TREND MICRO

PortalProtect™ 2.6

インストールガイド

Collaboration Security

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバ

P/N: PPEM28660/190425_JA_R1 (2022/06)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

PortalProtect により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。PortalProtect における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

第 4 章：よくある質問

付録 A：データベース権限の要件

索引

はじめに

Trend Micro PortalProtect (以下、PortalProtect) 2.6 インストールガイドへようこそ。本書には、PortalProtect を導入し、個々のニーズに基づいて SharePoint サーバを保護するために実行する必要があるタスクについての基本的な情報が記載されています。本書は、PortalProtect の計画、導入、およびテストを行うユーザを対象としています。

本章の内容は次のとおりです。

ドキュメント

PortalProtect には、次のドキュメントが付属しています。

- オンラインヘルプ (英語) — 各種作業を実行するための詳細な手順の説明。
- インストールガイド — 製品の概要、インストール計画、インストール、設定、起動方法に関する説明。
- 管理者ガイド — 製品の概要、インストール計画、インストール、設定、および製品環境を管理するために必要な詳細情報の説明。
- Readme — 基本的なインストール方法と既知の制限事項に関する説明。

注意

ドキュメントおよびプログラムファイルの最新版については、最新版ダウンロードサイト (https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp) から該当するリンクにアクセスしてチェックすることをお勧めします。

対象読者

PortalProtect のドキュメントは、セキュリティシステムや Microsoft Windows SharePoint サービスの管理について基本的な知識があることを前提としています。インストールガイド、管理者ガイド、およびオンラインヘルプはネットワーク管理者を対象に作成されています。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

第 1 章

インストールとアップグレードの計画

Trend Micro PortalProtect (以下、PortalProtect) 2.6 は、Microsoft SharePoint Server 2013/2016/2019/サブスクリプションエディション用のサーバベースのセキュリティソリューションです。PortalProtect は、ウイルスをはじめとするセキュリティの脅威による攻撃からコラボレーションシステムを保護します。

ここでは、Trend Micro PortalProtect のインストールの準備に必要な手順について説明します。また、アップグレードの一般的な問題に関する情報や、PortalProtect の各種機能に関する提案についても示します。本章の内容は次のとおりです。

システム要件

最新の情報については、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-and-collaboration/portalprotect-forsharepoint.html#requirement

ヒント

システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

導入計画

PortalProtect は、1 台のスタンドアロンサーバで実行するか、サーバファームの構成を使用するように設定できます。次のいずれかのモデルで PortalProtect がサーバファームを使用するように設定します。

