ivanti

Windows の管理者権限を持つエンドユーザーを制限する 9 つの方法

ホワイトペーパー

目次

はじめに

社内に存在する Windows 管理者アカウントの数を把握していますか？社内に多数の管理者アカウントが存在する場合、権限が付与されたそれらの特権アカウントが与えられた役割を遂行するためにそこまでのアクセス権を必要としない社員や、1 つか 2 つの作業を行うための権限のみ必要な社員に使用されている可能性があります。

IT システム管理者としてトレーニングを受けていない社員に対して完全な管理者権限を付与すれば、セキュリティのリスクが高まり、管理コストが膨らみ、コンプライアンス遵守が困難になります。本書では、Ivanti® Security Controls を使用してすぐに導入できる 9 つの制限をご紹介します。これらの制限を組み合わせて使用すれば、企業は次のようなメリットを得られます。

- 社員が一部の管理者設定を誤って変更してしまい、問題を解決するために IT 部門のサポートが必要となる状況を軽減できます。
- 自社のエンドポイントの特定の保護を社員が変更することや、無効化することをさらに難しくすることができます。

さらに保護を強化するための企業が目指すべき長期的目標は、不必要なアカウントを標準のユーザーアカウントに変更し、必要最低限の権限のみを付与するアプローチを社内に導入することです。この目標もまた、Ivanti Security Controls で達成できますが、本書で扱う範囲を超えていますので本書でその方法についての説明は提供しておりません。

管理者権限を持つ管理者ではない社員を制限する機能は、Ivanti Security Controls の一部である Application Control の権限管理のサブ機能の一部となります。Security Controls エージェントの一部である Application Control エンジンは、すべてのエンドポイントで実行します。このエンジンは、構成で定義された一連のルールを施行し、Application Control の挙動を指定します。本書内のスクリーンショットには、各制限に必要な構成が示されています。

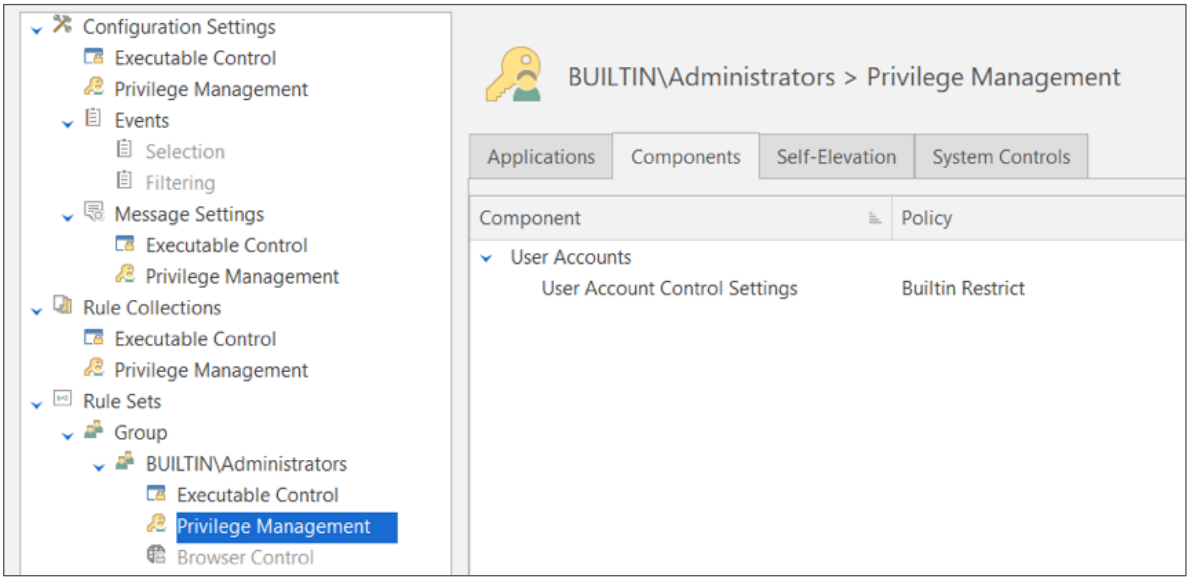
制限 1 - ユーザーによる UAC 設定の変更防止

Ivanti は、管理者アカウントを持つユーザーを含むすべてのエンドユーザーにユーザーアカウント制御（UAC）を導入することを推奨しています。Microsoft は自社のウェブサイトで次のように明言しています。

