Microsoft Windows ユーザアカウント制御（UAC）

本書の目的は、Qualys ユーザが、UAC テクノロジの基本を理解し、UAC の使用が Microsoft Windows オペレーティングシステムを実行するコンピュータの Qualys スキャンにどのような影響を与えるかを理解できるようにすることです。

目次

1. 概要

1.1 UAC が Qualys スキャンに与える影響

リモートレジストリへのアクセス

- デフォルトでは、ローカルセキュリティポリシーにより、リモートレジストリサービスは無効になっています。
- レジストリにアクセスするには、Qualys Dissolvable Agent（DA）をインストールする必要があります。
- デフォルトでは、ドメインユーザ（ローカル Administrators グループのメンバー）とビルトイン Administrator ユーザのみが Qualys DA を使用できます。
- ローカルユーザ（Administrator グループのメンバー）は、Qualys DA を使用できないため、レジストリにアクセスできません。

ファイルシステムへのアクセス

- ドメインユーザ（ローカル Administrators グループのメンバー）とビルトイン Administrator のみがリモートから C$ 共有にアクセスできます。
- ローカルユーザ（Administrator グループのユーザ）は、C$ 共有にアクセスできません。Qualys スキャンにより、システムおよびアプリケーションファイルのバージョン情報が読み取られるのを防ぐためです。

1.2 UAC による Qualys スキャン結果の変更の確認方法

- 通常のスキャンおよびコンプライアンススキャンでは、部分的な結果が返されます。
- ローカルユーザ（Administrator グループのユーザ）の権限が不十分な場合、DA のインストールが失敗します。

1.3 UAC 設定の調整をしない場合のスキャンへの影響

- ローカルユーザ（Administrator グループのユーザ）は、デフォルトで ADMIN$ 共有へのアクセスが無効になっているため、Qualys DA をインストールできません。

2. 基本原理

ユーザアカウント制御（UAC）は、最初に Windows Vista に導入されたテクノロジで、現在 Microsoft Windows オペレーティングシステムのすべての最新バージョンでサポートされています。

UAC テクノロジの詳細については、以下の記事（Microsoft TechNet Magazine 発行、Sysinternals 共同設立者 Mark Rossinovich 著）を参照してください。

Windows Vista ユーザアカウント制御の内部:
http://technet.microsoft.com/en-us/magazine/2007.06.uac.aspx

Windows 7 ユーザアカウント制御の内部:
http://technet.microsoft.com/ja-jp/magazine/2009.07.uac.aspx

3. UAC の設計

UAC 設計者の主な目的は、Microsoft Windows のセキュリティ向上でした。これは、管理者以外のユーザによるオペレーティングシステムの使用を標準にすることで達成されました。すなわち、ビルトイン Administrator であるか、Administrators グループの他のメンバーであるか、他のグループであるかに関係なく、常に標準ユーザとして Windows を使用するということです。また、昇格した権限が要求される管理タスクは、ユーザが必要とした場合または特に要求した場合にのみ実行できるようになっています。管理者権限を昇格させる UAC モードは「管理者承認モード」と呼ばれます。

この仕組みを説明するために、以下に例を挙げます。

例 1 - Alice は Users グループのメンバーで、レジストリエディタ（regedit.exe）アプリケーションを実行して、システムレジストリに変更を加えたいと思っています。Alice は、HKEY_CURRENT_USER ハイブの変更はできますが、HKEY_LOCAL_MACHINE の変更は拒否されます。この場合、Alice はレジストリエディタを管理者として実行することでき、UAC は、Alice のこの権限を完全に拒否するか、Administrators グループのメンバーの承認を求めるダイアログボックスを Alice に表示することで、このプロセスを制御します。

例 2 - Bob は Administrators グループのメンバーで、レジストリエディタ（regedit.exe）アプリケーションを実行して、システムレジストリに変更を加えたいと思っています。この場合、UAC は、そのままプログラムの実行を許可するか、昇格した権限でプログラムを実行するための承認を求めるダイアログボックスを Bob に表示することで、このプロセスを制御します。

