Cloud Agent for Windows

インストールガイド

April 26, 2024

Qualys, Inc.

919 E Hillside Blvd

4th Floor
Foster City, CA 94404

1 (650) 801 6100

目次

前書き

Qualys Cloud Agent for Windows へようこそ。このユーザーガイドでは、ネットワーク内のホストにクラウドエージェントをインストールする方法について説明します。

クオリスについて

Qualys, Inc. (NASDAQ: QLYS) は、クラウドベースのセキュリティおよびコンプライアンス ソリューションのパイオニアであり、リーディング プロバイダーです。Qualys Cloud Platform とその統合アプリは、重要なセキュリティ インテリジェンスをオンデマンドで提供し、IT システムと Web アプリケーションの監査、コンプライアンス、保護の全範囲を自動化することで、企業がセキュリティ運用を簡素化し、コンプライアンス コストを削減するのに役立ちます。

1999 年に設立された Qualys は、Accenture、BT、Cognizant Technology Solutions、Deutsche Telekom、Fujitsu、HCL、HP Enterprise、IBM、Infosys、NTT、Optiv、SecureWorks、Tata Communications、Verizon、Wipro などの主要なマネージドサービスプロバイダーおよびコンサルティング組織と戦略的パートナーシップを確立しています。同社は、Cloud Security Alliance (CSA) の創設メンバーでもあります。 詳細については、 www.qualys.com をご覧ください。

Qualys サポートへのお問い合せ

Qualys は、最も徹底したサポートを提供することをお約束します。Qualys は、オンライン ドキュメント、電話ヘルプ、直接の電子メール サポートを通じて、お客様の質問に可能な限り最速で回答することを保証します。年中無休、24 時間対応しています。www.qualys.com/support/ でサポート情報にアクセスします。

はじめに

Qualys Cloud Agent にご関心をお寄せいただきありがとうございます。

このドキュメントでは、Qualys Cloud Agent for Windows のインストールについてすべて説明します。要件、インストール手順、プロキシサポート、証明書サポート、ウイルス対策と HIPS の除外、ベストプラクティスなどについて説明します。

Qualys Cloud エージェント 序章

Qualys Cloud Platform は、すべてのグローバル IT 資産を継続的に保護するために必要なすべてを提供します。Qualys Cloud Agent を使用すると、ラップトップ、デスクトップ、仮想マシンなど、どこにいても、どこにいても、軽量のクラウド エージェントを数分でインストールすることで、ネットワークを保護する革新的な新しい方法が提供されます。

Qualys Cloud Agent (CA) に関する情報をすばやく入手できます。

ビデオチュートリアル

Cloud Agent Platform Introduction (2m 10s)

Getting Started Tutorial (6m 34s)

Installing MSI Based Package

Cloud Agent プラットフォームの可用性マトリックス

バージョンとモジュールを持つサポートされているクラウドエージェントの最新リストについては、 Qualys Cloud Platform については、次の記事を参照してください:
Cloud Agent Platform 可用性マトリックス

知っておくべきことがいくつかあります...

クラウドエージェントの要件

- ホストは、HTTPS ポート 443 経由で Qualys Cloud Platform (または Qualys Private Cloud Platform) に到達できる必要があります。Qualys Cloud Platform にログインし、[ヘルプ>について] に移動して、ホストがアクセスする必要がある URL を確認します。
- Cloud Agent for Windows をインストールするには、ホストに対するローカル管理者権限またはドメイン管理者権限が必要です。プロキシ構成がサポートされています。詳細については、「プロキシー構成」を参照してください。

ハードウェア要件

Cloud Agent Windows の場合、最小システム要件は次のとおりです：

知っておくべきことがいくつかあります...

- インベントリ、脆弱性管理(VM)、ポリシーコンプライアンス(PC)などのスキャンベースの機能用の 512MB の RAM。
- ファイル整合性監視 (FIM) とパッチ管理 (PM) 用の 1 GB の RAM。
- Endpoint Detection and Response (EDR) のシステム要件については、Qualys EDR オンボーディング ガイドを参照してください。
- 最低 200 MB の使用可能なディスク容量。

インストール手順は何ですか?

Cloud Agent UI では、ホストにエージェントをインストールする手順を順を追って説明します。エージェントをインストールしたら、エージェント構成ツールを使用してプロビジョニングする必要があります。

トラブルシューティングに関するヘルプ

次の場所にあるエージェントのログ ファイルを調べることをお勧めします。

C:¥ProgramData¥Qualys¥QualysAgent

XP および Server 2003 では、ログ ファイルは次の場所にあります。

C:¥Documents and Settings¥All Users¥Application Data¥Qualys¥QualysAgent

注: セキュリティ権限により、QualysAgent フォルダーに直接アクセスできない場合があります。QualysAgent フォルダーを別の場所にコピーして、ログ ファイルを調べます。

ログファイル

Cloud Agent は、モジュールごとに C:¥ProgramData¥Qualys¥QualysAgent¥Log ディレクトリ内に個別のログを作成します。

Cloud Agent(バージョン 4.5 以降)のインストールまたはアンインストール中に問題が発生した場合は、%ProgramData%/Qualys/QualysAgent フォルダの下にある次のログファイルを参照してください。

- CloudAgentInstaller.log ファイル
- MSI によって生成された MsiLog_TimeStamp.log ファイル

注: クラウドエージェントのログディレクトリ (%ProgramData%/Qualys/QualysAgent)またはログファイルにアクセスできない場合、ログファイルは C:¥Windows¥Logs¥QualysAgent に作成されます。

ログレベルの変更

レジストリ値を設定することで、エージェントのデバッグレベルのログを有効にすることができます。レジストリ キー - HKEY_LOCAL_MACHINE¥SOFTWARE¥Qualys¥QualysAgent¥Logs で、次の値を持つエントリを作成します。

- データ型 - DWORD (32 ビット)
- 値名 - TraceLevel

- 値データ – 6

Cloud Agent サービスを再起動して、エージェントがすべてのログファイルにデバッグメッセージのログを記録できるようにします。

注: レジストリキーに設定された値は、config.db ファイルの値よりも優先されます。

追加情報

トラブルシューティング

エラーメッセージ

インストール

Cloud Agent for Windows のインストールは簡単です。手順を簡単に説明します。

Qualys は、サポートされているオペレーティング システムごとにコーディングされたインストーラーとパッケージを提供します。あるプラットフォーム用にコーディングされたエージェントを別のプラットフォームで使用することはできません。SCCM、Intune、BigFix、rpm、Casper などのソフトウェア配布ツールを使用して、エージェントをターゲット・マシンにインストールできます。Cloud Agent は、VM テンプレートやクラウドプロバイダイメージ(Amazon AWS、Microsoft Azure、Google Compute Platform など)などのゴールドイメージにインストールできます。

Qualys Platform は、重複するエージェント ID の検出をサポートし、重複するエージェントを自動的に再プロビジョニングします。初期プロビジョニングを行わずにゴールドイメージにエージェントをインストールする方法については、 クローン作成/ゴールドイメージのためのクラウドエージェントの準備を参照してください。これは、資産レコードの重複を防ぐために推奨される方法です。

ソフトウェア配布ツールを使用している場合は、Qualys が提供するインストーラーを、特定のアクティベーション キーと顧客 ID 文字列とともにパッケージ化してください。エージェントのインストール時に、インストール環境はその特定のマシンのキー設定されるため、エージェントによってインストールされた成果物を独自のインストーラーにパッケージ化しないでください。これらのアーティファクトを含めると、プラットフォームが簡単に重複排除できない可能性のある重複が作成されます。

注意点 - 環境によっては、ネットワーク上のエージェント ホストと Qualys Cloud Platform 間の通信をサポートするための手順を実行する必要がある場合があります。

ヒントとおすすめの方法

Microsoft Windows の修正プログラムが必要

Microsoft Windows セキュリティ更新プログラムが必要

TLS バージョンが必要

エージェントインストーラをダウンロードする方法

ヒントとおすすめの方法

アクティベーションキーとは何ですか?

エージェントをインストールするには、エージェントのアクティベーションキーが必要です。これにより、エージェントをグループ化し、Qualys Cloud Platform を使用してサブスクリプションにバインドする方法が提供されます。さまざまなビジネス機能およびユーザに対して異なるキーを登録することができます。 **アクティベーションキーにアセットタグを追加する利点** アクティベーションキーに割り当てられたタグは、エージェントホストに自動的に割り当てられます。これは、エージェントの管理とエージェントホストに関するレポート作成に役立ちます。

エージェント インストーラーの実行

管理者特権のコマンド プロンプトからインストーラーを実行するか、システム管理ツールを使用する必要があります。

サブスクリプションでライセンスされているモジュール(脆弱性管理 (VM)、ポリシー コンプライアンス (PC)、ファイル整合性監視 (FIM)、エンドポイント検出と応答 (EDR)、パッチ管理 (PM)) をプロビジョニングするには、必ずエージェントをアクティブ化してください。モジュールのエージェントをアクティブ化すると、モジュールライセンスが消費されます。自動アクティベーションは、アクティベーションキーのモジュールを定義して設定することも、Cloud Agent UI で手動で行うこともできます。

アプリケーションのアクティベーションをスキップするとどうなりますか?エージェントは、インベントリ情報(IP アドレス、OS、DNS、NetBIOS 名、MAC アドレス、インストールされているソフトウェア)にのみ同期します。

インストールできるエージェントはいくつですか?

エージェントはいくつでもインストールできますが、製品モジュールのエージェントをアクティブ化できるのは、そのモジュールのライセンスを持っている場合のみです。Cloud Agent UI の [エージェント] タブには、インストールされているエージェントが表示されます。

エージェントが接続されていることを確認する

インストール されたエージェントは、Qualys クラウドプラットフォームとプロビジョニングとエージェントのステータスは [エージェント] タブで確認できます。 これはエージェントのチェックイン時に更新されます。エージェントにステータスがない場合は、クラウドプラットフォームに正常に接続されていないため、トラブルシューティングが必要です。

Qualys Cloud Agent サービスの既定のスタートアップの種類は何ですか?

Qualys Cloud Agent サービスの [スタートアップの種類] は [自動 (遅延開始)] に設定されています。

Microsoft Windows 修正プログラムが必要

Cloud Agent を実行し、古い Windows オペレーティング システムから Qualys Platform に接続するには、次の修正プログラムが必要です。

Hotfix	KB Article	Archive	Language	Platform
Windows XP SP3+ x86 SHA2 Cert Hotfix	968730	375554_ENU_i386_zip.exe	English	i386

Windows Server 2003 SP2+ x86 SHA2 Cert Hotfix	968730	375510_ENU_i386_zip.exe	English	i386
Windows XP SP3+ x64 & Windows Server 2003 SP2+ x64 SHA2 Cert Hotfix	968730	375531_ENU_x64_zip.exe	English	x64

注: アーカイブ名は将来変更される可能性があります。

これらの修正プログラムを入手するには、Microsoft サポートにお問い合わせください。

Microsoft Windows セキュリティ更新プログラムが必要

Windows セキュリティ更新プログラム KB4474419 Microsoft をインストールし、システムを再起動して、Windows 7 SP1 および Windows Server 2008 R2 SP1 および SP2 に Qualys Cloud Agent ドライバーを正常にロードします。

詳細については、 Microsoft サポート ドキュメントを参照してください。

TLS バージョンが必要

クライアントマシンで TLSv1.2 以降が有効になっていることを確認し、Qualys Cloud Platform と通信します。

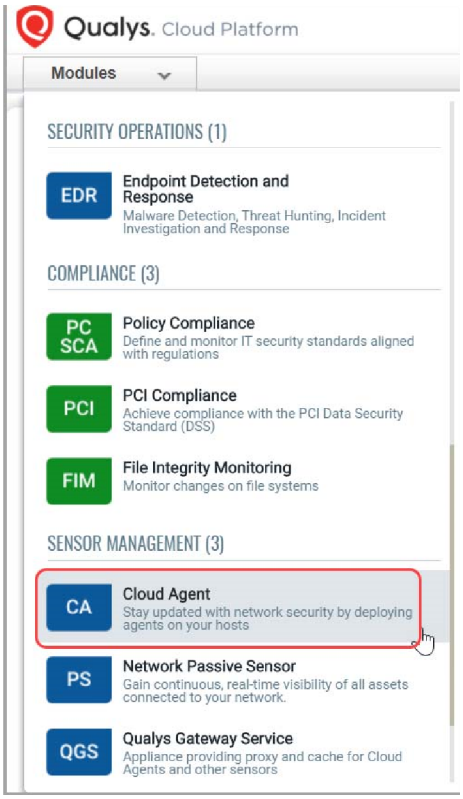
Cloud Agent for Windows は、Windows オペレーティング・システムによって提供される暗号化プロトコル・サポートを使用します。古い Windows オペレーティングシステム(Windows XP、Embedded Standard、Server 2003/SP2、Server 2008/SP1/SP2、および明示的に設定されている場合はその他のオペレーティングシステムを含む)では、Cloud Agent が使用するオペレーティングシステムで TLS 1.2 をサポートしていません。