> *ユーザーアカウント制御（UAC）は、マルウェアによる PC への攻撃を防止し、企業がさらに管理が強化されたデスクトップを展開する上で役立ちます。UAC を導入すれば、管理者がシステムを指定し、そのシステムに対して管理者レベルのアクセス権を付与しない限り、アプリやタスクは常に管理者アカウント以外のアカウントのセキュリティ環境で実行します。UAC は、不正アプリの自動インストールをブロックし、システム設定への意図せぬ変更を防止します。*

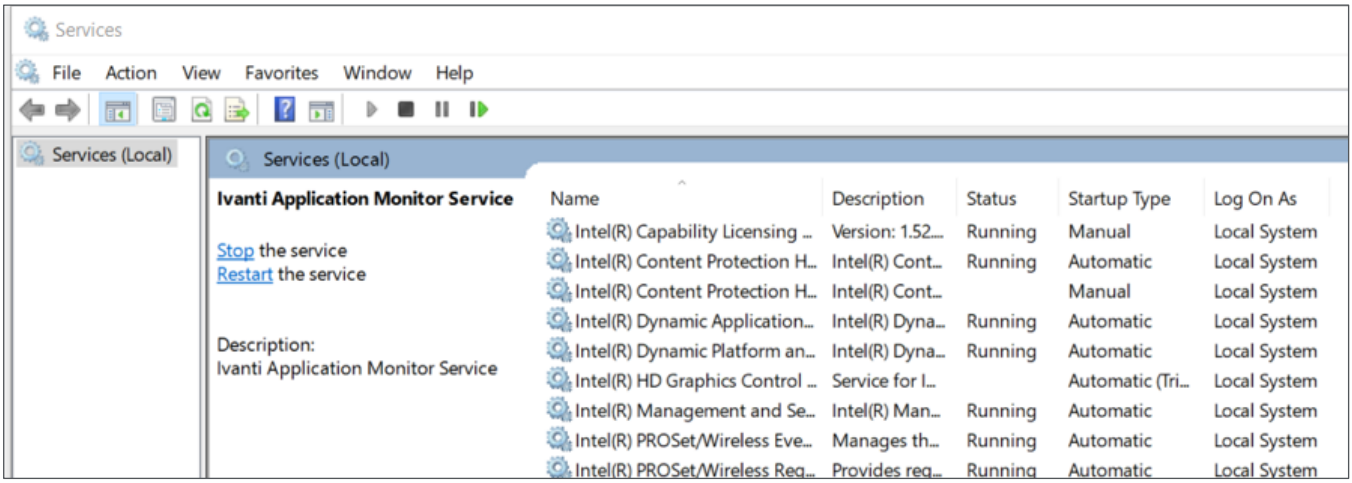
すべてのマシンで、「常に通知する」の設定を選択し、UAC を有効に設定することが推奨されています。UAC はグループポリシー経由で有効に設定できます。Ivanti Security Controls は、管理者がユーザーアカウント制御をオフに設定することを防止できます。

下に示されている Configuration Editor のように、[Components]（コンポーネント）タブにアクセスし、Windows のコンポーネントである[User Account Control Settings]（ユーザーアカウント制御設定）を選択します。その後、ルールのポリシーを[Builtin Restrict]（ビルトイン制限）に設定します。