SharePoint Services 小規模サーバファーム

注意

PortalProtect は、Web アプリケーションサーバ (サービス) が稼働しているサーバ (Web フロントエンドサーバ) にインストールします。

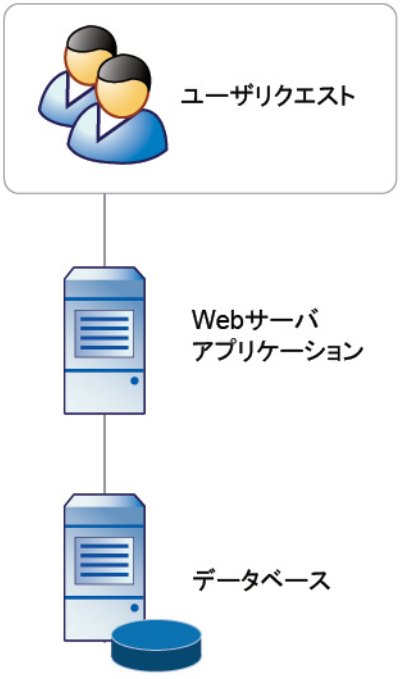

図 1-1. 小規模サーバファームの構成

SharePoint Services 中規模サーバファーム

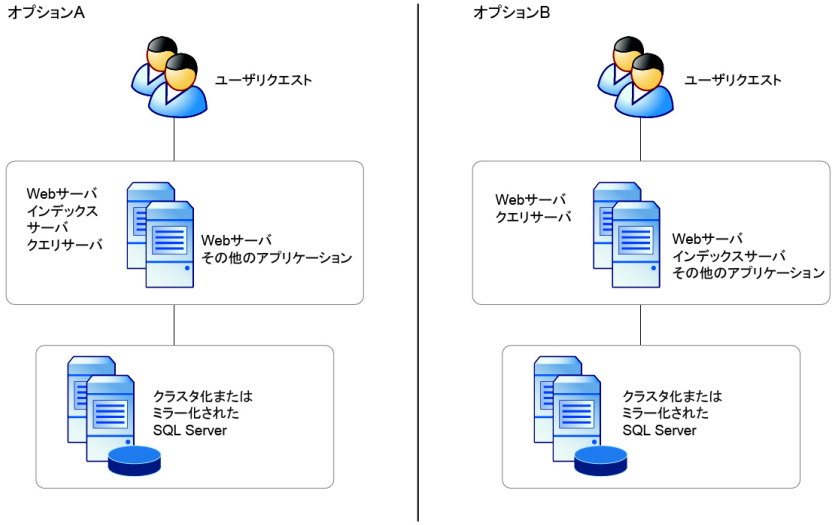

図 1-2. 中規模サーバファーム

SharePoint Services 大規模サーバファーム

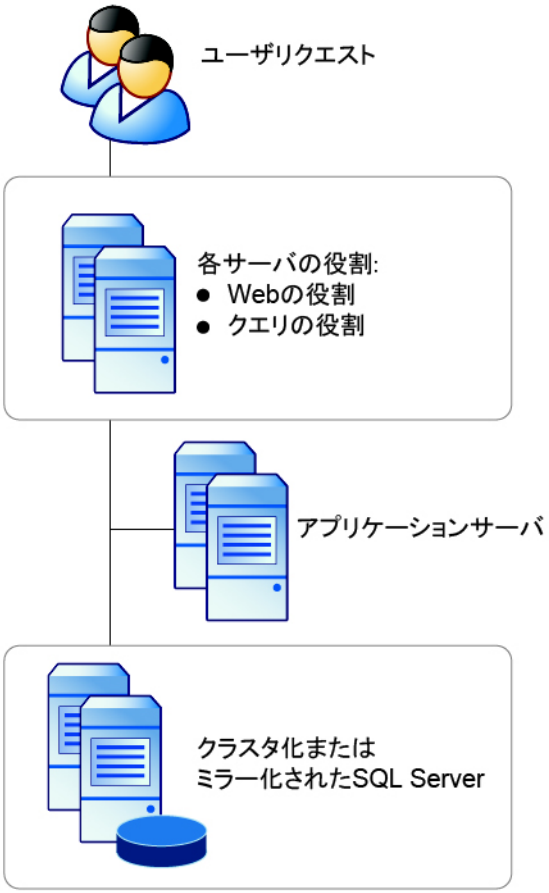

図 1-3. 大規模サーバファームの構成

インストールの準備

ネットワークに PortalProtect をスムーズに設置するためには、次の項目について考慮してください。

- 適切なサーバプラットフォームがインストールされているサーバに PortalProtect をインストールします。詳細については、12 ページの「システム要件」を参照してください。正常にインストールするには Microsoft Internet Information Services (IIS) が必要です。
- PortalProtect のインストールには、起動済みの IIS Web アプリケーションプールである DefaultAppPool を使用します。DefaultAppPool が存在しない場合は、次の基本設定を使用して作成します。
  - .NET CLR バージョン: V4.0
  - マネージ パイプライン モード: 統合
- レジストレーションキー/アクティベーションコード: インストール時には、セットアッププログラムからアクティベーションコードを要求されます。PortalProtect に付属のレジストレーションキーを使用して、トレンドマイクロの Web サイトでアクティベーションコードを取得します。セットアッププログラムには、トレンドマイクロの Web サイトへのリンクが表示されます。
- 必要なアカウントの権限: インストールに必要な次のアカウントに権限を指定します。
  - プログラムのセットアップアカウント: インストールプログラムの実行を承認するために使用します。インストールプログラムを起動するコンピュータのローカル管理者権限と、PortalProtect のインストールを計画しているすべての対象サーバのローカル管理者権限が必要となります。このアカウントは、PortalProtect をインストールするサーバが属するドメインに参加しているユーザアカウントである必要もあります。
  - PortalProtect 設定データベースアクセスアカウント: PortalProtect 設定データベースにアクセスするアカウントに必要なデータベースの役割を指定します。詳細については、93 ページの「データベース権限の要件」を参照してください。

- SharePoint データベースアクセスアカウント: SharePoint データベースにアクセスするアカウントに必要なデータベースの役割を指定します。詳細については、93 ページの「データベース権限の要件」を参照してください。

注意

PortalProtect と SharePoint のデータベースへのアクセスには、同じアカウントを使用することを強くお勧めします。

- プロキシサーバの情報: インストール時には、セットアッププログラムからプロキシサーバの情報を要求されます。使用環境のネットワークでインターネットトラフィックをプロキシサーバが処理している場合は、プロキシサーバの情報、ユーザ名、パスワードを入力し、ウイルスパターンファイルと検索エンジンのアップデートを取得します。インストール時にプロキシサーバの情報を入力しない場合は、[Administration] メニューで後から設定できます。
- 管理グループ: インストール時には、セットアッププログラムから管理グループの選択を要求されます。既存の管理用 Active Directory グループを選択します。セットアッププログラムによって、このグループに PortalProtect を管理するための権限が与えられます。このグループのユーザは、PortalProtect の Web 管理コンソールにログオンできます。

第 2 章

インストールとアンインストール

ここでは、Trend Micro PortalProtect (以下、PortalProtect) 2.6 をインストールおよびアンインストールする方法について説明します。また、PortalProtect の各種機能に関する情報や提案についても示します。

管理者は、PortalProtect をローカルサーバに、または同時に複数のサーバへ速やかにインストールできます。同様に、PortalProtect を 1 つまたは複数のサーバからアンインストールする場合も、シンプルで直感的な手順が提供されます。

本章の内容は次のとおりです。

新規インストールの実行

ヒント

PortalProtect をインストールする前に、Readme ドキュメントに記載されている既知の問題を確認してください。

PortalProtect は、次の 2 種類の方法でインストールできます。

- インストールプログラム (`setup.exe`) を使用する (20 ページの「setup.exe を使用したインストール」を参照)
- サイレントインストールプログラム (`SilentSetup.bat`) を使用する (40 ページの「新規サイレントインストール」を参照)

setup.exe を使用したインストール

PortalProtect には、ローカルとリモートの両方のインストールに使用できるインストールプログラムがあります。このセットアッププログラムによって、PortalProtect を 1 つまたは複数のサーバにインストールし、社内のすべての SharePoint サーバにすばやく導入できます。