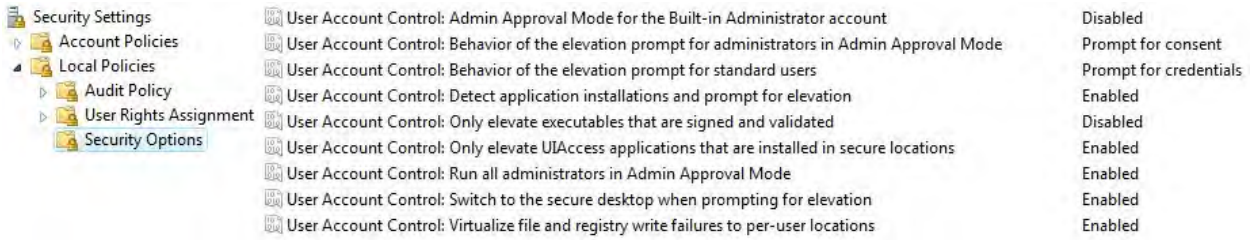
4. UAC ポリシー – デフォルトの設定

ローカルセキュリティポリシーは、上記の動作を制御する多数の UAC 設定を定義します。例えば、UAC ポリシーは、署名されていない Windows プログラムの起動を禁止するように設定することができます。

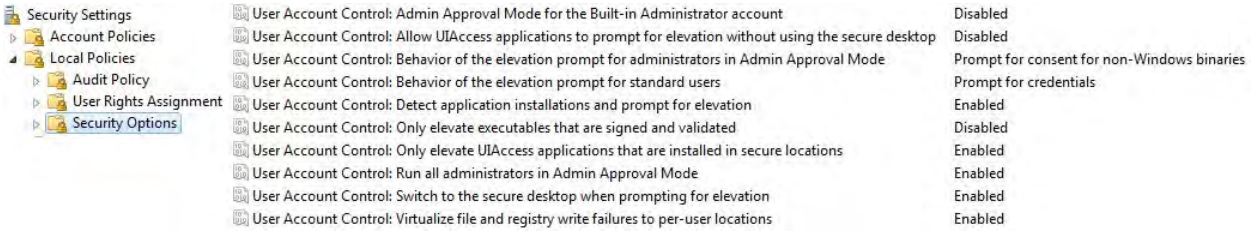
UAC 設定は、ローカルセキュリティポリシーで定義され、接頭辞として“ User Account Control ”が使用されます。ローカルセキュリティポリシーエディタは、「Administrative Tools」→「Local Security Policy」を選択して、直接起動できます。また、Microsoft 管理コンソール（mmc.exe）アプリケーションを実行し、ローカルコンピュータにローカルポリシーエディタまたはグループポリシーオブジェクトエディタのスナップインを追加して、起動することもできます。