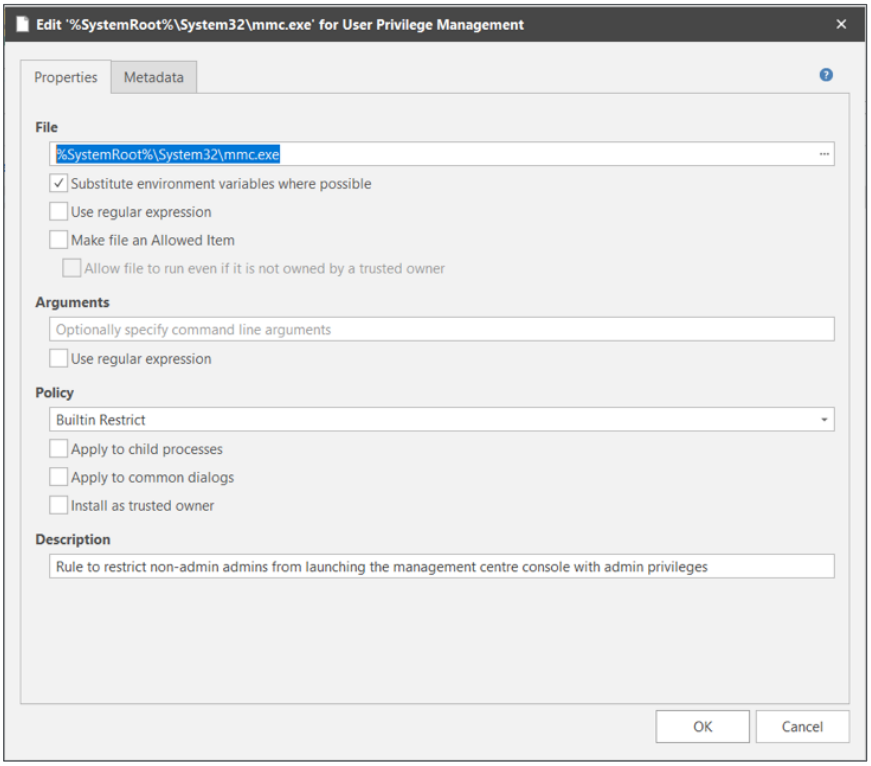
制限 2 - ユーザーによる管理者権限での MMC の実行防止

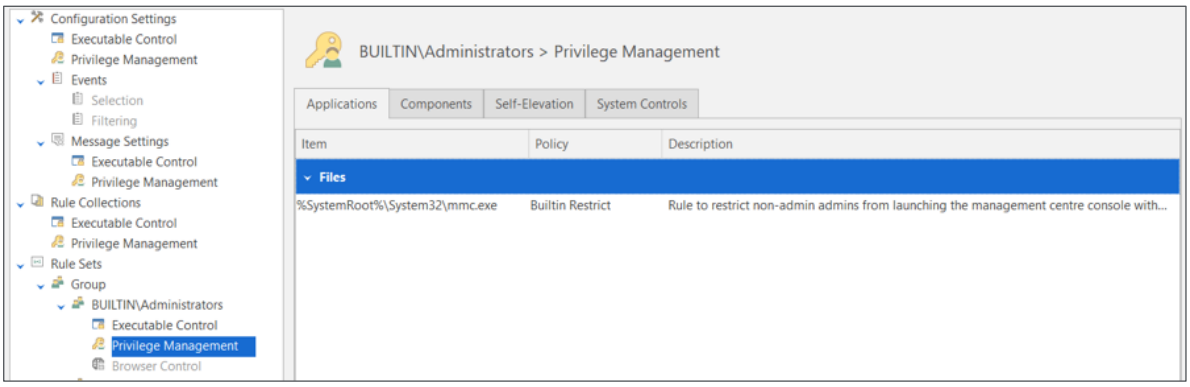
Microsoft 管理コンソール（MMC）は、オペレーティングシステムの管理および構成のためのインターフェースをエンドユーザーに提供するフレームワークです。MMC は、エンドユーザーがスナップインを読み込むことを可能にします。各スナップインは、Windows の特定の機能を管理するためのツールです（例えば、「サービス」スナップインは、Windows のサービスを管理するためのツールです）。



スナップインは大きな影響をもたらす可能性があります。例えば、管理者権限を持つエンドユーザーは「サービス」スナップインでサービスを停止させることができます。停止されたサービスがアンチウイルスソフトウェアの一部だった場合、実行されるダウンロードすべてのウイルススキャンが停止してしまうため、マルウェアからの脅威が高まります。

Ivanti Security Controls を導入すれば、管理者アカウントを使用しているエンドユーザーが、管理者権限を使用して MMC を実行することを防止できます。Configuration Editor の[Applications]（アプリケーション）タブでファイルルールを作成します。その後、ルールのポリシーを[Builtin Restrict]（ビルトイン制限）に設定します。