詳細については、「TLSv1.0 および TLSv1.1 の非推奨」を参照してください。

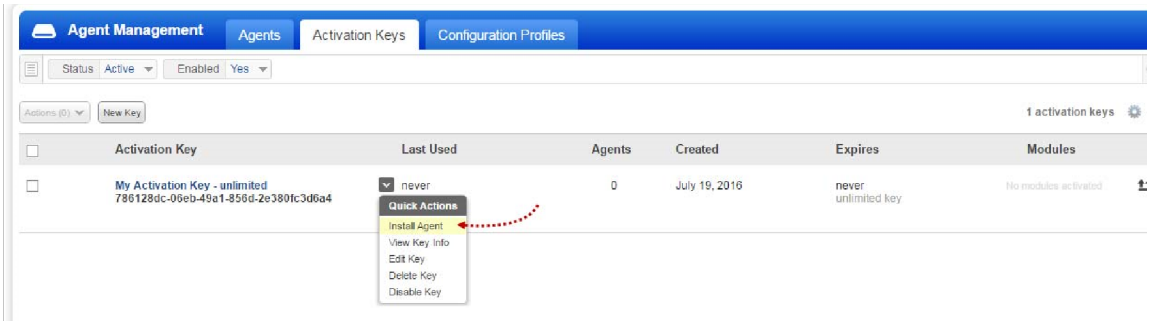
エージェントインストーラをダウンロードする方法

Qualys Cloud Platform からインストーラーをダウンロードし、関連するアクティベーション ID と顧客 ID を取得する方法は次のとおりです。

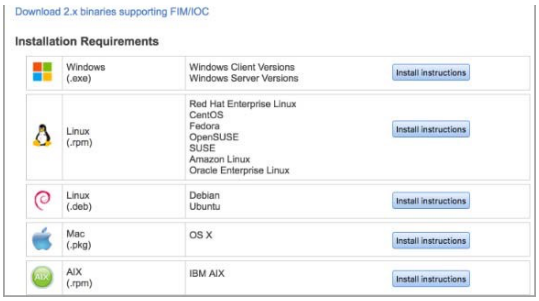
Qualys Cloud Platform にログインし、 Cloud Agent モジュールで [CA] を選択します。



アクティベーションキーを選択し(必要に応じて作成します)、 クイックアクションメニューからエージェントのインストールを選択します。



Windows(.exe)の横にある[インストール手順]をクリックします。



どうなるでしょうか?エージェントインストーラーがローカルシステムにダウンロードされ、UI に関連付けられたアクティベーションキーID とカスタマーID が表示されます - これをコピーして安全な場所に貼り付けると、手動またはソフトウェア配布ツールを使用してインストールを完了する必要があります。

注: GoldenImage パラメータを「True」として使用すると、エージェントが非実行状態でインストールされるため、HostID は生成されません。HostID の生成とプロビジョニングは、次回のエージェントの起動時に行われます。

exe ベースのパッケージのインストール手順

必要なもの

クラウドエージェントをインストールするには、クラウドエージェントインストーラをダウンロードし、関連する ActivationID と CustomerID を取得する必要があります。Qualys Cloud Platform にログインし、クラウド エージェント (CA) モジュールに移動し、Windows (.exe) のインストール手順に従うだけで、必要なものがすべて揃っています。

クラウドエージェントの要件

エージェントをインストールする手順

エージェントをインストールするホストに Qualys Cloud Agent インストーラーをコピーし、コマンドを実行するか、システム管理ツールを使用して、組織の標準プロセスに従ってエージェントをインストールし、ソフトウェアをインストールします。

> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

WebServiceUri=<platform_url>/CloudAgent/

Installation steps for msi based package

プロキシサポート付きエージェントをインストールする手順

デフォルトのプロキシ構成は、エージェントのインストール時に引数として指定できます。プロキシ パラメータは、Proxy 引数 (Proxy="<argument-to-pass>") を介して渡すことができます。proxy 引数には、プロキシ URL、対応するユーザー名、およびパスワードが含まれます。

QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <proxy url> /n

<proxy username> /p <proxy password>"

エージェントのインストール時に、セミコロンで区切られた複数のプロキシを引数として渡すこともできます。

QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <1st proxy url>;<2nd proxy url> /n <proxy username> /p <proxy password>"

Note: 複数のプロキシユーザー名とプロキシパスワードはサポートされていません。

ゴールデンイメージにエージェントをインストールする手順

インストール中に GoldenImage=true がパラメーターとして渡された場合、エージェントは非実行状態でインストールされるため、レジストリに HostID がありません。エージェントは、マシンの再起動後、またはエージェント サービスの手動起動後に開始され、その後、HostID がエージェントによって生成されます。

コマンドを実行するか、システム管理ツールを使用して、組織の標準プロセスに従ってゴールデンイメージにエージェントをインストールし、ソフトウェアをインストールします。

> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxxxxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ GoldenImage=true

For more information on deployment, see Cloud Agent Preparation for Cloning / Gold Image.

msi ベースのパッケージのインストール手順

必要なもの

クラウドエージェントをインストールするには、クラウドエージェントインストーラをダウンロードし、関連する ActivationID と CustomerID を取得する必要があります。Qualys Cloud Platform にログインし、クラウド エージェント (CA) モジュールに移動し、Windows (.exe) のインストール手順に従うだけで、必要なものがすべて揃っています。

クラウドエージェントの要件

MSI パッケージの抽出

ダウンロードした exe ファイルから MSI を抽出するには、次のコマンドを実行します。

QualysCloudAgent.exe 抽出 MSI=<値>

ExtractMSI の場合は、ホスト アーキテクチャに従って次の値 (値) を使用します。

たとえば、64 ビットマシンにクラウドエージェントをインストールする場合は、ExtractMSI=64 の値を持つ MSI パッケージを抽出する必要があります。

- **32**：32 ビット MSI インストーラを抽出
- **64**:64 ビット MSI インストーラを抽出

- **BOTH**: MSI インストーラの両方 (32 ビットと 64 ビット) を抽出します。
- **AUTO:** OS アーキテクチャに基づいて適切な MSI を抽出します。32 ビットマシンで 32 ビット MSI を抽出し、64 ビットマシンで 64 ビット MSI を抽出します

MSI ファイルは、利用可能な exe ファイルと同じディレクトリに抽出されます。

MSI パッケージのインストール

エージェントをインストールするホストに Qualys Cloud Agent インストーラーをコピーし、コマンドを実行するか、システム管理ツールを使用して、組織の標準プロセスに従ってエージェントをインストールし、ソフトウェアをインストールします。以下は、32 ビットインストーラ用の MSI パッケージをインストールするためのサンプルコマンドです。

Msiexec.exe /i CloudAgent_x86.msi CustomerId={12345678-1234-1234-

1234-123456789012} ActivationId={12345678-1234-1234-1234-

123456789012} WebServiceUri=<platform_url>/CloudAgent/

ここには CloudAgent_x86.msi 32 ビットインストーラ用の MSI ファイルを抽出したものです。

次に何が起こるか?

アセットデータのクラウドへの同期を開始します!

インストールされると、エージェントは Qualys Cloud Platform に接続し、それ自体をプロビジョニングします。エージェントは、関連する構成プロファイルをダウンロードし (定義された設定に従い)、アクティブ化されたモジュールのマニフェストをダウンロードし、Qualys Cloud Platform に送信する各モジュールのアセット メタデータの収集を開始します。

あなたも興味があるかもしれません...

プロキシー構成

証明書のサポート

アンチウイルスと HIPS の除外

証明書のサポート

Qualys Cloud Platform 認定では SHA-256 が使用されます。Windows XP と Windows Server 2003 には、既定で SHA2 サポートは含まれていません。そのため、これらのシステムに SHA2 修正プログラムをインストールする必要があり、インストールしないと認定が失敗します。「Microsoft Windows の修正プログラムが必要」セクションを確認します。

詳細については、SHA-256 サポートに関する Microsoft サポート技術情報の記事を参照してください。

Windows 7 SP1 および Windows Server 2008 R2 SP1 および SP2 に Qualys Cloud Agent ドライバーを読み込むには、Microsoft Windows セキュリティ更新プログラムが必要です。Microsoft Windows セキュリティ更新プログラムが必要セクションを確認します。

証明書の更新

DigiCert は、以前のバージョンとは異なる認証局 (CA) で署名されたタイムスタンプ用の新しい証明書を提供しています。新しい CA 名は「DigiCert Trusted Root G4」です。

エラーが発生した場合 - 「エラー: パッチ: PE バイナリファイルの署名を検証できませんでした...statusHandler.dll」の場合は、「DigiCert Trusted Root G4」証明書が信頼できるルート証明機関で使用可能であることを確認します。

証明書が使用できない場合は、次のいずれかの方法を使用して証明書を更新します :

- Active Directory の使用 - Active Directory を使用して証明書を更新するには、「証明書リンクを使用してグループ ポリシーを使用してクライアント コンピューターに証明書を配布する」で詳しく説明されている手順に従います。

- 手動更新- インターネットに接続している場合は、次のコマンドを使用して証明書を手動で更新します：

certutil -urlcache -f

http://cacerts.digicert.com/DigiCertTrustedRootG4.crt DigiCertTrustedRootG4.crt
certutil -addstore -f root DigiCertTrustedRootG4.crt

アンチウイルスと HIPS の除外

ウイルス対策、EDR、または HIPS ソフトウェアがインストールされていますか?Cloud Agent との競合を回避するには、システムにインストールされているすべてのセキュリティソフトウェアから次のファイル、ディレクトリ、およびプロセスを除外してください。

エージェントプロセス

QualysAgent.exe - これは Qualys エンドポイント サービスです

QualysCloudAgent.exe - MSI 以外のインストーラーは、ディスクとレジストリの場所にアクセスする必要があります (以下を参照)

uninstall.exe - これは Qualys エンドポイント サービスのアンインストーラーです - 次のディスクとレジストリの場所への r/w/d アクセスが必要です。

アンチウイルスと HIPS の除外

QualysSPConfig.exe - Qualys Cloud Agent Self Protection Configuration Utility。自己保護を無効にするために使用します。

QualysProxy.exe - Qualys プロキシ構成ツール。Qualys Cloud Agent のプロキシ設定を構成するために使用されます。

QualysAgentUI.exe – パッチ管理プロンプト/UI を表示するために使用される実行可能ファイル。

Program Files¥Qualys¥QualysAgent の下のプロセスでは、エージェントで Qualys File Integrity Monitoring がアクティブになっている場合、Qualys FIM ドライバーをロードおよびアンロードできます。

実行可能ファイルとプロセス

%ProgramData%¥Qualys¥QualysAgent¥PatchManagement¥Resources¥ - Various Patch Management executables.

%ProgramFiles%¥Qualys¥QualysAgent¥EDR¥ - Driver Management Utilities.

%ProgramData%¥Qualys¥SandboxRO¥agentid-service.exe – Agent Scan Merge executable.

%ProgramData%¥Qualys¥QualysAgent¥ LogCollector¥Resources¥qualys-beat_x86_64.exe - XDR executable for 64-bit.

%ProgramData%¥Qualys¥QualysAgent¥ LogCollector¥Resources¥qualys-beat_x86.exe - XDR executable for 32-bit.

%ProgramData%¥Qualys¥QualysAgent¥SwCA¥Resources¥SwCAScanner.exe-Scanner executable for Software Composition Analysis.

%ProgramData%¥Qualys¥QualysAgent¥QCAPS¥Resources¥qcaps.exe - Cloud Agent Passive Sensor.

File

%ProgramData%¥Qualys¥QualysAgent - we read/write/create/delete files in this directory and sub-directories

%ProgramFiles%¥Qualys¥QualysAgent - this is where the service and uninstall are installed. The service will create processes so AV/EDR/HIPS needs to make sure to unblock this action.This path is same for both x86 and x64-bit systems.

Registry

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥QualysAgent - this is where the agent setup installs the service into the system.

HKEY_LOCAL_MACHINE¥SOFTWARE¥Qualys - this is where breadcrumb information lives to merge agent and appliance scanner results. The agent needs c/r/w/d access here; setup needs to create the key; uninstall needs ability to delete the key.

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥qmon - this is where the agent setup installs the driver into the system if Qualys File Integrity Monitoring (FIM) is activated or Self-protection is enabled or Qualys EDR is activated on the agent.

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥qnetmon - this is where the agent setup installs the driver into the system if Qualys EDR is activated on the agent.

