

インヴェンティット株式会社

"Don't worry about what anybody else is going to do...
The best way to predict the future is ***to invent it****."*

本資料には関係者外秘内容が含まれております。
本資料のお取扱いには十分ご注意ください。
本資料は複写厳禁とさせていただきます。

はじめに

本資料は、Windows 8.1版MobiConnectエージェントアプリケーション（以下「エージェントアプリ」）をActive Directoryにてドメイン参加した端末上で利用する際の注意事項をまとめた資料となります。

本資料内に記載された情報は、弊社において動作確認を行なった結果をもとにまとめた内容となるため、ユーザー様の環境下において、本資料に記載された動作や結果と異なる場合があります。また、本資料の内容について、マイクロソフト社にその内容の妥当性について確証を得たものではありません。

本資料は、エージェントアプリとActive Directoryを併用するにあたり、予め注意点や想定される挙動をご理解いただき、ユーザー様における導入ならびに運用をよりスムーズに実施していただくことを目的としております。

また、本資料はドメイン参加が可能（Active Directoryの利用が可能）で、且つOpen MDM方式の利用が可能なWindows 8.1 Proを対象としています。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.　Confidential

前提条件

本資料の前提条件は以下になります。

【前提条件】
・対象端末は、Active Directoryによるドメイン参加が可能であり、且つ、Open MDM方式の登録が可能なWindows 8.1 Pro以上のOSを搭載した端末となります。
・本資料における動作確認は、端末がドメイン参加しており、Active Directoryユーザーが端末に設定されている状態で、且つActive Directoryによるポリシーが一切適用されていない状態において実施しております。*1

*1：Active Directoryのポリシーを提供した状態でのご利用につきましては、適用されたいポリシーを設定した上で、ユーザー様自身にて、本導入前に予め動作に問題ないかご確認をお願いします

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

Windows 8.1端末に設定できるアカウントについて

Windows 8.1端末に設定できるアカウントは主に以下の3種類となります。

アカウントの種類	説明
Microsoftアカウント	Microsoft社が提供するさまざまなサービスが利用可能なアカウント。Windowsストアアプリを利用する場合には必要です。また、複数の端末で同じMicrosoftアカウントを利用すると、お気に入り等、個人設定がオンラインで同期され、どの端末からでも同じ設定を利用することが可能。
ローカルアカウント	端末毎に設定する必要があります。ローカルアカウントで作成した個人設定は同期されないため、他の端末を利用する場合は、新たに個人設定が必要となります。
ADアカウント	Active Directoryに登録されているアカウントになります。ドメイン参加した端末からADアカウントを利用して端末にサインインします。Active Directoryで適用可能な設定やポリシーを端末に登録されているアカウントに対して適用可能です。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

Microsoftアカウントとの関連付けについて（１）

「ローカルアカウント」および「ADアカウント」はMicrosoftアカウントに関連付けることが可能です。各アカウントにおいてMicrosoftアカウントを関連付けた場合の違いについて下記に記します。

アカウント種別	関連付け後のサインアウト	アカウント名		関連付け後のユーザーフォルダ名*1	関連付け解除後のアカウント再設定
		関連付け前	関連付け後		
ローカルアカウント	強制的にサインアウト	ローカルアカウント名	関連付けたMSアカウント名	関連付け前と同じフォルダ名	必要*2
ADアカウント	なし	ADアカウント名	ADアカウント名	関連付け前と同じフォルダ名	不要

*1：ユーザーフォルダー名はどのアカウントの場合でも、関連付け前、関連付け後、関連付け解除後で、変わることはありません。

*2：解除後のアカウント名およびパスワードを再設定する必要があります。関連付け前と同じ設定も可能です。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.　Confidential

Microsoftアカウントとの関連付けについて（２）

下記のアカウント名やユーザーフォルダー名を例として、MSアカウントに関連付けた際の違いについて、下記に記します。

【例】
ローカルアカウント名：local-ivi
ローカルアカウントのユーザーフォルダー名：local-ivi-folder
ADアカウント名：ad-ivi
ADアカウントのユーザーフォルダ名：ad-ivi-folder
関連付けるMSアカウント名：ms-ivi

アカウント種別	関連付け後のサインアウト	アカウント名		関連付け後のユーザーフォルダ名*1	関連付け解除後のアカウント再設定
		関連付け前	関連付け後		
ローカルアカウント	強制的にサインアウト	local-ivi	ms-ivi	iocal-ivi-folder	必要*2
ADアカウント	なし	ad-ivi	ad-ivi	ad-ivi-folder	不要

*1：ユーザーフォルダー名はどのアカウントの場合でも、関連付け前、関連付け後、関連付け解除後で、変わることはありません（この例では、どの状態でも「local-ivi-folder」または「ad-ivi-folder」になります）

*2：解除後のアカウント名およびパスワードを再設定する必要があります。関連付け前と同じ設定も可能です。この例では、「local-ivi」と言うアカウント名（関連付け前と同じ）でも、全く異なるアカウント名でも設定可能です。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.
Confidential

MobiConnect Open MDM方式登録について

「ADアカウント」を設定した場合、ADアカウント内でMobiConnectのOpen MDMに登録することはできません。Open MDM方式の登録を行なう場合は、ADアカウントとは別に、ローカルアカウントまたは単独のMSアカウントを端末に設定することで、いずれかのアカウント内で登録する必要があります。

アカウント種別	Open MDMの登録	Open MDMの解除
ローカルアカウント	可能	可能
MSアカウント	可能	可能
ADアカウント	不可	可能
ADアカウント （MSアカウント関連付け状態）	不可	可能