次の項では、ローカルセキュリティポリシー内の UAC ポリシーの場所と UAC のデフォルト値を示します。

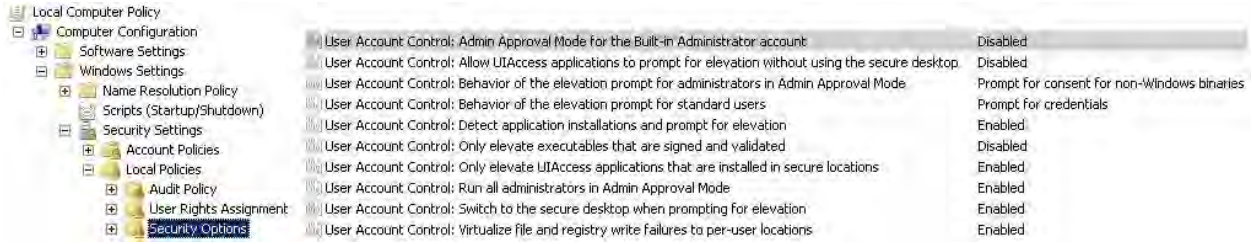
Windows Vista



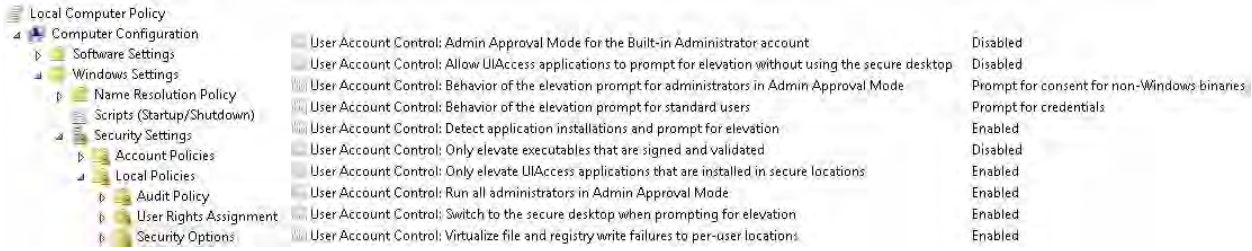
Windows 7



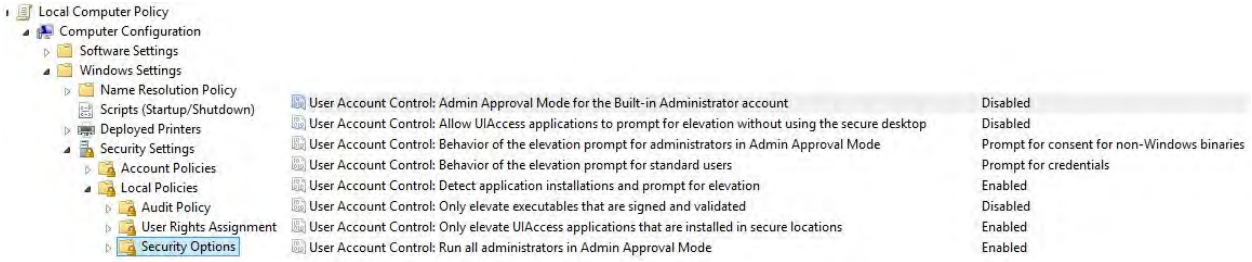
Windows 2008、Windows 2008 R2



Windows 2012、Windows 2016



Windows 8、Windows 8.1



5. 管理者承認モード

管理者承認モードには、通常のデスクトップまたはセキュアデスクトップ上で切り替えることができ、特定の UAC ポリシー設定によってこのプロセスが制御されます。通常のデスクトップの場合、管理者権限の昇格を承認するためのダイアログボックスがデスクトップに表示され、他のアプリケーションの使用が禁止されることはありません。セキュアデスクトップの場合は、管理者権限の昇格を承認するためのダイアログボックスを表示する専用のデスクトップが新たに作成され、承認が許可または拒否されるまで、他のアプリケーションの使用は禁止されます。

6. ローカルポリシーの UAC の設定

UAC ポリシーには、UAC をサポートするすべての Windows バージョンに共通する 2 つの設定があります。その他の UAC の設定は、Windows システムの Qualys 認証スキャンには影響しません。

6.1 ユーザアカウント制御: 管理者承認モードですべての管理者を実行する

この設定は、UAC を有効にするか、無効にするかを効果的に制御します。デフォルトは「有効」です。このオプションを「無効」に変更すると、UAC がオフになり、システムの再起動が必要になります。