Upgrading the Cloud Agent

QualysAgent.exe

必要に応じて CreateProcess を呼び出して外部プロセスを起動します。

CoCreateInstance を呼び出して COM オブジェクトをインスタンス化します。

ProgramData ディレクトリからファイルを作成/読み取り/書き込み/削除します。

hklm¥software¥qualys レジストリ キーから作成/読み取り/書き込み/削除します。

すべてのファイルとレジストリの場所を列挙して読み取ります 。

クラウドエージェントのアップグレード

Qualys プラットフォームを使用すると、構成プロファイルの設定に応じて、エージェントがプラットフォームにチェックインするときに、エージェントを新しいバージョンにアップグレードできます。

ソフトウェア配布ツールは、すでにインストールされているエージェントが自動アップグレード用に構成されていないため、新しいバージョンのクラウドエージェントインストーラをパッケージ化できます。

Windows クラウド エージェント インストーラーは、インストールされたエージェントのプレース アップグレードを可能にするコマンド ライン引数 ("PatchInstall") をサポートし、エージェントの UUID、顧客 ID、およびアクティブ化キー構成をシステム上に保持します。

***必須**: ソフトウェア配布ツールでは、特定のコマンドライン引数を使用して、既存のインストール済み Windows エージェントをアップグレードする必要があります。特定のコマンドライン引数が使用されない場合、インストーラは既存のインストール済み Windows エージェントのアップグレードに失敗します。

exe ベースのインストーラーの場合:

QualysCloudAgent.exe PatchInstall=TRUE

MSI ベースのインストーラーの場合:

Msiexec.exe /i CloudAgent_x86.msi Patchinstall=true

注: "patchinstall" 引数を使用する場合は、Customer ID または Activation Key 引数を追加しないでください。 **セルフパッチについて** Cloud Agent は、セルフパッチによって自動的にアップグレードされます。セルフパッチ適用を成功させるには、ホストがエージェントバイナリの署名に使用されるパブリックルート証明書を受け取るために、Cloud Agent が次の失効サーバにアクセスする必要があります：

http://ctldl.windowsupdate.com/
http://rb.symcd.com/
http://rb.symcb.com/

注: これは、2.0.2 - 2.0.6 から 2.1.x にアップグレードするエージェントにのみ必要です。

クラウドエージェントのアンインストール

クラウドエージェントのアンインストール

Cloud Agent モジュールの UI または API からのエージェントのアンインストール

Cloud Agent モジュールのユーザーインターフェイスまたは Cloud Agent API を使用して Cloud Agent をアンインストールすると、エージェント、そのアセットレコード、

アクティブ化されたモジュールのライセンス、および関連するデータと評価結果が Qualys サブスクリプションから削除されます。

Qualys Platform にチェックインするエージェントは、システムからローカルにアンインストールされます (サービス、

プログラム ファイル、およびプログラム データ) ですが、レジストリ エントリはエージェント ホスト ID (エージェント UUID)、アクティベーション キー、カスタマー ID、およびその他のレジストリ キーとともに保持されます。これにより、エージェントが同じ資産に再インストールされた場合に同じエージェントのパーソナリティを維持し、認証されたスキャンのエージェントレス追跡をサポートできます。

ホスト自体からのエージェントのアンインストール

アンインストール・ユーティリティを使用してホスト自体からクラウド・エージェントをアンインストールすると、エージェント、そのライセンス使用状況、およびスキャン結果は Qualys Platform サブスクリプションに引き続き存在します。

システム(サービス、プログラムファイル、およびプログラムデータ)からローカルにアンインストールすると、エージェントホスト ID(エージェント UUID)、アクティベーションキー、カスタマーID、およびその他のレジストリキーを含むレジストリエントリが保持されます。これにより、エージェントが同じ資産に再インストールされた場合に同じエージェントのパーソナリティを維持し、認証されたスキャンのエージェントレス追跡をサポートできます。

exe および/または MSI ベースのインストーラーの場合:

Uninstall.exe Uninstall=True

MSI ベースのインストーラーの場合:

Msiexec.exe /x CloudAgent_x86.msi

アンインストール中は、Customer ID と Activation Key の引数を使用しないでください。

エージェントのアセットレコード、ライセンス、および評価結果をプラットフォームから削除するには、Cloud Agent モジュールのユーザーインターフェースまたは Cloud

Agent API を使用してエージェントをアンインストールします。これは、エージェントがローカルシステムからアンインストールされた後に実行できます。

注: アンインストールの一部として Qualys ディレクトリを削除するには、Uninstall.exe プログラムを Qualys ディレクトリの外部から呼び出す必要があります。

クリーンアンインストール

デフォルトのアンインストール動作では、エージェントの UUID、カスタマーID、およびアクティベーションキーがシステムに保持されます。これは、新しいエージェントのインストールで元のエージェント UUID を再利用するため、プラットフォーム内でそのアセットのライフサイクルが一貫しています。また、エージェントレス追跡に対して認証スキャンが有効になっていて、UUID を保持する必要がある場合。

Windows クラウド エージェント インストーラーは、エージェント UUID、顧客 ID、およびライセンス認証キーをシステムから削除する必要がある場合に備えて、クリーンアンインストール機能をサポートしています。インストーラに次の引数を指定します。

Uninstall.exe Uninstall=True Force=True

クリーンアンインストールが実行されたシステムにエージェントをインストールすると、そのシステムに新しいエージェント UUID が作成され、Cloud Agent UI または API の [アンインストール] アクションを使用して元のホストレコードが削除されなかった場合、プラットフォームに重複するホストレコードが作成される可能性があります。

注: アンインストールの一部として Qualys ディレクトリを削除するには、Uninstall.exe プログラムを Qualys ディレクトリの外部から呼び出す必要があります。

クリーンアンインストールエージェントコマンドの例

"%programfiles%¥qualys¥qualysagent¥uninstall.exe" Uninstall=True Force=True

クラウドエージェントの Qualys 自己保護機能

Cloud Agent の Qualys 自己保護機能により、信頼できないプロセスが Cloud Agent に不要な変更を加えるのを防ぎます。

自己保護機能により、次のことが防止されます。

- クラウドエージェントのアンインストール。
- クラウドエージェントプロセスの終了。
- Cloud Agent ファイルとディレクトリの改ざん - 上書き、削除、名前変更、変更、メモリ マッピング。
- Cloud Agent ドライバーの改ざん - ドライバーのアンロードまたはデタッチ。
- クラウドエージェントレジストリキーの改ざん:
    - レジストリ キーと値の上書き、削除、および変更
    - レジストリ キーの名前変更
- デバッガーが Qualys エージェント サービスに接続されないようにします。
- ユーザー定義のスクリプト、つまりカスタム評価と修復 (CAR) とパッチ管理によってアップロードされたスクリプトが保護領域に変更を加えないようにします。

この機能は、デフォルトでは有効になっていません。Cloud Agent の Qualys 自己保護を有効にするには、Qualys の担当者にお問い合わせください。

注: Qualys の自己保護機能は、Windows 7 以降のオペレーティング システムでのみ使用できます。

自己保護の無効化

ログファイルなどのデバッグに必要なエージェントデータアーティファクトにアクセスするには、Cloud Agent の自己保護を無効にする必要があります。

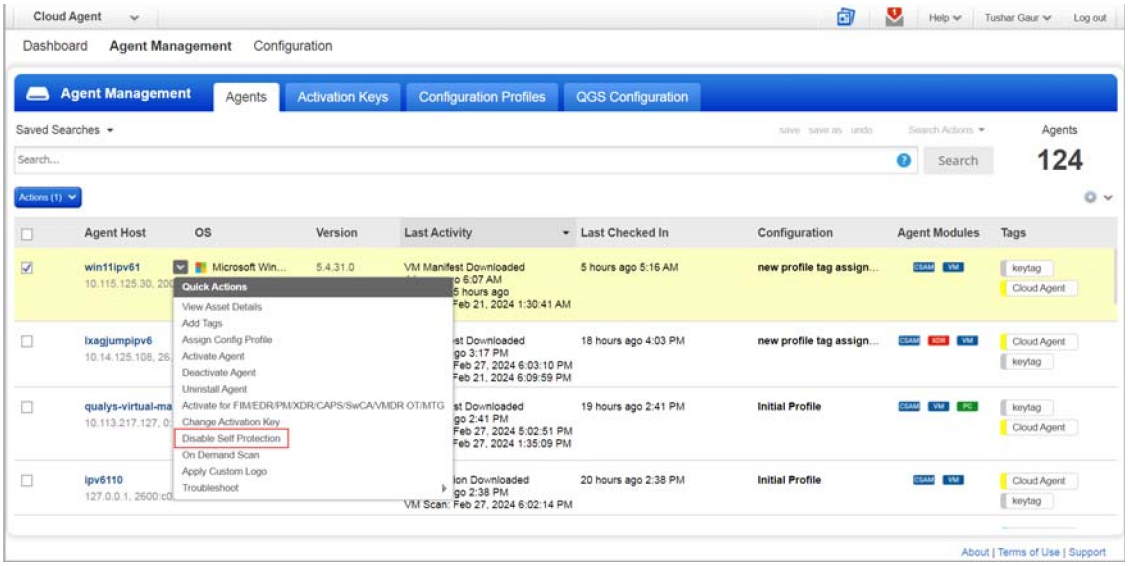
エージェントの自己保護を無効にするには、キーを生成する必要があります。デフォルトでは、自己保護を無効にするキーの有効期間は 1 日 (24 時間) です。ただし、要件に応じて構成できます。トラブルシューティングオプションを使用して、クラウドエージェントの自己保護を無効にすることもできます。

注: CA Manager ロールを持つユーザのみが、クラウド エージェントの自己保護を無効にするキーを生成できます。

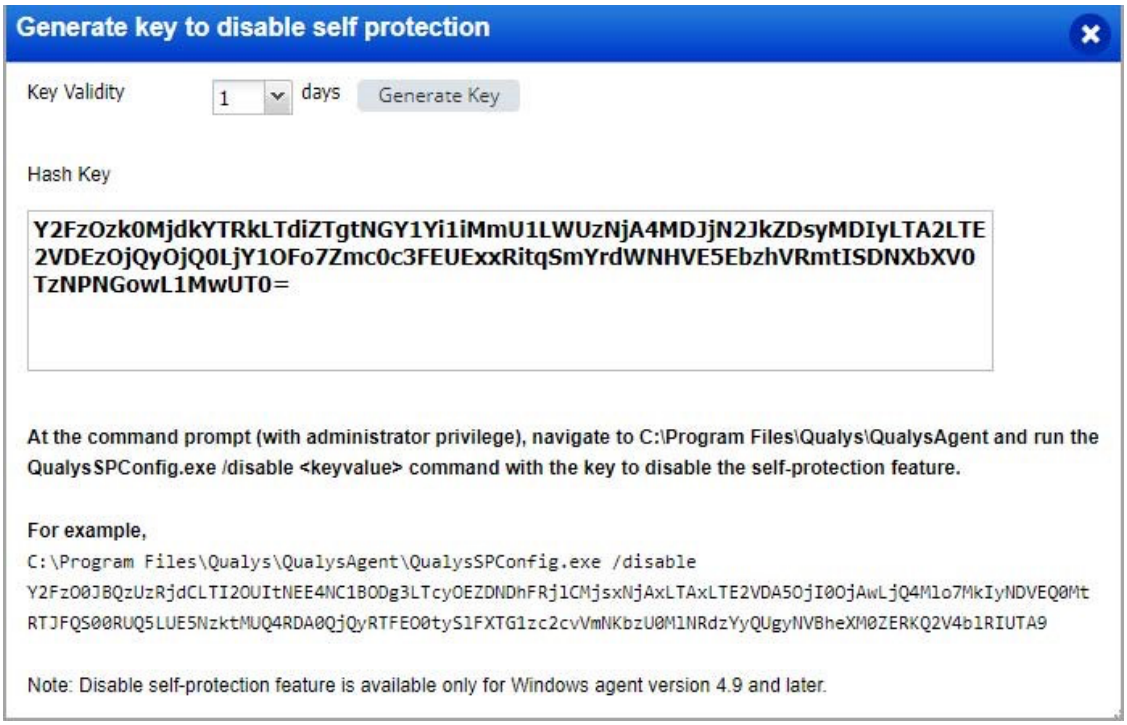
クラウドエージェントの自己保護を無効にする手順

クラウドエージェントの自己保護を無効にするには:

- Cloud Agent アプリケーションを開きます。
- [エージェント管理] > [エージェント] に移動し 、自己保護を無効にするインストール済みのクラウドエージェントを選択します。
- [クイック アクション] メニューで、[自己保護を無効にする] をクリックします。



- [自己保護を無効にするためのキーの生成] 画面で 、[キーの生成] をクリックし、プロセスに従ってそのエージェントの自己保護を無効にします。



注: Cloud Agent の自己保護を無効にするこのオプションは、Qualys Cloud Agent for Windows バージョン 5 以降で使用できます。

セルフプロテクションを使用したクラウドエージェントのアンインストール

以下は、自己保護を有効にしてクラウドエージェントをアンインストールするコマンドです。これらのコマンドを使用すると、エージェントホスト自体から Cloud をアンインストールできます。