インストール先サーバはネットワーク内に存在する必要があり、設定するユーザには管理者権限が必要です。

手順

1. PortalProtect の `setup.exe` を実行して、インストールを開始します。

PortalProtect インストールの開始画面が表示されます。

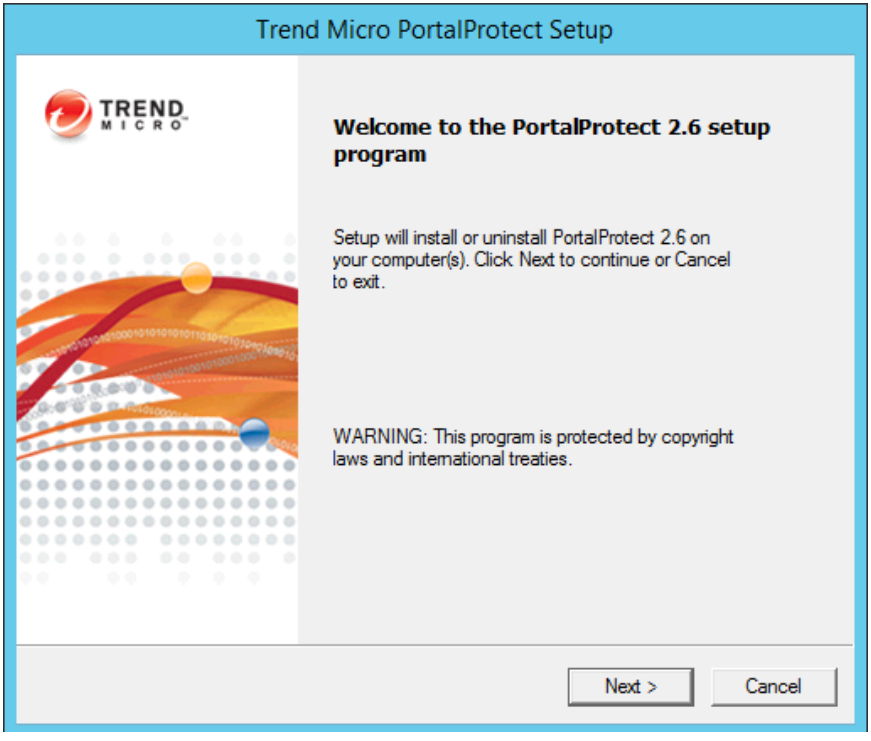

図 2-1. インストールの開始画面

2. [Next >] をクリックします。

[License Agreement] 画面が表示されます。

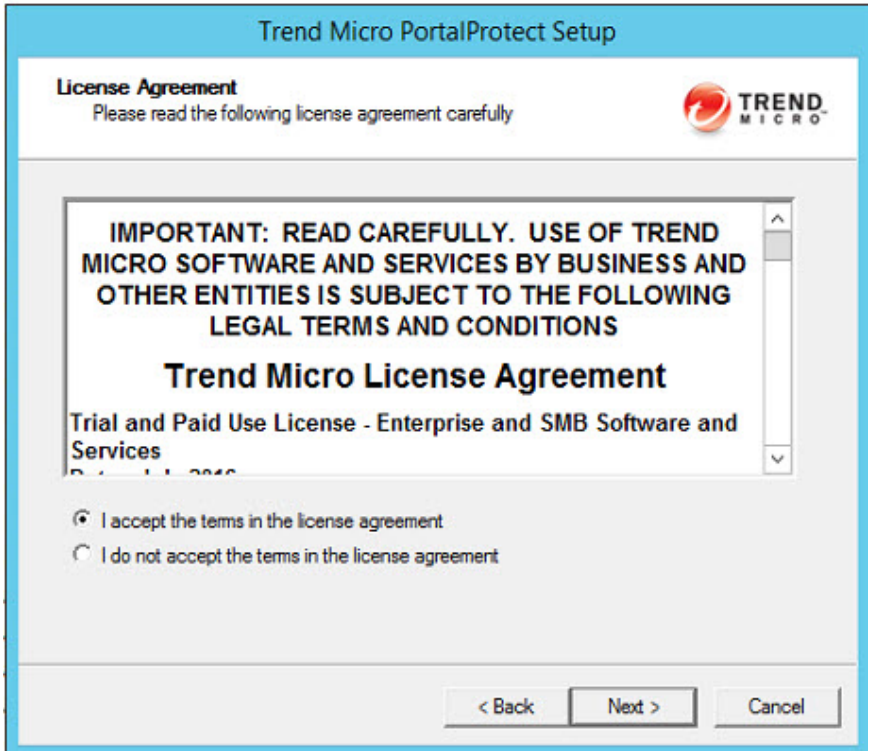

図 2-2. [License Agreement] 画面

3. 使用許諾契約書を確認します。契約に同意する場合は、[I accept the terms in the license agreement] を選択して [Next >] をクリックします。セットアッププログラムによって、システムが要件を満たしているかどうかのチェックが開始されます。契約に同意できない場合は、[Cancel] をクリックしてセットアッププログラムを終了します。

[Select an Action] 画面 (1) が表示されます。

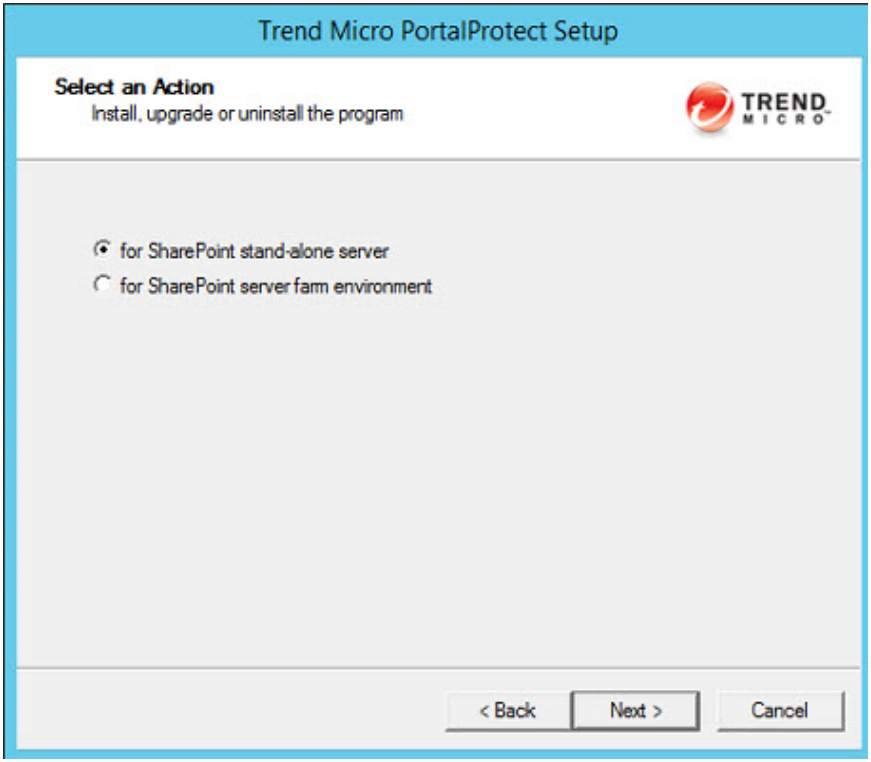

図 2-3. [Select an Action] 画面 (1)

4. 次のいずれかのインストールオプションを選択します。
   - for SharePoint stand-alone server
   - for SharePoint server farm environment
5. 適切なオプションを選択したら、[Next >] をクリックします。