6.2 ユーザアカウント制御: ビルトイン Administrator アカウントのための管理者承認モード

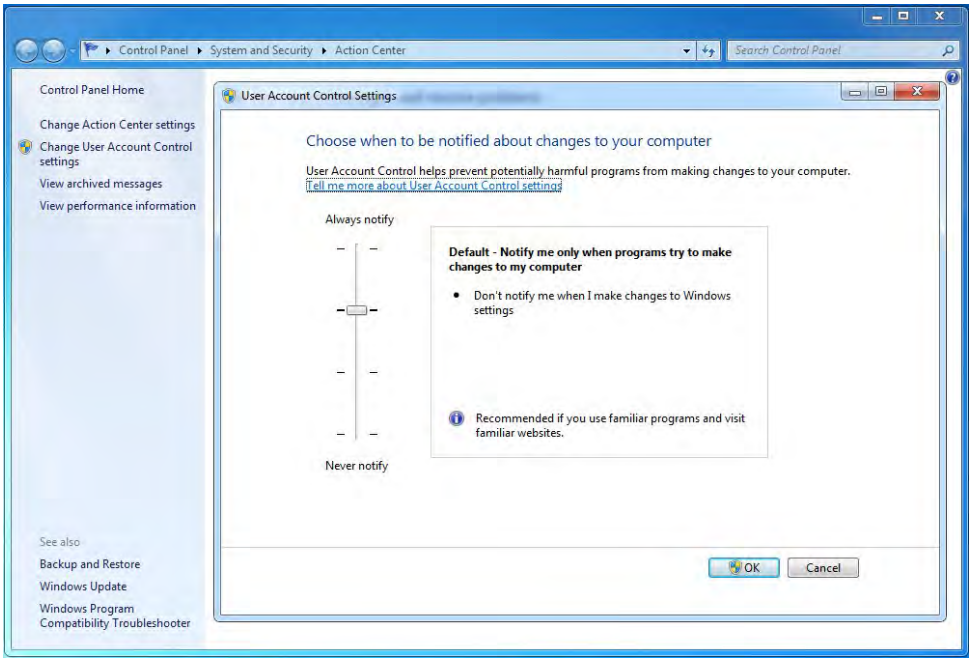
この設定は、ビルトイン Administrator ユーザにのみ影響します。ユーザが Administrators グループのメンバーであるかどうかに関係なく、他のユーザアカウントには一切影響しません。

デフォルトは「無効」です。すなわち、ビルトイン Administrator ユーザがアプリケーションを起動する場合、管理者承認モードは必要なく、自動的に承認が付与されます。

7. UAC の設定 – 代替インタフェース

代替インタフェースには 4 つの異なる通知タイプがあり、シンプルなスライダコントロールを使用して選択できます。このインタフェースは、Windows 2008 と 2012 を含め、Windows Vista 以降の Windows バージョンでサポートされています。

このインタフェースにアクセスするには、「Control Panel」→「System and Security」→「Action Center」→「Change User Account Control settings」(下記の例を参照)を選択します。スライダコントロールを「Never notify」に設定すると、UAC が無効になります。設定を適用するには、システムを再起動する必要があります。



Windows 2016 以降では、UAC を無効にするには、「User Accounts」→「Turn User Account Control On or Off」を選択し、「Use User Account Control (UAC) to help protect your computer」オプションをオフにします（チェックマークを外します）。「OK」をクリックして変更内容を保存します。

8. ADMIN$ 共有へのアクセス

Qualys スキャンで ADMIN$ 共有へのアクセスが必要な理由はいくつかあります。この項では、その一部について説明します。

8.1 リモートレジストリサービス

リモートレジストリサービスは、Windows Vista 以降ではデフォルトで無効になっています。リモートレジストリサービスは、システムレジストリへのリモートアクセスをサポートする API を提供します。この API は、ADMIN$ 共有へのアクセスを必要とせず、SMB/TCP 経由の RPC と IPC$ 共有へのアクセスを使用してアクセスされます。

Windows システムの Qualys スキャンでは、レジストリ API へのアクセスが必要です。レジストリ API には、次のいずれかの方法でアクセスできます。

- リモートレジストリサービスを有効にします。この操作は、ユーザの Windows コンピュータに設定された既存のセキュリティポリシーと競合する場合があります。
- リモートレジストリサービスを無効のままにして、Dissolvable Agent を有効にすると、レジストリ API にアクセスできます。Dissolvable Agent のインストールおよび削除には、ADMIN$ 共有へのアクセスが必要です。