- EXE および MSI ベースのエージェント インストーラ パッケージの場合

  Uninstall.exe Uninstall=True SPFKEY=Hash Key

- EXE および MSI ベースのエージェント インストーラ パッケージの場合

  Msiexec.exe /x CloudAgent_x86.msi SPFKEY=Hash Key

注: クラウドエージェントの自己保護を無効にするためのハッシュキーは、クラウドエージェント UI で使用可能な「自己保護を無効にする」オプションを使用して生成する必要があります。

クラウドエージェントヘルスチェックツール

Cloud Agent ローカルヘルスチェックツールは、特定のホスト上の Qualys エージェントのヘルスを評価します。このツールは、Windows プラットフォーム用のクラウド エージェント セットアップで使用できます。このツールは独立して実行され、パラメータは必要ありません。

QualysAgentHealthCheck.exe は、

C:¥ProgramFiles¥QualysAgent¥Qualys ディレクトリにあります。

次のコマンドを使用して、Qualys エージェントのヘルスチェックツールを実行します。

"%programfiles%¥qualys¥qualysagent¥QualysAgentHealthCheck.exe"

注: このツールは、Qualys Cloud Agent for Windows 5.5 で使用できます。

エージェントのヘルスステータス評価

このツールは、インストール状況、通信状態、アプリケーション機能に基づいて、クラウドエージェントの全体的な正常性状態を評価します。ヘルスステータスについて評価されるアプリケーションは、脆弱性管理 (VM)、ポリシーコンプライアンス (PC)、セキュリティ構成評価 (SCA)、およびパッチ管理 (PM) です。

- エージェントの通信の正常性は、プロキシ設定と Qualys Server エンドポイントへの接続に基づいて評価されます。
- スキャンベースのアプリケーションの正常性は、スキャン間隔、アップロード間隔、および最終スキャン/最終アップロード時間に基づいて評価されます。
- パッチ管理の正常性の場合、ツールは指定された URL からパッチのダウンロードを開始し、ファイルハッシュを検証します。パッチのダウンロードに失敗すると、パッチの健全性は不良としてフラグが立てられます。ただし、パッチが正常にダウ

ンロードされたが検証に失敗した場合、パッチ管理の正常性には影響しません。代わりに、パッチ検証の失敗を示すエントリが JSON のエラーセクションに記録されます。

エージェントのヘルスステータスレポート

エージェントの正常性ステータスツールは、コンソール出力、わかりやすいテキストの概要、および詳細な JSON レポートを提供します。テキストレポートと JSON レポートは、ツールが実行されるのと同じディレクトリにある HealthCheck ディレクトリに生成されます。

ヘルスステータスと説明

次の表に、正常性の状態と説明を示します。

ヘルスステータス	**説明**
Good	エージェントヘルス状態は Good
Bad	エージェントに通信の問題が発生しているか、エージェント サービスがダウンしているか、いずれのアプリケーションも正常に機能していません。
Poor	Qualys エージェントの一部のアプリケーションは正常に機能しています。
Not Installed	Qualys エージェントが資産にインストールされていません。
Not Provisioned	Qualsy Agent はインストールされているがプロビジョニングされていません。
Tool Error	Agent Health Status ツールは Agent Health チェック中にクリティカルなエラーが発生に遭遇しました。

ヘルスチェックレポートの例

次のレポートは、レポートで強調表示されているように、パッチ管理アプリケーションの正常性の結果として、エージェントの全体的な正常性が「不良」であることを示しています。

テキストレポートの例:

```
**********************************************************************************************
Performing Health Checks
**********************************************************************************************
CoreHealthCheck 1 : Verifying if the Qualys agent is installed on your system.
CoreHealthCheck 2 : Retrieving information about qualys services currently running on your system.
CoreHealthCheck 3 : Retrieving information about qualys processes currently running on your system.
CoreHealthCheck 4 : Retrieving certificate information
CoreHealthCheck 5 : Retrieving proxy details
CoreHealthCheck 6 : Assessing connectivity to the backend system.
CoreHealthCheck 7 : Retrieving information about Agent communication.
CoreHealthCheck 8 : Gathering details about Qualys modules installed on the system.
CoreHealthCheck 9 : Assessing patch connectivity.

Evaluating overall health of the system.

**********************************************************************************************
Qualys Agent Local Health Check Tool Report :
**********************************************************************************************

Overall Health : Poor

Services :

      Name : qualysagent
      State : Running

Certificates :

      Name : DigiCert Global Root CA
      Installed : true

Agent Communication Details :

      Last CAPI : 2024-01-24 17:16:38.489
      CAPI Interval : 900

Backend Connectivity :

      Direct Connection :
            URL : https://qagpublic.p01.eng.sjc01.qualys.com/status
            Connection Succeeded : true

Modules :

      Name : Vulnerability
      Module Type : Scan based
      State : Ready for Scan
      Enabled : true
      Last Scan Time : 2024-01-24 15:38:44.889
      Scan Interval : 14400
      Next Scan Time : 2024-01-24 19:38:44
      VM Scan Deadline : 2024-01-26 19:38:44
      Module Health : Vulnerability Health Good

      Name : PolicyCompliance
      Module Type : Scan based
      State : Ready for Scan
      Enabled : true
      Last Scan Time : 2024-01-24 15:46:04.224
      Scan Interval : 14400
      Next Scan Time : 2024-01-24 19:46:04
      PC Scan Deadline : 2024-01-26 19:46:04
      Module Health : PolicyCompliance Health Good

      Name : SCA
      Module Type : Scan based
      Enabled : false

      Name : Patch Management
      Module Type : Realtime
      Enabled : true
      Patch Connectivity :
            Direct Connection :
                  URL : https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.5/npp.8.5.Installer.x64.exe
                  Connection Succeeded : false
      Module Health : Patch Management Health Bad

Errors :

      Severity : CRITICAL
      Win32 Error Code : 12002
      Error Description : Patch Webrequest [Direct Connection] failed for https://github.com/notepad-plus-plus/notepad-plus-
plus/releases/download/v8.5/npp.8.5.Installer.x64.exe(winhttp code: 12002), The request has timed out"

Detailed Report Location : C:\Program Files\Qualys\QualysAgent\HealthCheck\qualys_agent_health_check_124225725.json
Concise Text Report Location : C:\Program Files\Qualys\QualysAgent\HealthCheck\qualys_agent_health_check_124225725.txt
```

JSON レポートの例:


```
{
  "OverallHealth": "Poor",
  "Timestamp": "2024-01-24T17:27:25Z",
  "ToolVersion": "5.4.36.1",
  "JSONSchemaVersion": "1.0",
  "FreeDiskSpaceInMB": 1298,
  "CustomerID": "{3C59A6A1-51E6-75B4-81FD-BFFD25CDCCFA}",
  "AgentID": "{94792BDB-A522-4E2F-8B1C-0B79DEA4E13D}",
  "ActivationID": "{F635D621-1FC4-4C70-B964-ACA13AAE642C}",
  "ConfigID": "{6E057275-2293-4634-B7AB-50A27B64FCFA}",
  "QGSEnabled": false,
  "CloudProvider": "Auto",
  "Provisioned": true,
  "QualysAgentPerformanceCounters": {
    "CPUUsageInMilliseconds": 1426859,
    "RAMUsageInMB": {
      "WorkingSet": 38,
      "PrivateUsage": 41,
      "PeakWorkingSet": 110
    },
    "ProgramDataSpaceUsageInMB": 671,
    "ProgramFilesSpaceUsageInMB": 611
  },
  "QualysDrivers": [
    {
      "Name": "qmon",
      "State": "Running",
      "Version": "5.3.0.0"
    },
    {
      "Name": "qnetmon",
      "State": "Running",
      "Version": "5.1.0.0"
    }
  ],
  "ProxyDetails": {
    "ProxyUrls": null,
    "PacFilePath": null,
    "DirectAttemptEnabled": true,
    "WinHttpEnabled": true,
    "WPADEnabled": true
  },
  [redacted]
  ],
    {
      "Name": "Patch Management",
      "Enabled": true,
      "ModuleHealth": "Patch Management Health Bad",
      "PatchCommunicationDetails": [
        {
          "VendorUrl": "https://github.com/notepad-plus-
plus/notepad-plus-
plus/releases/download/v8.5/npp.8.5.Installer.x64.exe",
          "Proxyresolution": "NoResolution",
          "Proxyused": false,
          "Timetocompleteinseconds": 21.0931034,
          "Win32errorcode": 12002,
          "Connectionsucceeded": false
        }
      ]
    }
  ],
  "ErrorMessages": [
    {
      "ErrorCode": 87,
      "Severity": "INFO",
      "ErrorDescription": "No Proxy set hence skipping proxy
test",
      "DiagnosticChecks": [
        "Tool does not contain diagnostic steps for this error"
      ]
    },
    {
      "ErrorCode": 12002,
      "Severity": "CRITICAL",
      "ErrorDescription": "Patch Webrequest [Direct Connection]
failed for https://github.com/notepad-plus-plus/notepad-plus-
plus/releases/download/v8.5/npp.8.5.Installer.x64.exe(winhttp
code: 12002), The request has timed out\"",
      "DiagnosticChecks": [
        "Tool does not contain diagnostic steps for this error"
      ]
    }
  ]
}
```

プロキシ構成

Qualys Cloud Platform と通信するには、クライアント マシンで TLS 1.2 を有効にする必要があります。 TLS 1.2 は、より安全なプロトコルです。 TLS 1.2 を有効にすることが不可能な場合は、受信通信を TLS 1.2 プロトコルに変換できるプロキシ サーバーを介して通信を実行してから、Qualys Cloud Platform に送信する必要があります。

Cloud Agent Windows プロキシ設定は、Qualys レジストリ ハイブに保存されるか、Qualys レジストリ ハイブに保存されている PAC ファイルの URL を参照するか、システムが WPAD を使用するように構成されているかどうかが判断されます。

ソフトウェア配布ツールまたはシステム管理ツールでは、エージェントのインストール時またはエージェントのインストール後にエージェントのプロキシ構成を設定できます。

QualysProxy.exe クラウドエージェントとともにインストールされたコンパニオンユーティリティは、オプションでソフトウェア配布ツール、システム管理、または手動でエージェントのプロキシ構成を設定するために使用できます。 QualysProxy.exe ユーティリティは、プロキシ構成の設定中に必要なプロキシ認証資格情報を暗号化する唯一の方法です。

QualysProxy では、次のことができます。

- プロキシサーバーとポートを構成する
- プロキシのユーザー名とパスワードの資格情報を構成する
- WPAD が使用できない場合の PAC ファイル URL の構成
- WPAD 検出の有効化/無効化注

注 : プロキシ接続が失敗した場合、エージェントは直接接続のアウトバウンド (フェイルオープン) を試みます。

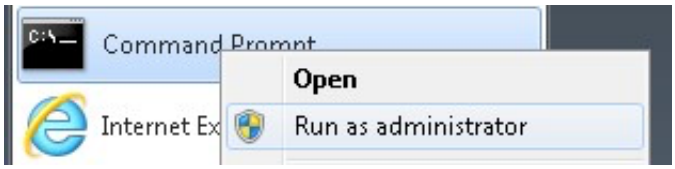
知っておくべきことは何ですか?