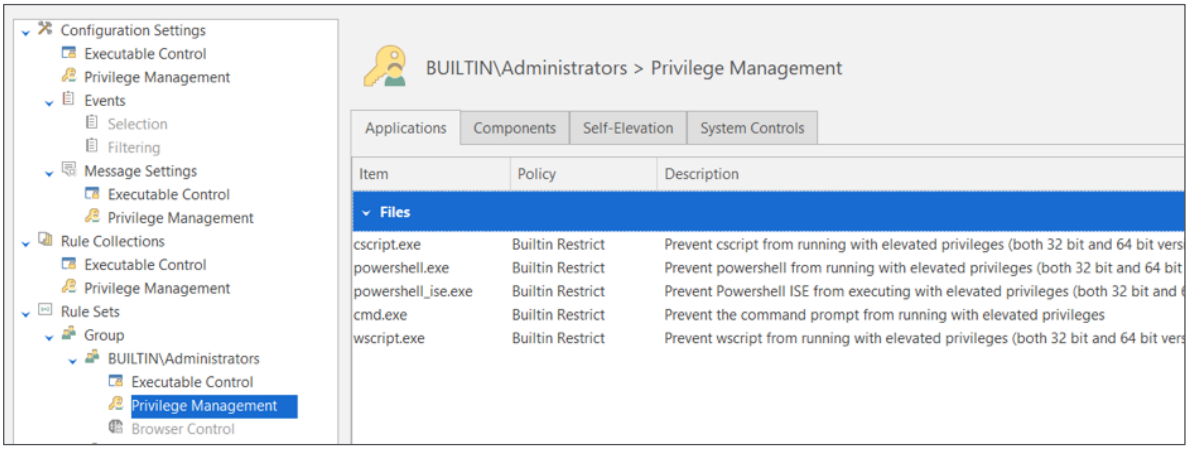


制限 3 - ユーザーによる管理者権限でのコマンドやスクリプトの実行防止

Windows は、コマンドラインインタプリタ経由で、もしくはスクリプトを実行することで、特定のコマンドを発行することにより、オペレーティングシステムを操作するいくつかの代替方法をサポートしています。コマンドラインインタプリタは管理目的で、スクリプトは一般的に自動化に使用されます。Windows 標準装備のコマンドラインインターフェースは、「コマンドプロンプト」と「Windows PowerShell」です。さらに、オペレーティングシステムには、様々なスクリプト言語のスクリプトを実行するために使用できる「Windows Script Host」も装備されています。

管理者権限を持つ社員であれば誰でもコマンドやスクリプトを実行できます。また、コマンドやスクリプトの実行は、多くのケースにおいて、本書で概説されている GUI ベースの制限をオーバーライドするための代替方法となります。このため、コマンドラインインタプリタと Windows Script Host を制限する必要があります。

Application Control は、この 2 つを制限する上で役立ちます。この制限を構成するため、各コマンドラインインタプリタに加え、Windows Script Host の Windows バージョンとコンソールバージョンに対してファイルルールを作成します。[Applications]（アプリケーション）タブで各ルール項目を作成し、各項目のポリシーを[Builtin Restrict]（ビルトイン制限）に設定します。

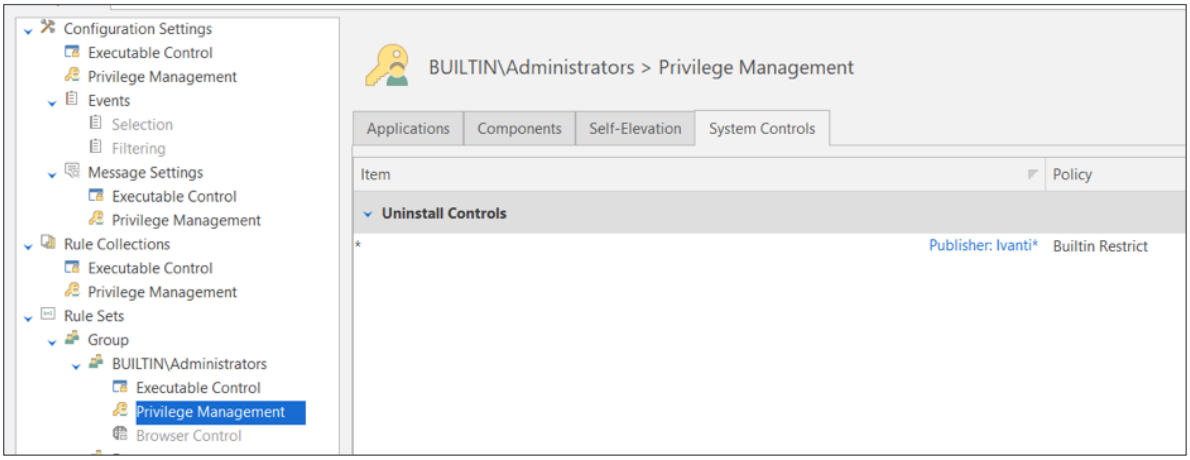


昇格権限でスクリプトを実行する必要が生じた場合、対象のスクリプトに対してのみスクリプトを実行することを可能にするため Application Control も構成できます。