8.2 Windows ファイアウォール

Windows ファイアウォールの設定は、ADMIN$ 共有へのアクセスに影響し、ファイアウォールルールは、ADMIN$ へのアクセスを管理する UAC ポリシーが評価される前に有効になります。

Windows ネットワーク共有へのアクセスには、ネットワークトランスポート（NetBIOS、SMB など）が必要です。Windows ネットワーク共有へのアクセスに一般的に使用されるトランスポートは、SMB over TCP です。SMB プロトコルは CIFS とも呼ばれます。

Windows ファイアウォールは、Windows Vista 以降ではデフォルトで有効になっています。TCP ポート 445 へのアクセスは、デフォルトでブロックされています。

ADMIN$ 共有にアクセスするには、ファイアウォールのルールで、Qualys スキャナの IP アドレスから TCP ポート 445 へのアクセスを許可する必要があります。新しいルールを作成するか、デフォルトで無効になっている既存のルールを変更します。

9. リモート UAC

ADMIN$ 共有へのアクセスは、UAC ポリシーのリモート UAC 部分で制御されます。ただし、ローカルポリシーエディタは、リモート UAC を制御する設定を定義しません。デフォルトでは、ADMIN$ 共有へのリモートアクセスは無効になっています。

リモート UAC の設定を変更して ADMIN$ 共有へのアクセスを有効にしても、UAC ポリシーで定義された管理者承認モードの設定には影響がありません。これにより、UAC は有効なまま、対話ユーザ向けに設計されたとおりに機能し、ADMIN$ 共有へのリモートアクセスが有効になります。
ADMIN$ 共有へのアクセスを有効にする設定は、システムレジストリで直接定義する必要があります。

なお、リモート UAC を有効にすると、ADMIN$ 共有へのアクセスが許可されるだけでなく、「Computer Management」→「Action」→「Connect to another computer」を選択することで、別の Windows コンピュータからリモートで Windows システムを管理できるようになります。

リモート UAC ポリシーについて以下で提示する変更は、デフォルトで ADMIN$ にアクセスできるドメインアカウントには影響しません。すなわち、リモート UAC ポリシーは、Administrators グループのメンバーであるローカルユーザアカウントにのみ影響します。

使用例

以下の例では、信頼済みスキャンを実行し、Administrators グループのメンバーであるローカルユーザアカウントで認証を行うために、ユーザがリモート UAC ポリシーを変更する必要があります。

1) ドメインメンバーシップを持たないスタンドアロンの Windows システム（GPO は、使用するドメインがないため、ここでは機能しません。他の何らかの自動処理により、レジストリの変更を行う必要があります。例えば、REG コマンドを呼び出すバッチファイルを使用します（下記参照））。

2) ローカルアカウントでスキャンを実行するドメイン参加の Windows システム（GPO を使用してレジストリを変更できます）。

設定手順

1) 「管理者として実行」モードでレジストリエディター（regedit.exe）を起動し、必要であれば管理者承認を付与します。

2) HKEY_LOCAL_MACHINE ハイブに移動します。

3) SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System キーを開きます。

4) 次のプロパティを指定して新しい DWORD（32 ビット）値を作成します。
　　名前: LocalAccountTokenFilterPolicy
　　値: 1

5) レジストリ エディターを閉じます。

警告: DWORD（32 ビット）と QWORD（64 ビット）のデータタイプの値は、64 ビットバージョンの Windows ではメニューで隣り合わせに位置しています。そのため、間違ったデータタイプを選択するミスが発生しやすくなっています。データタイプは、DWORD（32 ビット）であることが必要です。QWORD（64 ビット）を選択して、値を 1 に設定しても、リモート UAC は有効になりません。

システムの再起動またはサーバサービスの再始動の要請には疑問の余地があります。一部のドキュメントで推奨されているのにもかかわらず、レジストリでリモート UAC を無効にすると、これはすぐに反映されて、Qualys のスキャン中に ADMIN$ へのリモートアクセスが許可されます。