インストールについて QualysProxy ツールとプロキシ ツールの更新は、クラウド エージェントのインストールとともにインストールされ、クラウド エージェントのバージョ

ンがアップグレードされると必要に応じて更新されます。Qualys プロキシは、次の場所にあります。

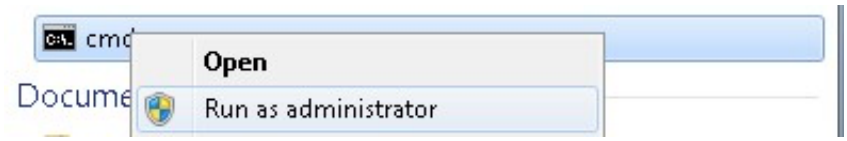
C:¥Program Files¥Qualys¥QualysAgent¥QualysProxy.exe

管理者特権のプロンプトから実行　プロキシ ツールは、管理者特権のコマンド プロンプトからコマンド プロンプトのスタート メニュー項目を右クリックして実行する必要があります。



QualysProxy syntax

…または、検索/実行スタートメニューの編集コントロールに cmd と入力し、cmd.exe メニュー項目を右クリックします。



システム管理ソフトウェアとリモートレジストリ管理を使用して、プロキシサーバーを設定できます。QualysProxy.exe コマンドラインインターフェイス (CLI) ツールは、システム管理ソフトウェアによって実行されるシェルスクリプトで使用するように設計されています。ツールの実行が完了すると、成功すると ERROR_LEVEL が 0 (ゼロ) に設定され、エラーが 0 以外に設定されます。[ユーザー インターフェイス] ウィンドウはユーザーに表示されません。

プロキシ ツールを介して行われた変更は自動的に行われるため、エージェント サービスを再起動する必要はありません。変更は、エージェントの log.txt ファイルを調べることで確認できます。

```
C:\ProgramData\Qualys\QualysAgent
```

XP および Windows Server 2003 では、エージェントの log.txt ファイルは次の場所にあります。

C:¥Documents and Settings¥All Users¥Application Data¥Qualys¥QualysAgent

エージェントがクラウドとの通信を試みるたびに、すべての接続エラーがログに記録され、プロキシ構成がアーカイブされます。

QualysProxy 構文

QualysProxy [/u <proxy url> [/n <proxy username>] [/p <proxy password] [/a <PAC file url>]]

QualysProxy [/w on|off]

QualysProxy [/d]

QualysProxy [/h on|off]

QualysProxy [/c] QualysProxy [/t on|off]

オプション	説明
/u	プロキシ URL。設定されている場合は、/x オプションを設定しないでください。
/n	プロキシへのアクセスに使用されるユーザー名。設定する場合は、/u オプションを設定する必要があります。
/p	プロキシへのアクセスに使用されるパスワード。設定する場合は、/u オプションを設定する必要があります。
/a	プロキシ自動設定用の PAC ファイルへの URL パス。設定されている場合は、/u オプションを設定しないでください。
/d	すべての Qualys クラウド エージェント プロキシ設定を削除します。 注: このオプションでは、システムのプロキシ設定や Web プロキシ自動検出 (WPAD) の設定は変更されません。

/w	ホストの WPAD 設定のエージェントの使用を有効または無効にします。
/h	システム全体の winhttp(s) プロキシ設定のエージェントの使用を有効または無効にします。
/c	現在の Qualys クラウド エージェント プロキシ設定を出力します。
/t	すべてのプロキシ サーバーに障害が発生した後、Qualys Cloud Platform への直接接続を有効または無効にします。デフォルトでは、プロキシ障害後の直接接続が有効になっています。

注：

- 引数にスペースが含まれている場合は、その引数を引用符で囲んでください。
- 引数に " 文字が含まれている場合は、その文字の前に円記号 '¥' を付けます。

プロキシ URL ファイルと PAC ファイルでの複数のプロキシ サーバーのサポート (Windows エージェント 3.1 以降)

クラウドエージェントは、プロキシ URL と PAC ファイルで定義された複数のプロキシサーバーをサポートしています。Cloud Agent は、接続にリスト内の最初のプロキシー・サーバーを使用し、接続に失敗した場合、エージェントは、すべてのプロキシー・サーバーが試行されるまで、リスト内の次に構成されたプロキシー・サーバーを順番に使用します。すべてのプロキシ サーバーが試行されると、Cloud Agent for Windows はプロキシ サーバー構成をバイパスする直接接続を使用して、Qualys プラットフォームに直接接続します。

クラウドエージェントは、Qualys プラットフォームに接続するたびに、常に順序付きリストの最初のプロキシサーバーを使用します。エージェントは、最後に使用されたプロキシー・サーバーの履歴を保持しません。

このプロキシ構成は、Qualys Gateway Service またはサードパーティのプロキシ サーバーで使用できます。フェイルオーバー・プロキシー・サーバーが最初のプロキシー・

サーバーと同じサブネット上にある必要はありません。クラウド・エージェントが他のサブネット上でも他のプロキシ・サーバーに接続できる限り、最初のプロキシ・サーバーが使用できない場合、エージェントはそれらのプロキシ・サーバーを使用します。

セミコロンで区切られた値を使用して、プロキシ URL で複数のプロキシ サーバーを定義します。PAC ファイルについては、複数のプロキシ サーバーを構成する方法を定義する PAC ファイル ベンダーのドキュメントを参照してください。

ユースケース

注: デフォルトでは、アプライアンスでキャッシュまたはパッチモードが有効になっている場合、Qualys Gateway Service (QGS) を介して接続するクラウドエージェントはキャッシュポートを使用する必要があります。キャッシュまたはパッチモードが有効になっていない場合、QGS キャッシュは使用できません。

例 1 – プロキシとポート番号を設定する

次の例は、プロキシとポート番号を設定する方法を示しています。

1. http 接続を使用する任意の HTTP_CONNECT プロキシ

   QualysProxy /u http://my-proxy:8080

2. http 接続を使用する QGS キャッシュポート

   QualysProxy /u http://my-qgs:8080

例 2 - フェイルオーバーに使用する複数のプロキシー・サーバーを定義する

次の例は、プロキシー番号とポート番号を設定する方法を示しています。

a) http 接続を使用する任意の 2 つの HTTP_CONNECT プロキシ

   QualysProxy /u http://my-proxy-1:8080;http://my-proxy-2:8080

b) http 接続を使用する任意の 2 つの QGS アプライアンスキャッシュポート

   QualysProxy /u http://my-qgs-1:8080;http://my-qgs-2:8080

例 3 - フェイルオーバー用に同じプロキシー・サーバー上に複数のポートを定義する

これは、単一の Qualys Gateway アプライアンスでキャッシュポートを最初に使用し、プロキシポートを 2 番目に(フェイルオーバーとして)使用するようにクラウドエージェントを設定するためにも使用できます。

次の例は、同じプロキシ サーバーに異なるポート番号を設定する方法を示しています。

a) Any HTTP_CONNECT proxy using http connection

QualysProxy /u http://my-proxy:8080;http://my-proxy:1080

b) QGS using cache port using http connection, then proxy port using http connectionQualysProxy /u http://my-qgs:8080;http://my-qgs:1080

例 4 – プロキシと資格情報を設定する

次の例は、プロキシ (デフォルト ポート: xxx) とプロキシ資格情報を設定する方法を示しています。

a) http 接続を使用する任意の HTTP_CONNECT プロキシ

QualysProxy /u http://my-proxy /n ProxyUsername /p ProxyPassword

例 5 – PAC ファイルを使用するようにエージェントに指示する

次の例は、WPAD 経由で検出できない場合に PAC ファイルを直接使用するようにクラウド エージェントに指示する方法を示しています (PAC ファイル プロキシが http 接続を使用していると仮定します)。

QualysProxy /http://my-pac-file-server/QualysAgent.pac

例 6 – PAC ファイルで使用する資格情報の指定

次の例は、PAC ファイルで使用する資格情報を指定する方法を示しています。資格情報は、結果のプロキシ URL に渡されます。

QualysProxy /n ProxyUsername /p ProxyPassword /a http://my-pacfile-server/QualysAgent.pac

クローン作成のためのクラウドエージェントの準備/ゴールドイメージ

Qualys Cloud Agent は、物理環境、仮想環境、クラウド環境 (Amazon AWS や Microsoft Azure など) でのクローン イメージへの構成と展開をサポートします。クラウドエージェントは、エージェントと Qualys プラットフォームまたはプライベートクラウドプラットフォーム間のプロビジョニングプロセスの一部として、エージェント ID としてユニバーサルユニーク識別子(UUID)を使用して作成されます。各クラウドエージェントには真に一意のエージェント ID が必要でなければ、管理とレポートに問題が生じます。

これらのベスト プラクティスのデプロイ ガイドラインに従って、生成された UUID が、クローン イメージまたはゴールド イメージのエージェント デプロイ全体で真に一意であることを確認します。

この方法は、サポートされているすべてのバージョンの Windows を対象としています。

1) オペレーティングシステム、アプリケーション、およびパッチをインストールします。ゴールデンイメージへのエージェントのインストールについては、QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <proxy url> /n <proxy username> /p <proxy password>".

- 続行する前に、ゴールド イメージのスナップショットを作成してください。

2) ゴールド イメージ インスタンスに、クラウド エージェントのインストール プロセス用に Qualys クラウド プラットフォームまたはデプロイされたプライベート クラウド プラットフォームへのネットワーク接続がないことを確認します。

- 仮想化マネージャーからゴールド イメージへのネットワークをオフにする
- ネットワーク接続のないネットワークでゴールドイメージを管理する
- ローカル hosts ファイル (

  C:¥Windows¥System32¥drivers¥etc¥hosts) エージェントが接続するパブリック POD または PCP の DNS 名 (例: 127.0.0.1) (ゴールド イメージのクローンを作成する前に、このエントリを必ず削除してください)
- クラウドエージェントプロセスがネットワーク経由で通信するのをブロックする一時的な Windows ファイアウォールルールを作成します(ゴールドイメージを複製する前に、このエントリを削除してください)

3) Qualys Cloud エージェントをインストールし、割り当てられたアクティベーション ID と顧客 ID を使用して構成します。

- クラウドエージェントは、プロビジョニングのために Qualys プラットフォームへの接続を試みます。接続がないと、エージェントは Qualys プラットフォームへの次の接続が成功するまで、プロビジョニングされていない状態のままになります。

４）これがゴールドイメージにインストールされる最後のアプリケーションまたはサービスでない場合は、クラウドエージェントサービスをシャットダウンし、その自動起動を「無効」に設定して、ゴールドイメージ構成の残りの部分でエージェントが起動およびプロビジョニングされないようにします。ゴールドイメージを複製する前に、クラウドエージェントサービスを「自動」開始に設定してください。

5) ゴールドイメージをシャットダウンし、クローン作成できるようにします。

6) クローンされたイメージの起動時に、Cloud Agent が起動し、Qualys Platform に接続してプロビジョニングされ、実行中のクローン インスタンスの UUID が生成されます。

別の方法: ホストの最終的なインストール/プロビジョニングの一部として、ドメイン参加スクリプトのインスタンスにクラウドエージェントをインストールできます。このアプローチにより、ゴールド イメージのインストールが大幅に簡素化されますが、ドメイン参加中に追加の処理が必要になります。

これらの手順に従わないと (またはエージェントの展開またはアップグレード時にソフトウェア配布ツールが正しく構成されていない場合) は、Qualys プラットフォームに重複するホスト レコードが作成される可能性があります。同じホスト名のホスト・レコードが 2 つある場合、1 つのレコードには古いエージェント UUID (使用されなくなった) があり、もう 1 つのレコードには新しいエージェント UUID (エージェントとプラットフォームの間で使用される) があります。この場合、通常、古いエージェント UUID レコードの「最終チェックイン」日は、エージェントが新しいエージェント UUID を使用している状態で再プロビジョニングが行われた日付です。すべての新しい脆弱性、コンプライアンス、および資産インベントリ情報は、新しいエージェント UUID およびホスト レコードに関連付けられます。

異なるエージェント UUID が生成されているために重複するホスト レコードがある場合は、Cloud Agent モジュールのユーザー インターフェイスまたは API を使用して古いホスト レコード/エージェント UUID をアンインストールすることで削除できます。これは、新しいエージェント UUID を使用して通信するエージェントの機能には影響しません。

重複したエージェントの数が多く、自分で削除するのが現実的でない、または面倒な場合は、Qualys カスタマー サポートにお問い合わせください。

オンデマンドスキャンと起動時スキャン

クラウドエージェント Windows 3.0 では、クライアント側で開始される「ScanOnDemand」機能とクライアント側で開始される「ScanOnStartup」機能が導入されています。この機能は、エージェントがオンデマンド マニフェスト収集を開始するようにトリガーするか、サポートされているアクティブ化されたモジュール (脆弱性管理、ポリシー コンプライアンス、およびインベントリ) に対してエージェント サービスが開始されたときに使用します。

この機能は、主に、新しくインストールされたパッチが関連するローカルホストの脆弱性を修正したことを確認する必要があるパッチ管理のユースケースをサポートするために導入されました。

オンデマンド・スキャンは、ホスト自体で手動で開始される、ローカルまたはリモートで実行されるスクリプトまたは GPO を使用するか、パッチ配布ジョブの最後にソフトウェア配布ツールから開始される 1 回限りの実行です。

[起動時のスキャン] は構成オプションであり、設定すると、Qualys エージェント サービスの起動時にマニフェスト スキャンが開始されます。主な使用例は、パッチ展開ジョブで脆弱性を完全に修復するためにホストを再起動する必要がある場合、またはイメージに脆弱性がないことを確認するためにゴールド イメージが構築されている場合に、アセットを再評価することです。

オンデマンドスキャンの開始または起動時のスキャンの設定に加えて、オンデマンドスキャンまたは起動スキャンのパフォーマンス値に CPU 制限を設定できます。この CPU 制限は、オンデマンドまたは起動時の実行のみを目的としており、構成プロファイルで設定された CPU 制限とは別のものです。最も一般的な使用例は、処理のエージェント部分を可能な限り高速に実行できるように、このスキャンの CPU 制限を高く設定するか、スロットルなし (100%) を設定することです。これにより、変更管理期間中のパッ