制限 4 - 自社システムを保護しているサードパーティーソフトウェアのユーザーによるアンインストールの防止

Ivanti Security Controls は、企業のエンドポイントを保護するため、エンドポイントにインストールされているエージェントに対して機能します。管理者権限を持つエンドユーザーはこのエージェントをアンインストールできます。ただし、アンインストールされた場合、保護が失われます。この事態の発生を防ぐため、[System Controls]（システムコントロール）タブでアンインストールのルールを構成します。アプリケーションの特定のバージョンを対象にアンインストールのルールを作成することや、より対象を広範にするためワイルドカードを使用してルールを作成することができます。

下のスクリーンショットでは、パブリッシャーのみが設定されています。この場合、設定されたパブリッシャーに一致するアプリケーションすべてが、管理者権限を持つエンドユーザーによってアンインストールできなくなります。



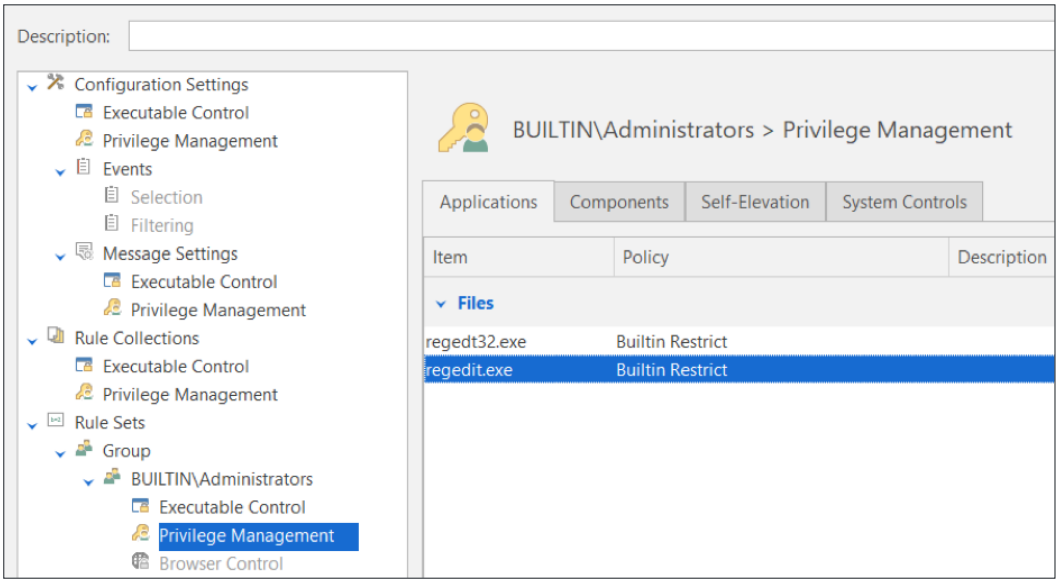
さらに、Ivanti Security Controls を使用して、同様のルールを作成し、他のサードパーティーソフトウェアのアンインストールを防止することもできます。

制限 5 - レジストリにおいてユーザーによってシステム設定が可能な状態になる事態の防止

Windows レジストリには、Windows のエンドポイントと各エンドポイントの構成に関する重要な情報に加え、インストールされているアプリケーションプログラムすべてに関する情報も保存されているため、レジストリは非常に重要なものです。レジストリキーに直接アクセスできる機能とレジストリキーを変更する機能を提供することで、管理者権限を持つエンドユーザーは、自分が選択した統合管理ポリシーにアクセスし、設定を変更できるようになります。さらにこのアクセ

ス権は、本書で説明されている多くの保護を回避する別の経路をユーザーに提供します。

最低でも、レジストリへの権限アクセスを制限する必要があります。Ivanti Security Controls を使用すれば、[Applications]（アプリケーション）タブで、各レジストリ編集アプリケーションに対してファイルルールを作成し、各ルールのポリシーを[Builtin Restrict]（ビルトイン制限）に設定することで、この制限を構成できます。