もう 1 つの方法

リモート UAC を有効にするには、(昇格権限のプロンプトを使用して)レジストリエントリコマンドを使用し、レジストリエントリを削除することもできます。

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

リモート UAC を無効にする方法

以下の方法を使用して、リモート UAC を無効にできます。

1) (昇格権限のプロンプトを使用して)レジストリ編集コマンドを使用します。

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0 /f
```

2) アカウント制御の設定を使用します。

「Control Panel」→「System and Security」→「Change User Account Control settings」を開きます。または、次の実行ファイルを実行します(「Start」→「Run」、またはコマンドプロンプトを使用します)。

```
C:\Windows\System32\UserAccountControlSettings.exe
```

次に、Windows バージョンに応じて、スライダを動かして「Never Notify」に設定するか、「Use User Account Control (UAC) to help protect your computer」オプションをオフにします(チェックマークを外します)。「OK」をクリックし、指示に従って管理者パスワードを入力します。

10. ADMIN$ 共有へのユーザアクセス

UAC は、ADMIN$ 共有へのアクセスを制御します。このパーミッションは、ユーザタイプによって異なります。ドメイン資格情報またはローカル資格情報を使用して、Windows システムにアクセスできます。この項では、さまざまなユーザが ADMIN$ 共有にリモートでアクセスする際の動作について説明します。

10.1 ドメインユーザ

ローカル Administrators グループのメンバーであるドメインユーザには、デフォルトで ADMIN$ 共有へのアクセスが付与されます。

Qualys スキャンが Windows ドメイン資格情報を使用し、(通常は Domain Admins グループなどのグループに含まれることにより)ユーザが Administrators グループのメンバーでもある場合、UAC ポリシーを変更することなく、ADMIN$ 共有にアクセスできます。

10.2 ローカルユーザ

UAC ポリシーの設定では、以下のユーザタイプが区別されます。
- ビルトイン Administrator
- Administrators（Administrators グループのメンバー）
- 標準ローカルユーザ

ADMIN$ 共有にアクセスするためのパーミッションの制御は、ユーザタイプごとに異なります。

10.2.1 ビルトイン Administrator

ビルトイン Administrator ユーザは、デフォルトで ADMIN$ 共有にアクセスできます。これは、6.2 項で説明した UAC ポリシーの設定で制御されます。
新しいコンピュータに Windows Vista 以降がインストールされると、ビルトイン Administrator アカウントは無効になります。インストール中に新しいユーザが作成され、Administrators グループに自動的に追加されます。このユーザは、後に管理者承認モードに切り替えることで、他のユーザを追加し、システム管理の管理タスクの優先順位を昇格させることができます。

ビルトイン Administrator ユーザはデフォルトで無効になっているため、使用するためには、アカウントを有効にし、パスワードを設定する必要があります。ビルトイン Administrator アカウントを使用する Qualys スキャンは、**デフォルト**の UAC ポリシーを変更することなく、ADMIN$ 共有にアクセスできます。

10.2.2 Administrators（Administrators グループのメンバー）

Administrators グループのメンバーは、リモート UAC が有効（8 項を参照）になっている場合、または UAC ポリシーが完全に無効になっている場合に、ADMIN$ 共有にアクセスできます。

ADMIN$ 共有にリモートでアクセスするには、既存の UAC ポリシーを維持したままでリモート UAC を有効にする方が、UAC ポリシーを完全に無効にするよりも安全性が高まります。

10.2.3 標準ユーザ

標準ユーザは、デフォルトで ADMIN$ 共有にアクセスできますが、付与されるアクセス権は読み取り専用モードであるため、Dissolvable Agent のインストールや削除はできません。

このパーミッションは UAC ポリシーに依存しません。Windows オペレーティングシステムのインストール時に ADMIN$ として共有される Windows インストールディレクトリに設定される NTFS パーミッションによって制御されます。