注意

SharePoint の配置モードに応じて、SharePoint スタンドアロンサーバへのインストール ([for SharePoint stand-alone server]) を選択するか、SharePoint サーバファーム環境へのインストール ([for SharePoint server farm environment]) を選択します。SharePoint をファームモードで配置する場合は、[for SharePoint server farm environment] を選択する必要があります。一方、SharePoint をスタンドアロンモード (基本的な配置) で配置する場合は、[for SharePoint stand-alone server] を選択する必要があります。

[Select an Action] 画面 (2) が表示されます。

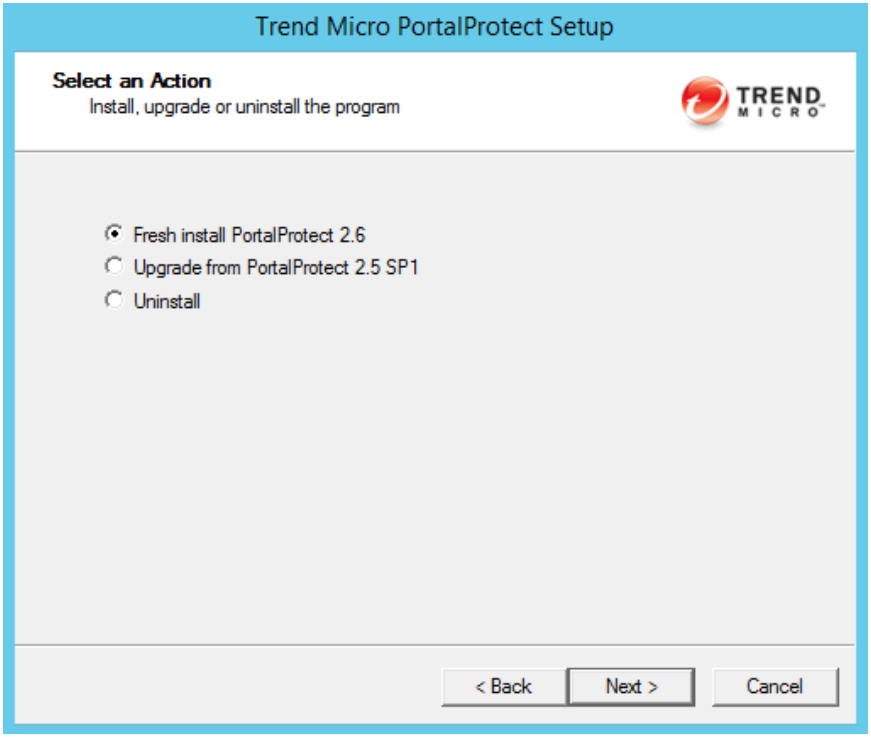

図 2-4. [Select an Action] 画面 (2)