【！注意！】
Open MDMをアカウント毎に登録することはできません。いずれかのアカウントにて、一度、Open MDMに登録した後は、他のアカウントでは解除のみ可能です（登録を解除するまでは、他のアカウントで登録操作を行なうことはできません）。

また、Open MDMの機能が利用できるのは、登録操作を行なったアカウントのみです。
該当アカウントにてサインインして、利用している時のみOpen MDMの機能を実行することが可能となります。これは、現状のMicrosoft社の仕様となります。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.
Confidential

MobiConnect Open MDM方式の機能について

「ADアカウント」を設定した状態で利用可能なOpen MDM方式の機能を以下に記します。
ただし、Open MDM方式は、その仕様上、Open MDMの登録操作を行なったアカウントのみで利用可能です。また、該当アカウントを利用中の状態のみで機能が実行されます（ロック画面状態では機能は実行されません）。

機能	実行可否
リモートロック	可能
端末情報取得	可能
ローカルセキュリティポリシー*1	可能

*1：パスワードポリシーの設定機能なります。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

MobiConnect エージェント方式登録について

「ADアカウント」を設定した状態でも、MobiConnectエージェント方式の登録操作は、管理者権限を有する、ADアカウントを含む、どのアカウントにおいても可能です。
ただし、管理者権限を有さない標準ユーザーの場合は、エージェントアプリをインストールすることができないため、登録操作を実施することはできません。

アカウント種別	エージェント方式の登録
ローカルアカウント*1	可能
MSアカウント*1	可能
ADアカウント*1	可能
ADアカウント*1 （MSアカウント関連付け状態）	可能

*1：管理者権限を有している必要があります。管理者権限がないとエージェントアプリをインストールすることはできません。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

MobiConnect エージェント方式の機能について（１）

「ADアカウント」を設定した状態で利用可能なエージェント方式の機能を以下に記します。
エージェント方式は、登録後は全てのアカウントにおいて機能を実行することが可能です。
ただし、**アカウントにより利用できない機能や機種固有の問題により実行できない場合もありますので、ご注意ください。**

機能	アカウント種別	実行可否
リモートロック	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	△*1
	ADアカウント （MSアカウント関連付け状態）	△*1
リモートアンロック	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	△*2
	ADアカウント （MSアカウント関連付け状態）	△*2

*1：実行は可能ですが、ADユーザーの場合、リモートロックをかけてもサインインすることが可能です。
リモートロックを実行しても変化はありません。

*2：実行は可能ですが、ADユーザーの場合、リモートロックをかけてもサインインすることが可能なため、
リモートアンロックを実行しても、変化はありません。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.
Confidential

MobiConnect エージェント方式の機能について（２）

機能	アカウント種別	実行可否
遠隔初期化*3	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	○
	ADアカウント （MSアカウント関連付け状態）	○
個別データ削除	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	○
	ADアカウント （MSアカウント関連付け状態）	○
端末情報取得	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	○
	ADアカウント （MSアカウント関連付け状態）	○

*3：Windows 8 RTならびにWindows 8 with BeingはBiLlockerが利用できないため、遠隔初期化機能は非対応です。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.　Confidential

MobiConnect エージェント方式の機能について（２）

機能	アカウント種別	実行可否
ファイルダウンロード	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	○
	ADアカウント （MSアカウント関連付け状態）	○
ファイルアップロード	ローカルアカウント	○
	MSアカウント	○
	ADアカウント	○
	ADアカウント （MSアカウント関連付け状態）	○

*3：Windows 8 RTならびにWindows 8 with BeingはBitlockerが利用できないため、遠隔初期化機能は非対応です。

Copyright,2015. Inventit Inc.　All other trademarks are properties of each respective owners.
Confidential

MobiConnect エージェント方式の機能について（３）

機能	アカウント種別	実行可否
デバイス利用制限 （USBメモリ制限）	ローカルアカウント	○（*）
	MSアカウント	○（*）
	ADアカウント	○（*）
	ADアカウント （MSアカウント関連付け状態）	○（*）

*） デバイス利用制限は機種依存が強く、現状、ほとんどの機種で提供できていないため、提供機種を増やせるように、対応方法の変更も含めて検討中となります。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

ADアカウントにおけるセキュリティについて（１）

ADアカウント利用時におけるMobiConnectのセキュリティ機能に関するガイドラインは以下になります。

1 リモートロックについて

リモートロックを実行しても、ADアカウントに関してはADアカウントのパスワードを入力することで、通常通りに端末にサインイン（ログイン）することが可能です。このため、ADアカウントに対してはActive Directory側にて該当するADアカウントを無効化し、端末にサインインできなくする運用が必要となります。また、ADアカウントを無効化しても、ネットワーク接続が有効でない、オフライン時には「キャッシュされたログオン機能」を使うことで、サインインが可能となってしまいます。「キャッシュされたログオン機能」は回数を設定することが可能ですので、紛失時の対策として、ADアカウントの無効化と「キャッシュされたログイン機能」をうまく併用する形での対策をおすすめします。

2 遠隔初期化（リモートワイプ）について

遠隔初期化機能は、ADアカウントを利用されている場合も問題なく実行が可能です。

従いまして、ADアカウントご利用時も紛失時の対策として有効な機能となります。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

ADアカウントにおけるセキュリティについて（２）

3 個別データ削除について

ADアカウント利用時も個別データ削除につきましては、利用可能です。遠隔初期化に代わる紛失時の対策として、ADアカウントの無効化と併せて利用することで有効な対策となります。

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.
Confidential

Copyright,2015. Inventit Inc. All other trademarks are properties of each respective owners.

Confidential