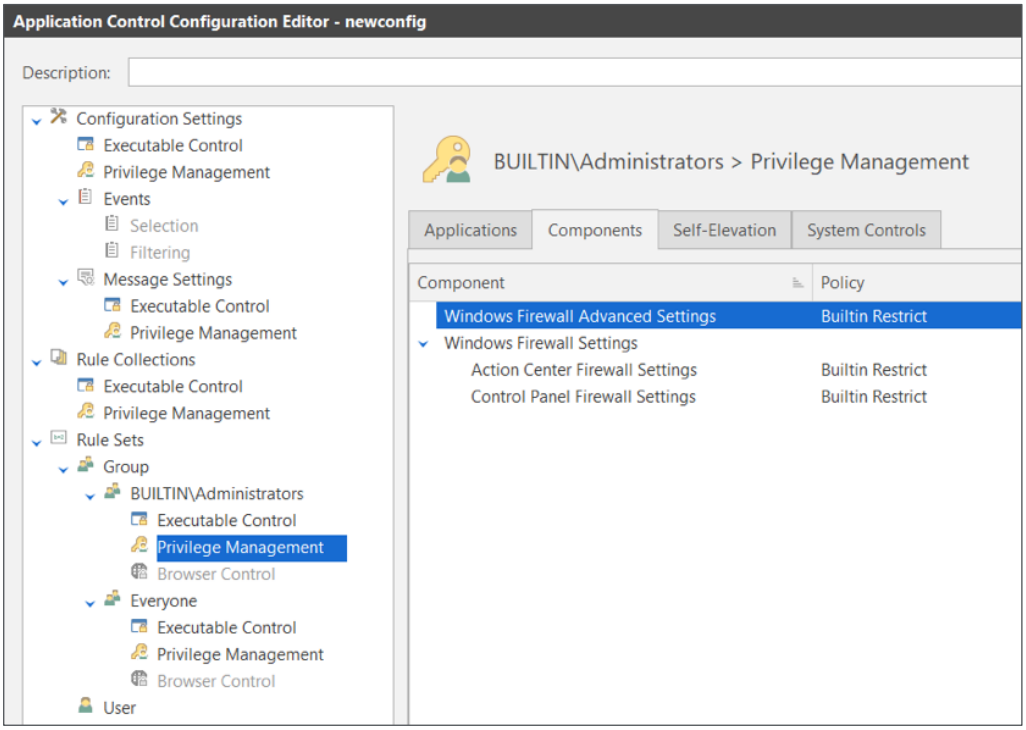


さらに保護を強化するため、Ivanti Security Controls は、管理者権限の有無を問わず、レジストリを編集するために使用されるアプリケーションにユーザーがアクセスすること自体を禁止することもできます。

制限 6 - ユーザーによるエンドポイントのファイアウォールの設定の無効化&変更防止

ファイアウォールは、企業のネットワークへのトラフィックと企業のネットワークからのトラフィックをモニタリングするネットワークセキュリティデバイスで、定義された一連のセキュリティルールに基づいてトラフィックを許可、またはブロックします。ファイアウォールにより、悪意のあるソフトウェアがネットワーク全体に拡散しにくくなります。

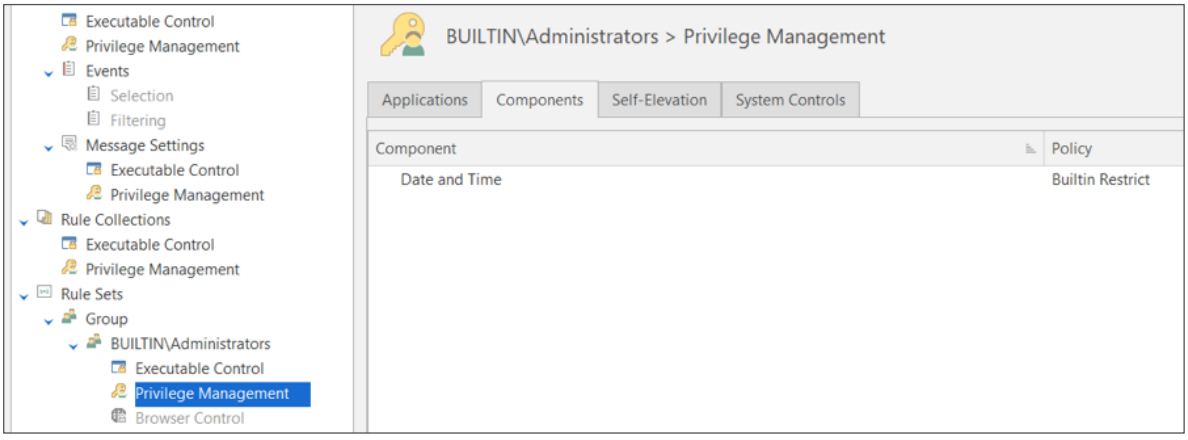
Windows Defender ファイアウォールを使用している場合、この機能の無効化を防止することを推奨します。無効化を防止するには、[Privilege Management]（権限管理）ノードで以下の Windows コンポーネントを選択し、各コンポーネントのポリシーを[Builtin Restrict]（ビルトイン制限）に設定します。