6. 適切なオプションを選択したら、[Next >] をクリックします。

[Product Activation] 画面が表示されます。

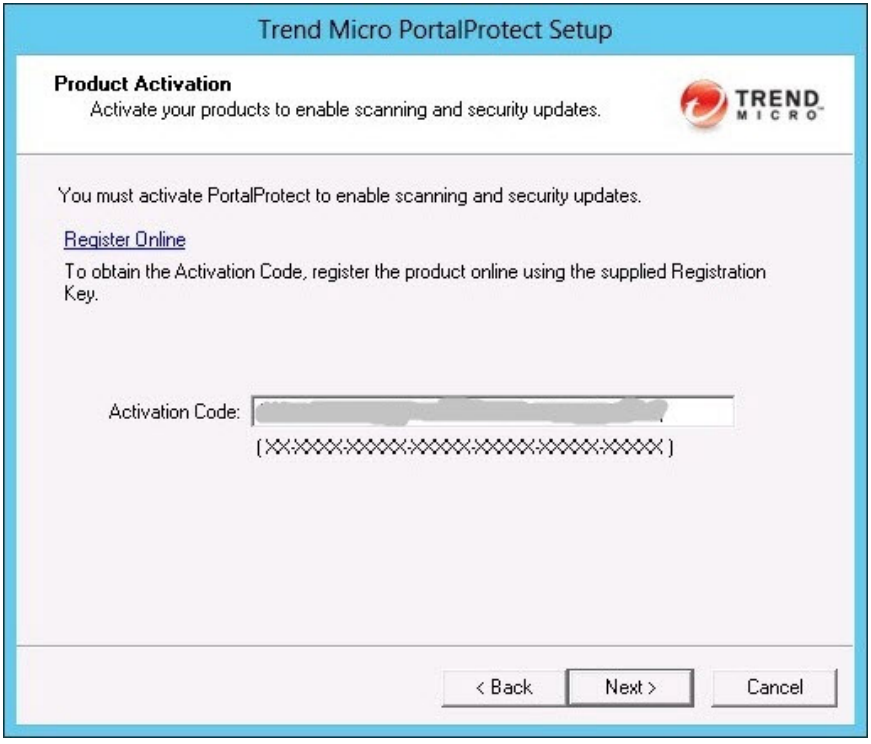

図 2-5. [Product Activation] 画面

7. アクティベーションコードを入力し、[Next >] をクリックしてインストールを続行します。

[Select Target Server(s)] 画面が表示されます。

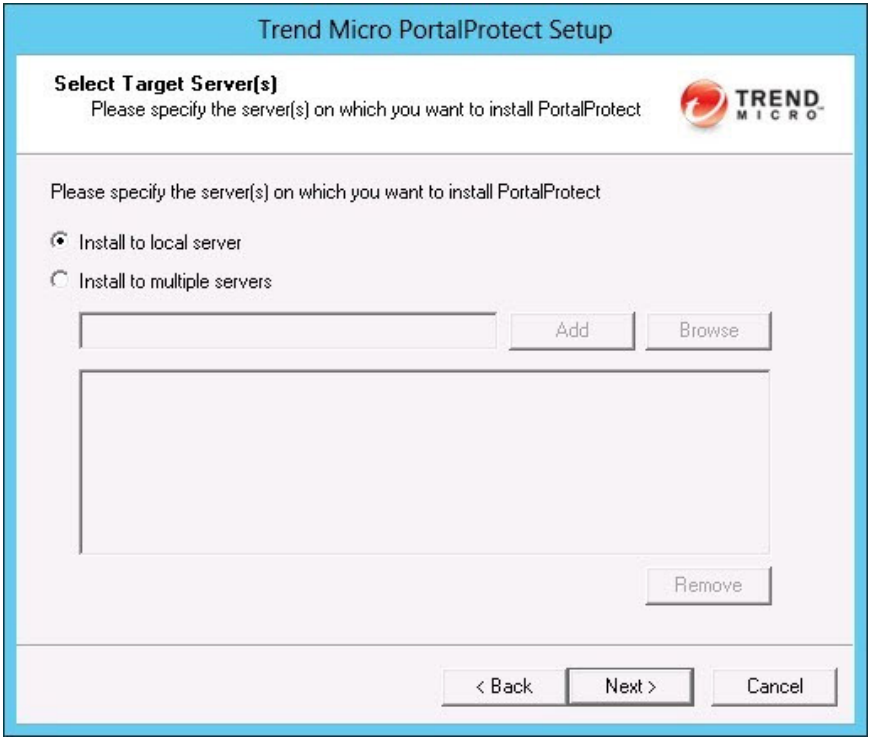

図 2-6. [Select Target Server(s)] 画面

8. 次のオプションから選択します。

   - Install to local server (推奨) — ローカルサーバにインストールします。選択したら、[Next >] をクリックしてインストールを続行します。
   - Install to multiple servers (リモートインストール) — PortalProtect をインストールするインストール先サーバを選択します。コンピュータ名を入力するか [Computer name] の [Browse] をクリックしてコンピュータを参照し、1 つまたは複数のサーバを [Add] をクリックして追加します。すべてのインストール先サーバをリストに追加したら、[Next >] をクリックしてインストールを続行します。リ

モートサーバのログオンアカウント情報を入力するように求められます。

[Configure Shared/Target Directory] 画面が表示されます。

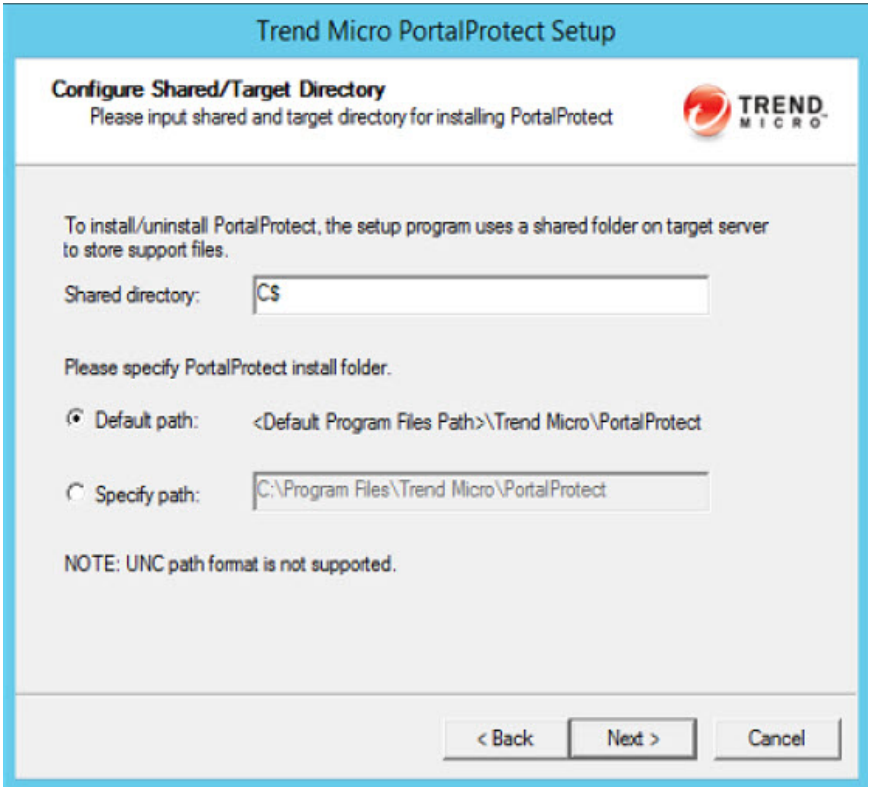

図 2-7. [Configure Shared/Target Directory] 画面

9. インストール先サーバの共有フォルダの初期設定パスをそのまま使用するか、[Specify path] に新しいパスを入力します。[Next >] をクリックします。

警告!