チ展開ジョブの一部として、通常の本番環境での使用に対して低いパフォーマンスプロファイルを維持しながら、迅速な収集が可能になります。

注: この機能は、エージェントが必要なメタデータを収集するためにマニフェストスキャンを開始する場合にのみ管理します。収集後、エージェントは差分の変更を計算し、処理のために変更をプラットフォームに送信します。プラットフォーム処理は、VM レポート、API、VM ダッシュボード、PC レポート、および AssetView で評価を利用できるようにするための通常の評価パイプラインに従って行われます。オンデマンドスキャン機能は、プラットフォーム上の評価処理のための通常の評価パイプラインを変更または高速化しません。

レジストリ構成

この機能の構成は、レジストリの Qualys エージェント ハイブで設定および管理されます。これにより、Qualys プラットフォームの UI や API にアクセスすることなく、パッチ展開やゴールドイメージのワークフローに統合できます。

エージェントは、Qualys レジストリ ハイブを

HKLM/Software/Qualys/QualysAgent/ScanOnDemand キーをリアルタイムで特定値に入力し、設定された値に基づいてサポートされている各マニフェストのスキャンを開始します。

Cloud Agent for Windows バージョン 4.8 以降では、モジュールがアクティブ化されると、エージェントはオンデマンド スキャン用のレジストリ構造とサブキーを自動的に作成します。4.8 より前のバージョンでは、ルート キーのみが作成され、スキャンを構成および実行するためのサブキー、データ、および値は、スクリプトまたはレジストリ構成ツールを使用して手動で設定する必要があります。

HKEY_LOCAL_MACHINE

SOFTWARE

Qualys

QualysAgent

ScanOnDemand

Inventory

CpuLimit

ScanOnDemand

ScanOnStartup

Vulnerability

CpuLimit

ScanOnDemand

ScanOnStartup

PolicyCompliance

CpuLimit

ScanOnDemand

ScanOnStartup

UDC

CpuLimit

ScanOnDemand

ScanOnStartup

SCA

CpuLimit

ScanOnDemand

ScanOnStartup

Registry Configuration Settings

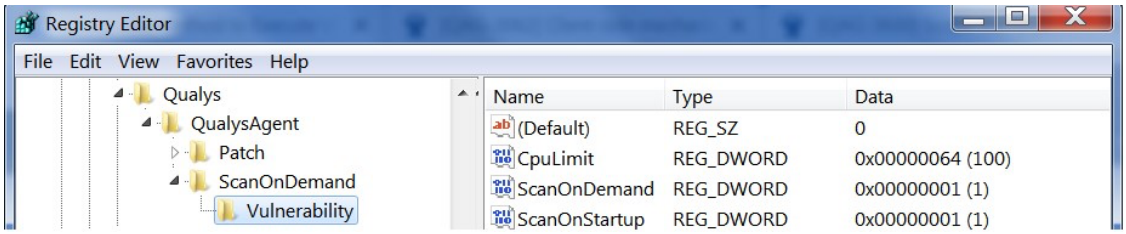
次の表に、オンデマンドスキャンおよび起動時スキャン機能の構成設定と機能を示します。

Module Key	Value	Type	Data	Description
Inventory Vulnerability PolicyCompliance UDC	CpuLimit	REG_DWORD (decimal)	2 - 100	Sets the CPU Limit (%) for the execution. Key is not required. Default value is 100 if no value exists or the data is not valid.

SCA	ScanOnDemand	REG_DWORD (decimal)	0 -completed 1 - execute now 2- in progress	Setting a data value of "1" will initiate the on demand scan. The data value will change to "2" when the scan is in progress. The data value will change to "0" when the scan is complete.
	ScanOnStartup	REG_DWORD (decimal)	1	A data value of "1" will configure the agent to execute the scan when the agent service starts up. After a completed scan, the scan interval for this manifest is reset. No execution if there is no value or the data is not valid.

例

CPU 制限を 100%にし、すぐに実行する「1」の「オンデマンド」データ、「エージェントサービスの起動時に実行する起動時のスキャンデータ」の設定例です。



機能に関する注意事項

エージェントが既にマニフェスト収集を実行している場合、または差分アップロード /PendingDelta 状態の場合、エージェントはオンデマンドまたは起動時のスキャンを開始しません。これにより、進行中のスキャンのエージェントとプラットフォーム間のデータ整合性が確保されます。

ネットワーク ブラックアウト ウィンドウが優先されます。

- エージェントがネットワーク ブラックアウト ウィンドウにある場合のオンデマンド スキャンまたは起動時のスキャンは引き続き実行されますが、エージェントがネットワーク ブラックアウト ウィンドウから外れるまで、デルタは Qualys プラットフォームにアップロードされません。
- エージェントがネットワーク・ブラックアウト・ウィンドウにあり、前回のスキャンの差分のアップロードが妨げられている場合、前回のスキャンの差分アップロードが完全に完了するまで、オンデマンド・スキャンまたは始動時のスキャンは実行されません。
- エージェントは、割り当てられていない(アクティブ化されていない)マニフェストの種類に対して、オンデマンドまたは起動時のスキャンを実行しません。

Microsoft Intune を使用した展開

Microsoft Intune を使用して、リモート資産に Qualys Cloud Agent for Windows をデプロイできます。Qualys Cloud Agent をリモートでデプロイするには、次の 2 つの方法があります。

- exe パッケージ ファイルを使用したデプロイ
- msi パッケージを使用したデプロイ

exe パッケージ ファイルを使用したデプロイ

ファイルを使用してクラウドエージェントをデプロイする手順.exe 次に示します。

Step 1: Create .intunewin Package

Step 2: Add App Information

Step 3: Set Program Information

Step 4: Set Requirements

Step 5: Set Detection Rule

Step 6: Scope tags

Step 7: Assignments

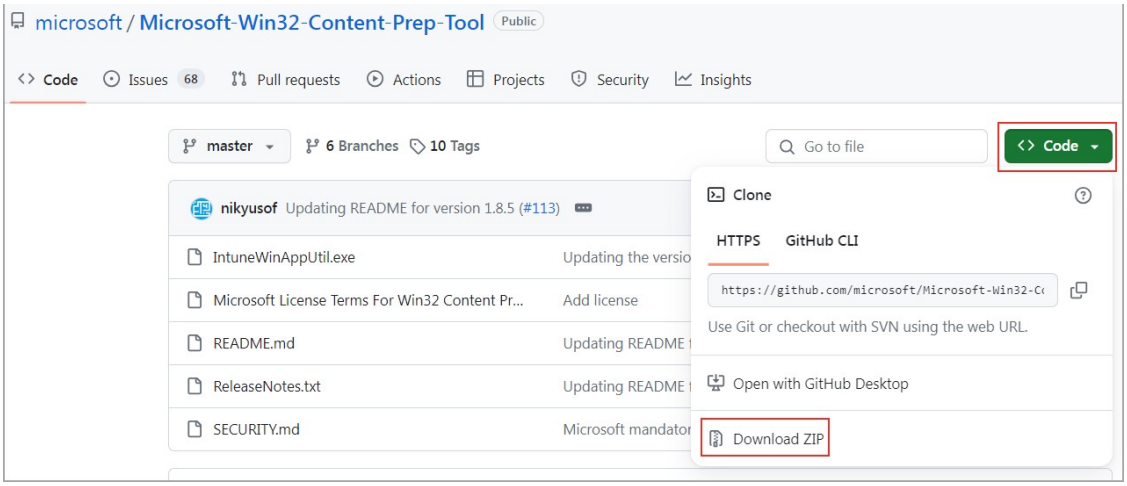
Step 8: Review + create

.intunewin パッケージを作成する

.exe ベースのクラウド エージェント パッケージを展開するには、まずクラウド エージェント インストーラーをダウンロードし、それを .intunewin パッケージ ファイルに変

換する必要があります。クラウド エージェント インストーラーをダウンロードし、.intunewin パッケージ ファイルを作成する手順は次のとおりです。

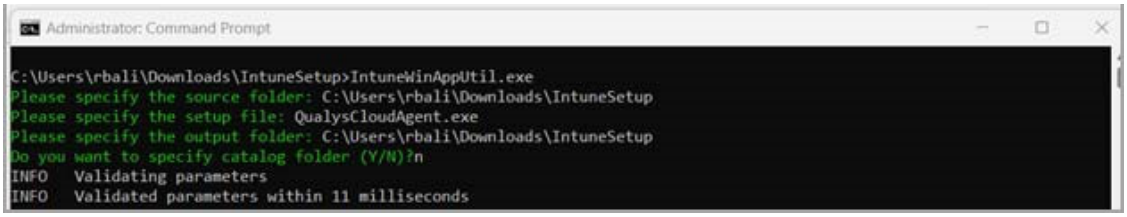
- GitHub から準備ツールをダウンロードします。準備ツールをダウンロードするには、GitHub 準備ツールを参照してください。準備ツールを.zip ファイルでダウンロードしてください
- 準備ツールをローカルフォルダ.zip ファイルに解凍します。



- Cloud Agent ユーザーインターフェイスから Cloud Agent インストーラーをダウンロードします。詳細は、エージェントインストーラのダウンロード方法をご参照ください。
- .intunewin パッケージ ファイルを作成するには:
  - ローカル フォルダーを作成し、ダウンロードしたクラウド エージェント ファイルをそのフォルダーに保存します。
  - 抽出した準備ツールファイルから IntuneWinAppUtil.exe ファイルを実行します。

- コマンドプロンプトウィンドウで、次の詳細を入力します。

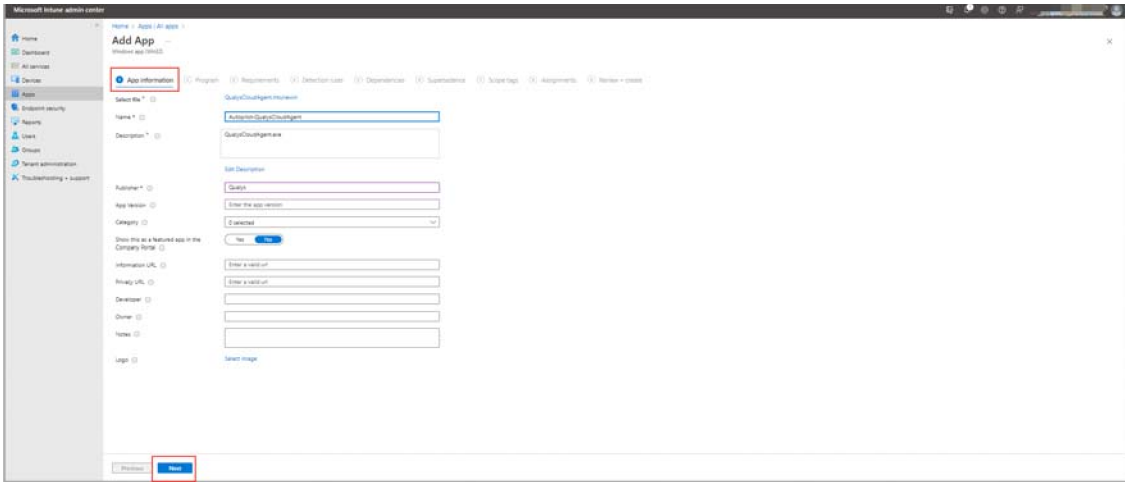
- Cloud Installer パッケージを含むソース フォルダー。
- Cloud Agent セットアップ ファイル
- .intunewin パッケージ ファイルの出力フォルダー



クラウドエージェント用の .intunewin ファイルが生成され、出力フォルダーに保存されます。

アプリ情報の追加

- Microsoft Intune 管理センターのホーム ページで、Apps > Add App >Windows をクリックします。
- [アプリ情報] ページで、[アプリ パッケージ ファイルの選択] をクリックします。[アプリの種類の選択] ウィンドウが開きます。
- [アプリの種類の選択] ウィンドウで、[Windows アプリ (Win32)] を選択し、[選択] をクリックします。
- App package file ウィンドウで、.intunewin パッケージ ファイルをアップロードし、[OK] をクリックします。
- App Information ページで、アプリの詳細を入力し、[次へ] をクリックします。[プログラム] ページが開きます。