制限 7 - ユーザーによる日時の変更防止

管理者権限を持つ管理者ではない社員は、日時を変更できます。これは大したことではないように聞こえますが、いくつかの深刻な状況を招く可能性があります。日時が誤っている場合、多くのアプリケーションは正常に機能しません。さらに、ログインがすべて誤ったタイムスタンプで記録されるため、監査が無効になる可能性や、トラブルシューティングが困難になる可能性があります。日時変更を制限するもうひとつの理由は、多くのユーザーがライセンスの制限を回避するために日時変更を利用し、時間を過去に戻すことで、同じトライアルライセンスを何度も何度も利用し続ける可能性があるからです。

Ivanti Security Controls は、管理者が日時変更することを防止できます。Windows の[Components]（コンポーネント）タブで[Date & Time]（日時）のコンポーネントを選択します。その後、コンポーネントのポリシーを[Builtin Restrict]（ビルトイン制限）に設定します。

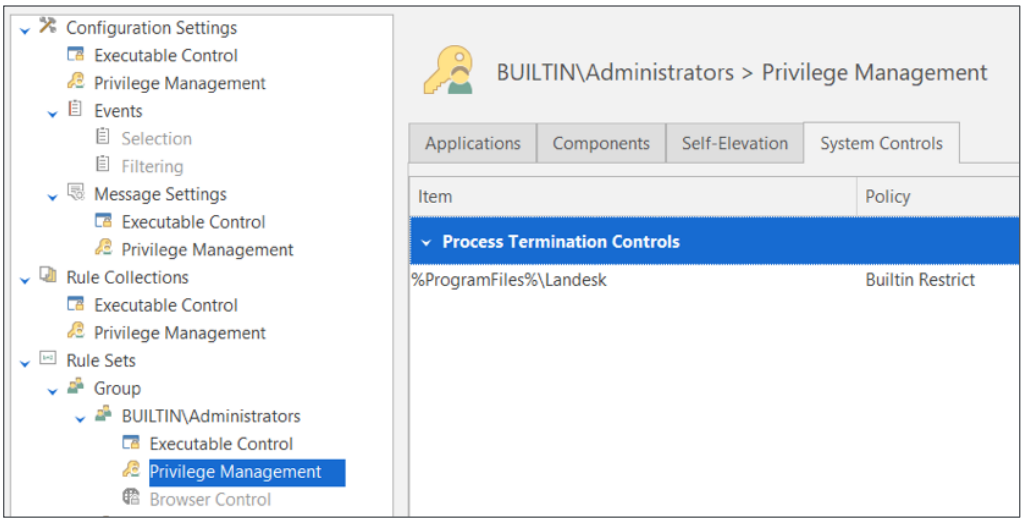


また、日時の変更は、管理者権限で日時のコマンドを使用してコマンドライン経由で行うこともできます。これに対する保護については、「制限 3」で説明されています。

制限 8 - ユーザーによるプロセス停止の防止

管理者権限を持つエンドユーザーは実行中のプロセスを停止できます。1) [タスクマネージャー]を使用して[タスクを終了]を選択する方法や、2) Process Explorer を実行し、[強制終了]を選択する方法は、プロセスを停止する方法の一例となります。これらは、システムで実行中の保護ソフトウェアをエンドユーザーが無効化する別の方法を示しており、こういった操作により、セキュリティのリスクが高まる可能性があります。