[Specify path] フィールドには英字のみを入力してください。そうしないと、インストールが正常に実行されません。

注意

PortalProtect では、共有ディレクトリに C$、D$などの Windows の初期設定の共有のみを使用できます。

[Web Server Information] 画面が表示されます。

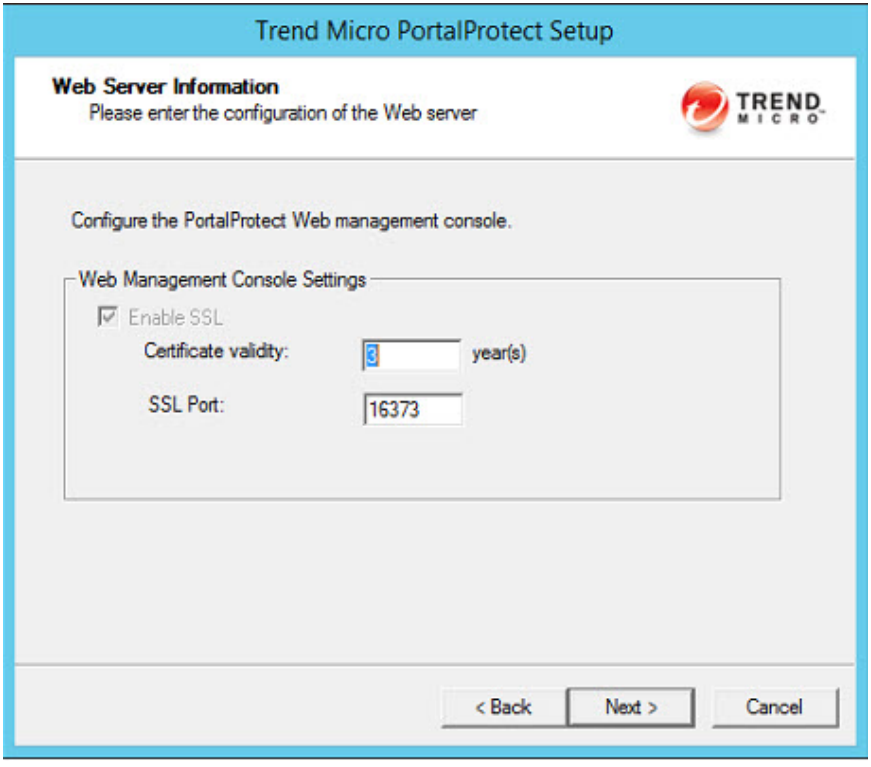

図 2-8. [Web Server Information] 画面

10. [SSL Port] に、Web 管理コンソールの SSL ポート番号を入力します。[Next >] をクリックします。

[PortalProtect Configuration Database] 画面が表示されます。

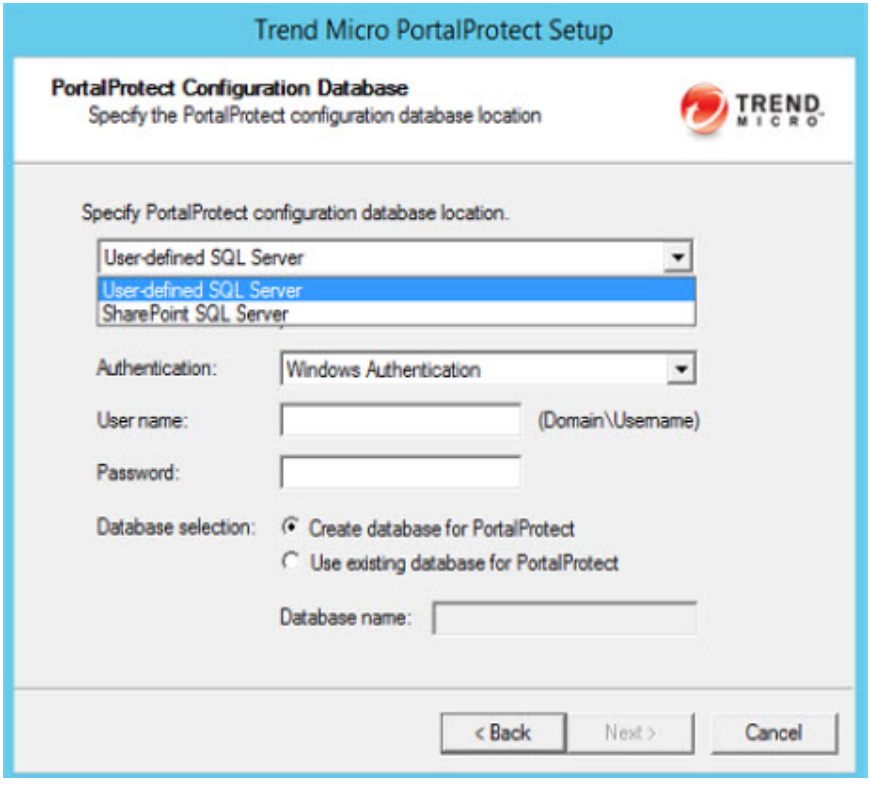

図 2-9. [PortalProtect Configuration Database] 画面

11. 次のオプションから選択します。

    - Specify PortalProtect configuration database location:

        - SharePoint SQL Server — PortalProtect を SharePoint SQL Server にインストールします。

        - User-defined SQL Server — PortalProtect をユーザ定義 SQL Server にインストールします。

> **注意**
>
> PortalProtect 設定データベースを自動作成するか既存の PortalProtect 設定データベースを使用するには、dbcreator 権限を持つアカウントでインストールを実行する必要があります。dbcreator の役割が使用できない場合は、93 ページの「データベース権限の要件」を参照してください。

- Authentication — [Windows Authentication] と [SQL Server Authentication] のいずれかを選択します。