プログラム情報の設定

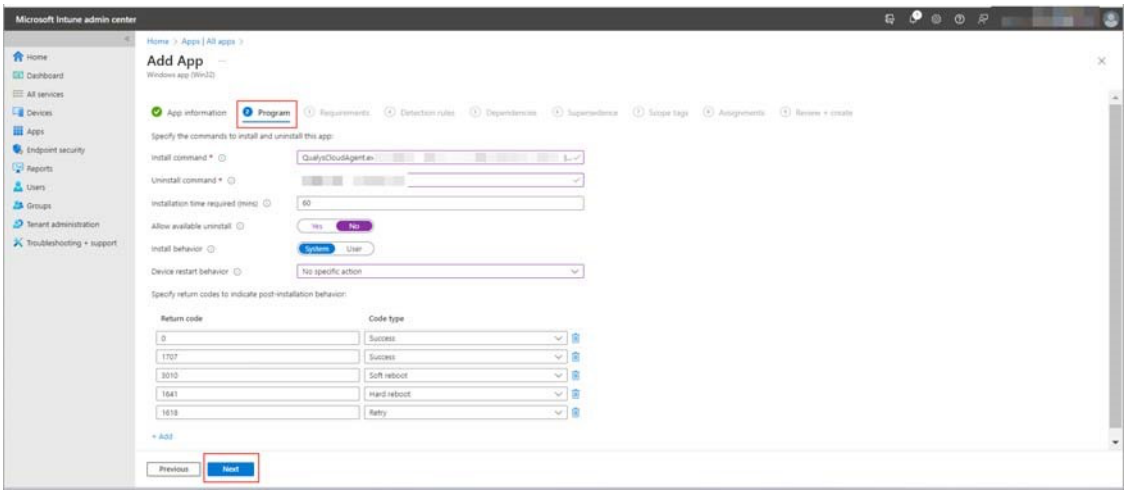
- [プログラム] ページで、[インストール] コマンドと [アンインストール] コマンドを入力します。インストール コマンドとアンインストール コマンドは、Cloud Agent インストーラに付属しています。
- インストール・コマンドの例:

QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxxxxxxxxxxxxxxxxxx}
ActivationId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx}
WebServiceUri=/CloudAgent/

- アンインストール用

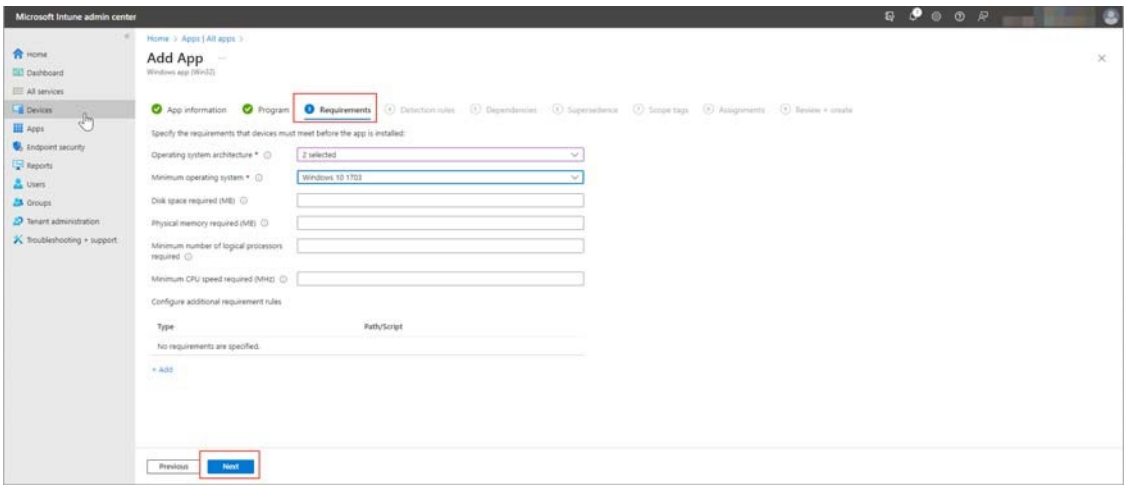
"%programfiles%¥qualys¥qualysagent¥uninstall.exe" Uninstall=True Force=True

- [使用可能なアンインストールを許可する] フィールドを [いいえ] に設定します。
- [次へ] をクリックします。[要件] ページが開きます。



要件の設定

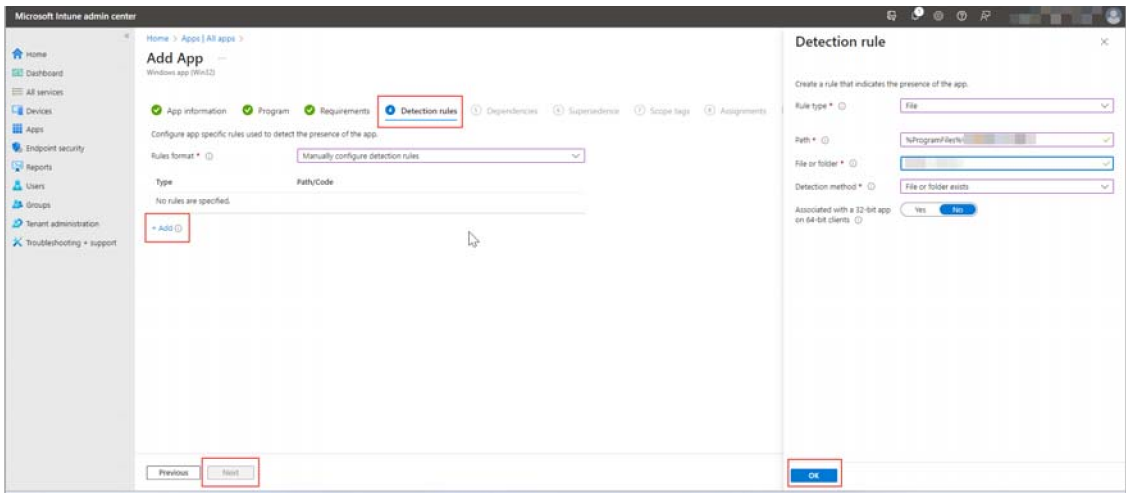
- [要件] ページで、使用可能なオプションから [オペレーティング システム アーキテクチャ] フィールドと [最小オペレーティング システム] フィールドの値を選択します。
- [次へ] をクリックします。[検出ルール] ページが開きます。



検出ルールの設定

- [検出ルール] ページの [ルール形式] で、[検出ルールを手動で構成する] を選択します。
- [検出ルール] ウィンドウの [ルールの種類] で [ファイル] を選択します。
- [検出ルール] ウィンドウで、次のフィールドを設定します。
  - Path：クラウドエージェントインストーラがダウンロードされるフォルダパス。
  - File or Folder :Cloud Agent インストーラファイル(.exe)。
  - Detection method：ファイルまたはフォルダが存在する。

- Next をクリックする。

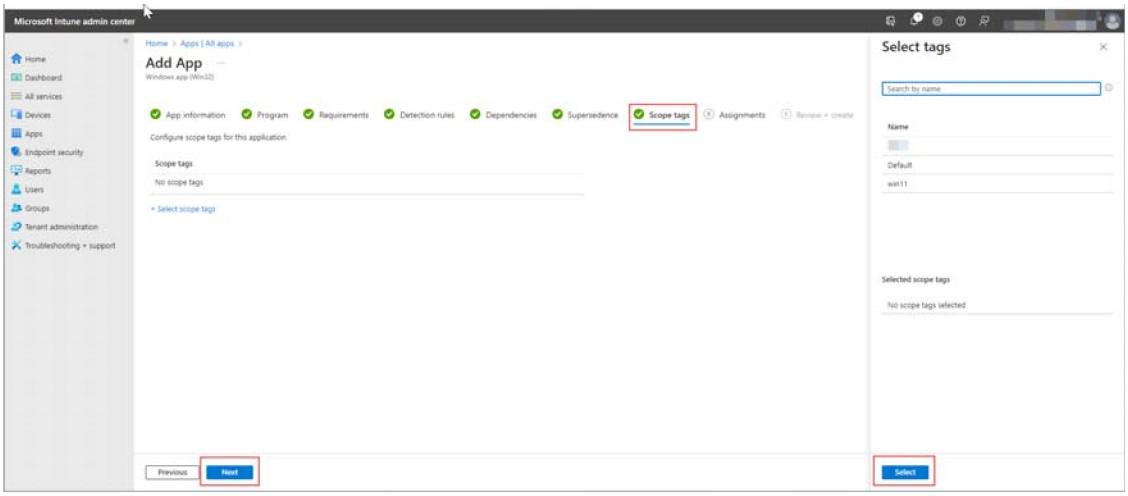


スコープタグ

次の手順を実行して、[割り当て] ページに進みます。

- 依存関係: クラウドエージェントのソフトウェア依存関係は、クラウドエージェントをインストールする前にインストールする必要があるアプリケーションです。このステップでは、依存関係の自動インストールを有効または無効にすることができます。[次へ] をクリックします。
- 置き換え: このステップでは、以前のバージョンのクラウドエージェントを更新するか置き換えるかを指定できます。[次へ] をクリックします。
- スコープタグ: このページでは、Cloud Agent のスコープタグを指定できます。
- [次へ] をクリックします。[割り当て] ページが開きます。

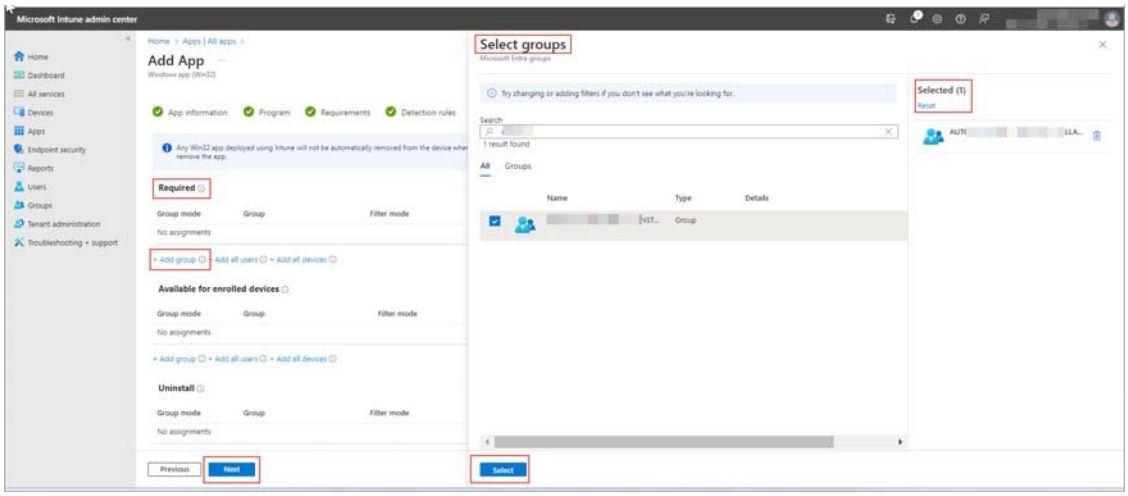
注: 上記のステップの値はユーザー定義です。要件に応じて、上記の手順のフィールド値を設定できます。



アサイメント

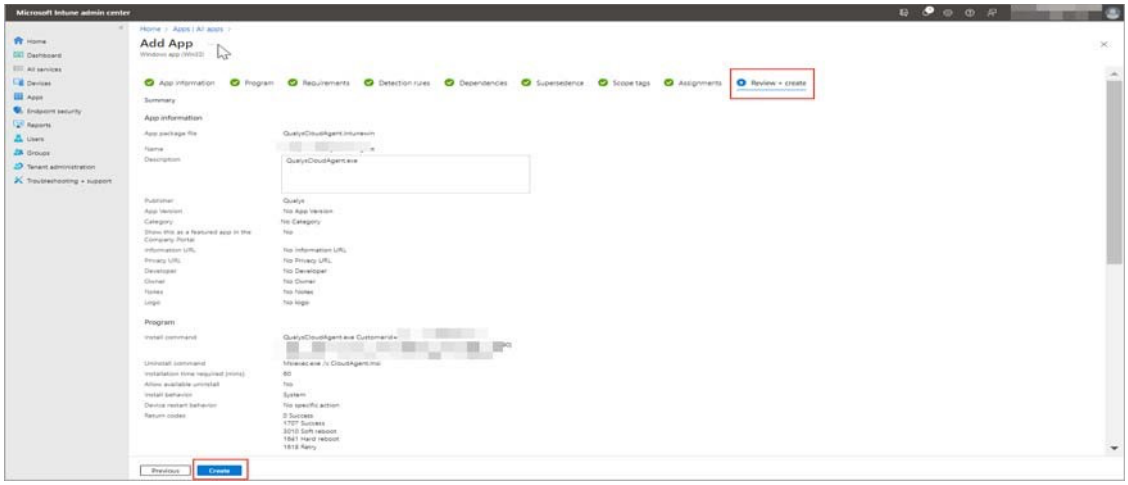
このページで、Cloud Agent をデプロイするグループを追加します。

- [割り当て] ページの [必須] セクション> [グループの追加] をクリックします。[グループの選択] ウィンドウが開きます。
- [グループの選択] ウィンドウで、資産グループに関連付けられているチェックボックスをオンにします。
- [選択] をクリックします。選択した資産グループは、[選択済み] ペインで表示できます。
- [次へ] をクリックして、[レビュー + 作成] ページに進みます 。



Review + create

- Cloud Agent デプロイメントパッケージに入力した情報を確認します。
- 前のページに移動するには、[前へ] をクリックします。
- [作成] をクリックして、クラウドエージェントをデプロイします。