Ivanti Security Controls エージェントソフトウェアが停止されることを防止するため、[System Controls]（システムコントロール）タブで構成に[Process Termination Control]（プロセス終了制御）フォルダーのルール項目を追加します。必ずルールで、保護対象のソフトウェアが保存されているフォルダーの場所（この例では「%ProgramFiles%\Landesk」を指定してください。また、必ずルールのポリシーを[Builtin Restrict]（ビルトイン制限）に設定してください。



さらに他のソフトウェアの停止を防止するため、他のルールを Application Control の構成に追加することもできます。

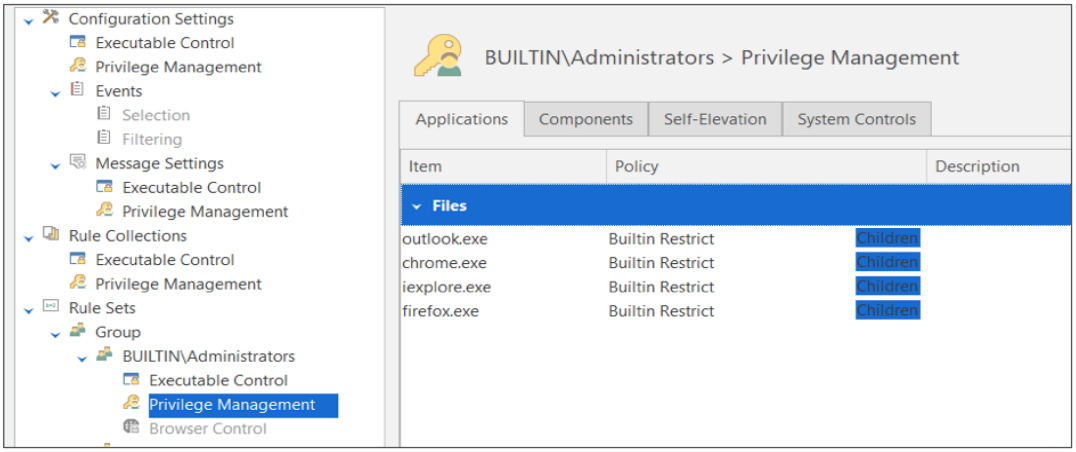
この制限は、特定の GUI アプリケーションからのプロセス停止を防止するものですが、管理者権限でのコマンドプロンプト（例：「強制終了」コマンドを使用するなど）から停止を実行することもできますのでご注意ください。ただし、制限 3 はこの操作を防止します。

制限 9 - マルウェアを侵入させる可能性のあるアプリケーションのユーザーによる昇格権限での実行を防止

管理者権限を持つエンドユーザーは、昇格権限を使用してあらゆるアプリケーションを起動できます。これらのアプリケーションの中には、エンドポイントにマルウェアを侵入させる可能性のあるメールアプリケーションやブラウザアプリケーションが含まれます。これらのアプリケーションは通常、管理者権限を持つユーザーが意図的に管理者権限で実行しない限り実行されません。この制限は管理者権限での実行を防止します。

これらのアプリケーションのいずれかが管理者権限で実行されている場合、そのアプリケーションの実行により生じたマルウェアを含む子プロセスすべてが管理者権限で実行されます。したがって、標準の権限だけでのみ実行されるようにするため、これらのアプリケーションを制限する必要があります。

Ivanti Security Controls を使用すれば、[Applications]（アプリケーション）タブで、各ブラウザアプリケーションまたはメールアプリケーションに対してファイルルールを作成し、各ルールのポリシーを[Builtin Restrict]（ビルトイン制限）に設定することで、この制限を構成できます。また、各項目で子プロセスにも制限を適用するオプションを必ず選択してください。下のスクリーンショットには、最も一般的なアプリケーションが一例として示されています。



次のステップ：

以上で、制限の概要についての説明は終了です。本書で紹介した制限を導入することで、1) 管理者権限を持つ管理者ではない社員が管理者設定を誤って変更してしまい、問題を解決するために IT 部門のサポートが必要となる状況を軽減でき、2) 管理者権限を持つ管理者ではない社員が自社のエンドポイントの特定の保護を社員が変更することや、無効化することをさらに難しくすることができます。

実際に Application Control の機能や動作を確認することを希望される場合は、デモをリクエストいただきますようお願いいたします。