> **注意**
>
> [Windows Authentication] を使用することを強くお勧めします。

- User name — 必要に応じて入力します。
- Password — 必要に応じて入力します。

12. [Next >] をクリックします。

[Checking Target Server System Requirements] 画面が表示されます。

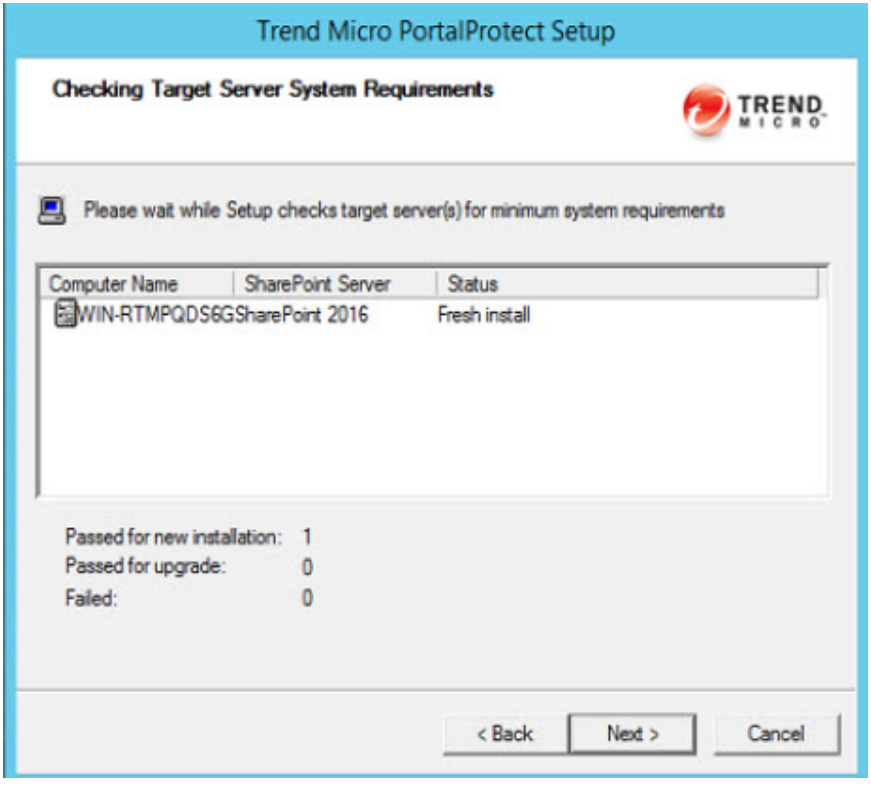

図 2-10. [Checking Target Server System Requirements] 画面

PortalProtect をインストールする各インストール先サーバで、インストールプログラムによって次の項目についてシステムが分析されます。

- インストール先サーバで正しいバージョンの Windows が実行されているかどうか
- インストール先サーバで正しい SharePoint のバージョンによって Web アプリケーションが実行されているかどうか
- インストール先サーバにログオンするための適切な権限が与えられているかどうか

- SharePoint configDB へのアクセスに、適切な SharePoint データベースアクセスアカウントが指定されているかどうか

13. [Status] に [Fresh Install] と表示されていることを確認して、[Next >] をクリックします。

    [Management Group Selection] 画面が表示されます。

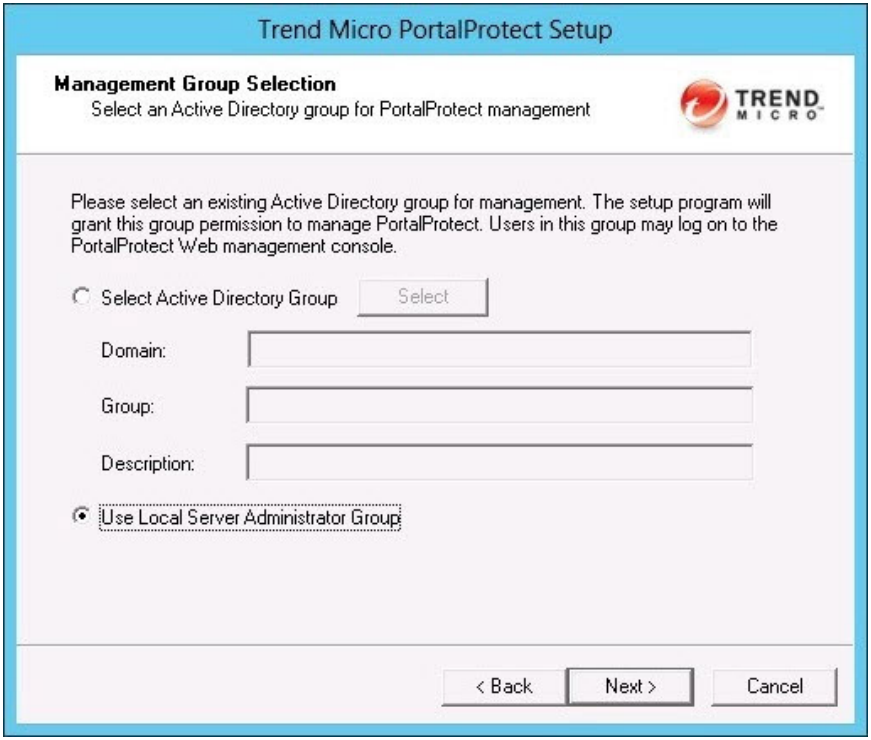

図 2-11. [Management Group Selection] 画面

注意

既存の Active Directory グループを使用するか、この手順を完了する前に新しいグループを作成する必要があります。[Use Local Server Administrator Group] を選択した場合、各インストール先サーバの管理者権限を持つアカウントは、ローカルの PortalProtect 管理コンソールにログオンできます。

14. ここで Active Directory グループを選択しない場合は [Use Local Server Administrator Group] を選択します。または、次の手順で Active Directory グループを選択します。

    [Select Active Directory Group] を選択し、[Select] をクリックして既存グループを選択します。[Domain]、[Group]、[Description] の順に入力します。

15. [Next >] をクリックします。

    [Connection Settings] 画面が表示されます。

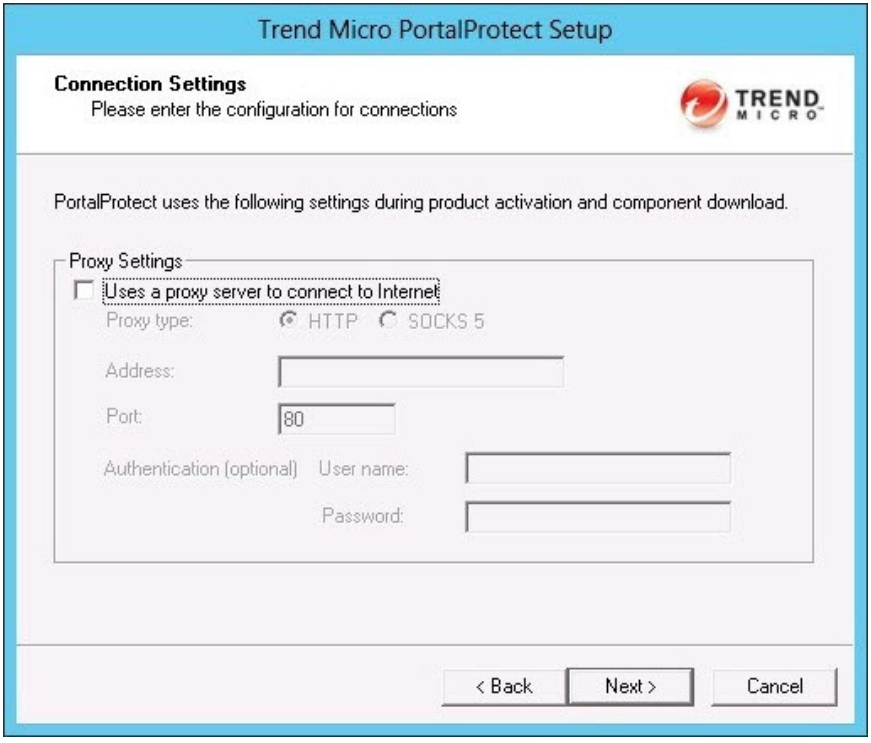

図 2-12. [Connection Settings] 画面

プロキシサーバを使用する場合は、[Uses a proxy server to connect to Internet] を選択して、次の情報を入力します。

- Proxy type — [HTTP] または [SOCKS 5]
- Address — IP アドレス
- Port — ポート番号
- プロキシサーバがパスワードを要求する場合は、ユーザ名とパスワードをそれぞれ [User name] と [Password] に入力します。