Microsoft Intune admin center
Add App
App information
Program
Requirements
Detection rules
Dependencies
Supersedence
Scope tags
Assignments
Review + create
Summary
App information
Program
Previous
Create

msi パッケージを使用したデプロイ

msi パッケージファイルを使用したクラウドエージェントのデプロイには、次の手順が含まれます：

Step 1: クラウドエージェントパッケージをダウンロードする

Step 2: msi パッケージ ファイルを抽出する

Step 3: msi パッケージ ファイルをデプロイする

クラウドエージェントパッケージをダウンロードする

Cloud Agent インストーラパッケージのダウンロードについて詳しくは、「Agent インストーラのダウンロード方法」を参照してください。

msi パッケージ ファイルを抽出する

ファイルから msi パッケージ ファイルを抽出.exe。詳細は、MSI パッケージの抽出を参照してください。

msi パッケージ ファイルをデプロイする

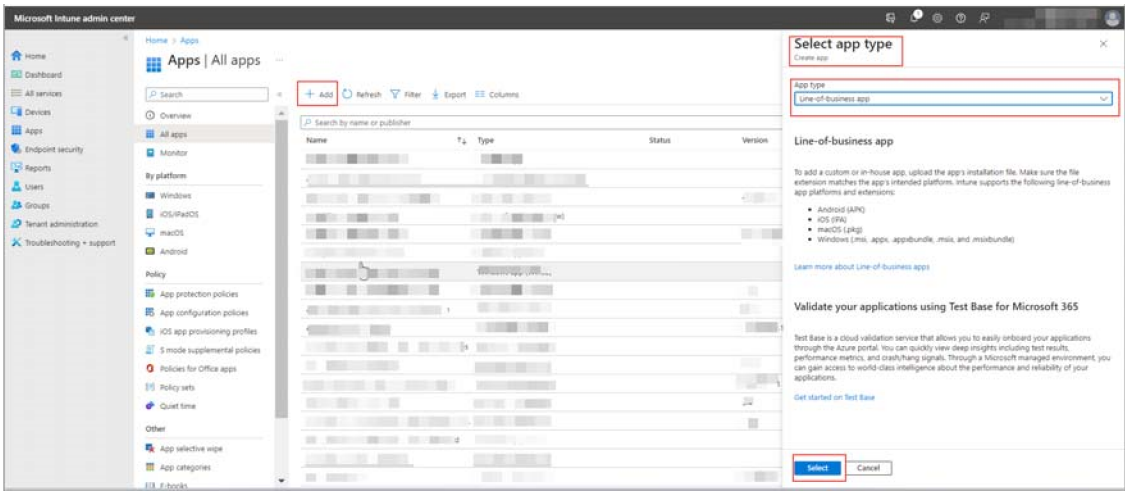
msi パッケージ ファイルを使用して Qualys Cloud Agent をデプロイする手順は次のとおりです。

アプリ情報

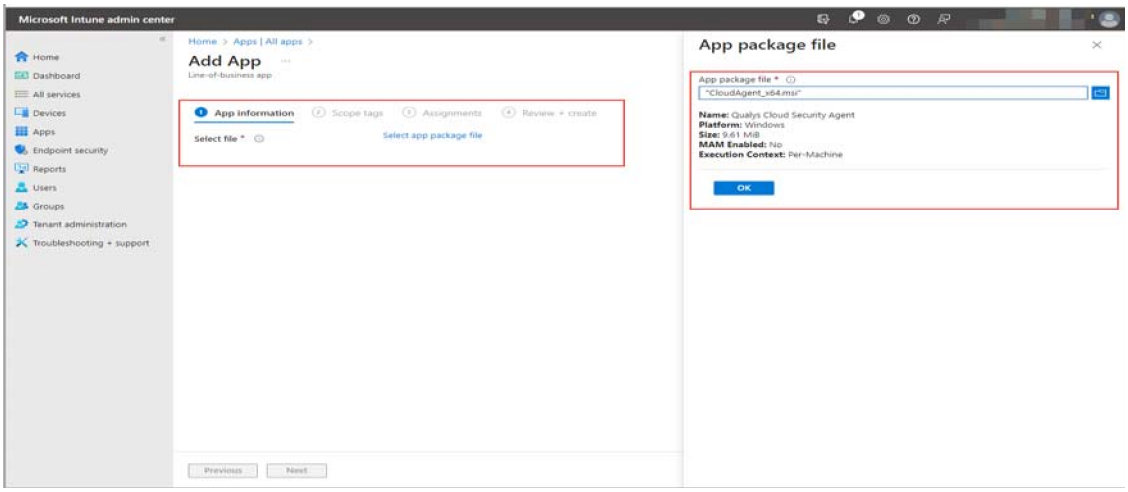
- Microsoft Intune 管理センターにログインします。
- Microsoft Intune 管理センターで、[すべてのアプリ] > [追加] をクリックします。[アプリの種類の選択] ウィンドウが開きます。
- 基幹業務アプリ を選択し、選択 をクリックします。

Deployment using Microsoft Intune

Deployment using msi Package

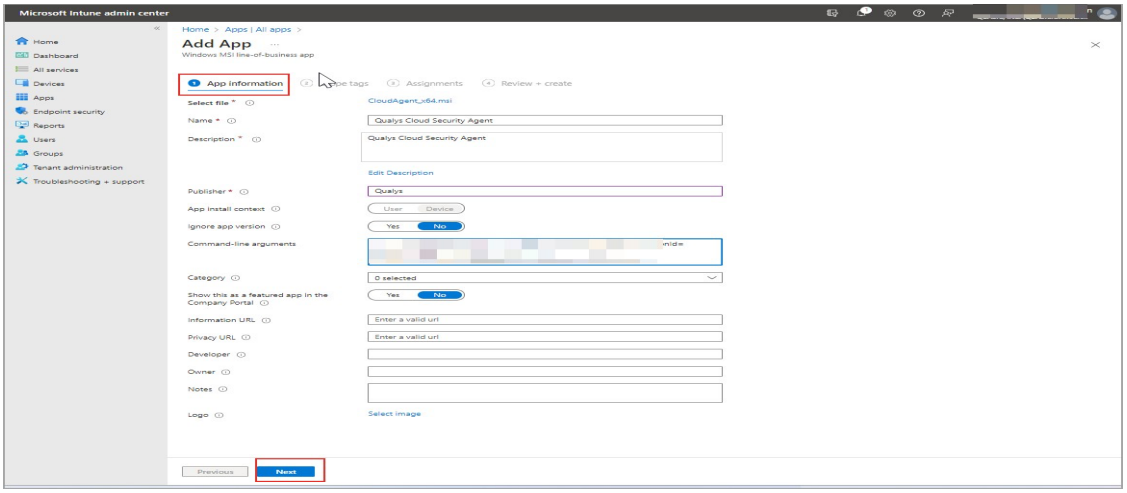


- アプリ情報ページで、[アプリパッケージファイルの選択] をクリックします。[アプリ パッケージ ファイル] ウィンドウが開きます。
- [アプリパッケージファイル] ウィンドウで、Cloud Agent パッケージファイル (.msi)をアップロードし、[OK] をクリックします。



- [アプリ情報] ページで、クラウドエージェントのアプリケーション情報を入力します。
- [コマンドライン引数] フィールドに、次のコマンドを入力します。

QualysCloudAgent.msi CustomerId={12345678-1234-1234-1234123456789012} ActivationId={12345678-1234-1234-1234-123456789012} WebServiceUri=/CloudAgent/



- [次へ] をクリックします。
- [スコープ タグ] ページで、クラウド エージェントのスコープ タグを指定します。[次へ] をクリックします。

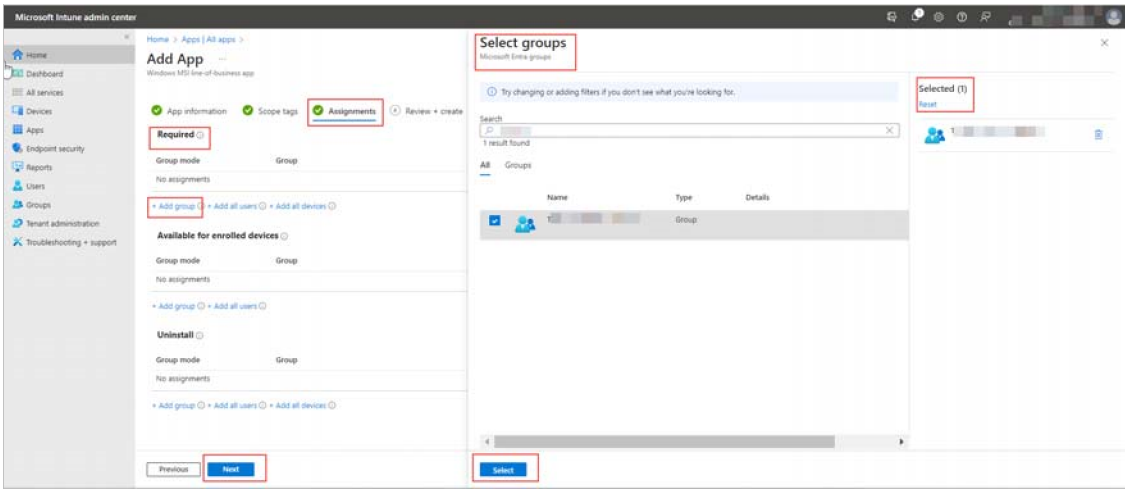
割り当て

このページで、Cloud Agent をデプロイするグループを追加します。

- [割り当て] ページの [必須] セクション> [グループの追加] をクリックします。[グループの選択] ウィンドウが開きます。
- [グループの選択] ウィンドウで、資産グループに関連付けられているチェックボックスをオンにします。
- [選択] をクリックします。選択した資産グループは、[選択済み] ペインで表示できます。
- [次へ] をクリックします。[レビュー + 作成] ページが開きます。

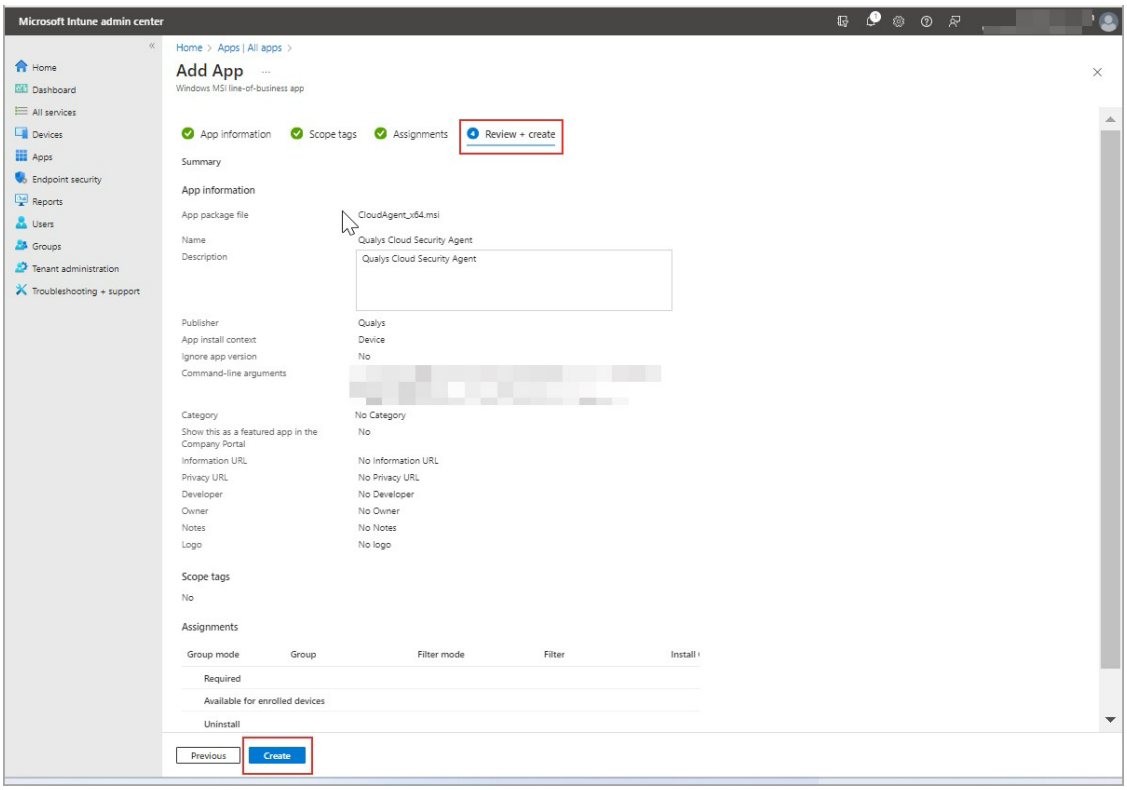
Deployment using Microsoft Intune

Deployment using msi Package



Review + create

- Cloud Agent デプロイ パッケージに入力した情報を確認します。
- [作成] をクリックして、クラウドエージェントをデプロイします。



注: 必要に応じて、「前のページ」に移動して情報を編集できます。