16. [Next >] をクリックします。

    [Control Manager Server Settings] 画面が表示されます。

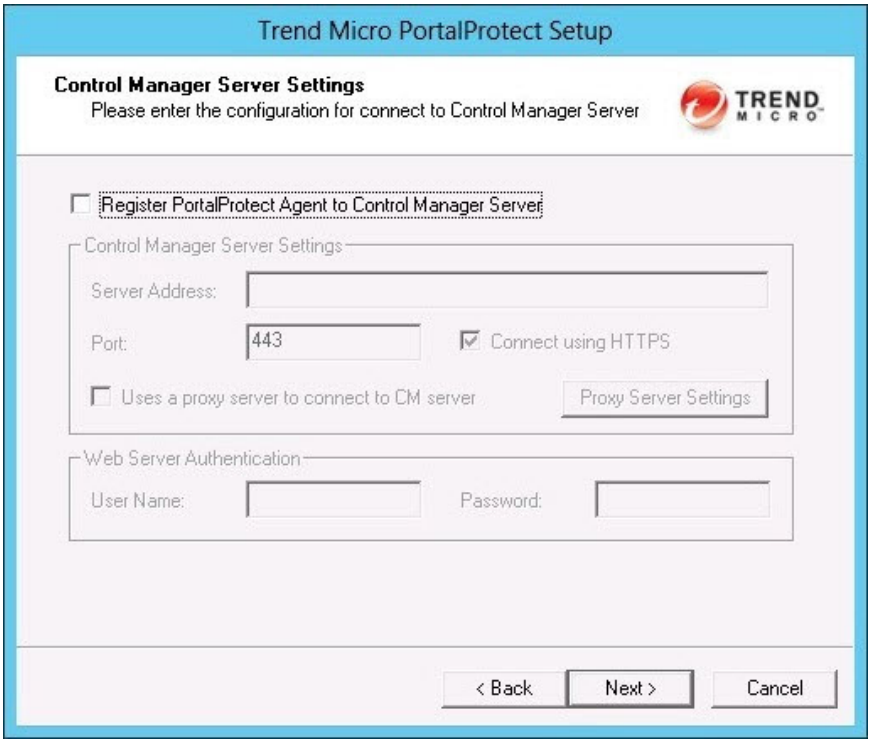

図 2-13. [Control Manager Server Settings] 画面

17. [Next >] をクリックして次の設定に進んでください。

- Server Address
- Port — ポート番号
- Connect using HTTPS (必要に応じて)
- プロキシサーバを使用する場合は、[Uses a proxy server to connect to CM server] を選択し、[Proxy Server Settings] をクリックして変更します。詳細については、管理者ガイドを参照してください。
- [Web Server Authentication]が必要な場合は、ユーザ名とパスワードをそれぞれ [User Name] と [Password] に入力してください。

18. [Next >] をクリックします。

[Email Notification Settings] 画面が表示されます。

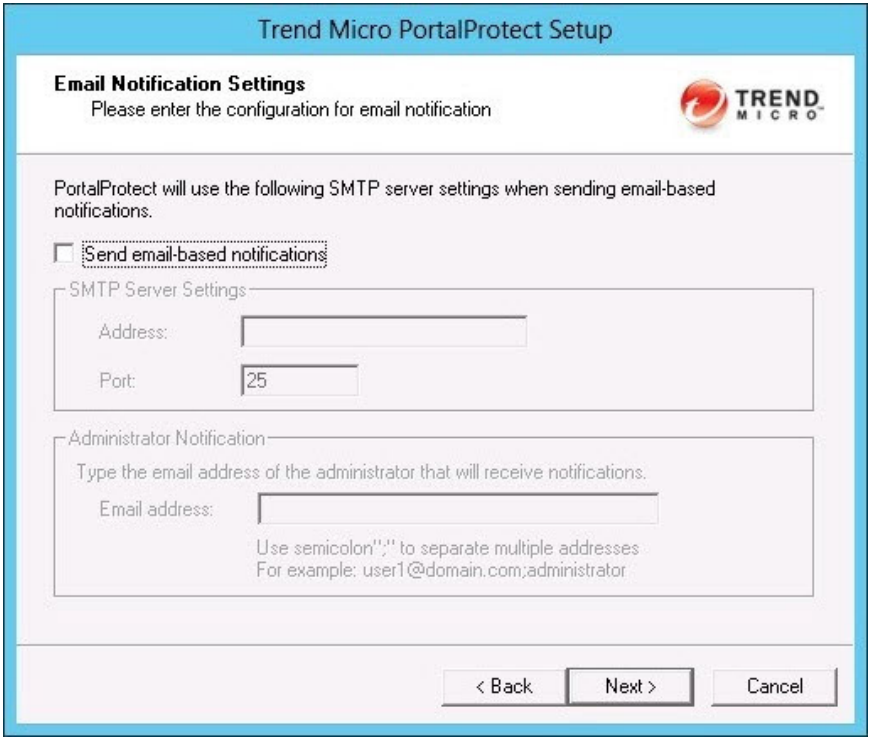

図 2-14. [Email Notification Settings] 画面

通知をメールで送信する場合は、次の情報を入力します。

- [Send email-based notifications] を選択します。
- [Address] と [Port] に SMTP サーバのアドレスとポートを入力します。
- 管理者へのメール通知を有効にするには、[Email address] に管理者のメールアドレス (複数可) を入力します。複数のアドレスはセミコロン (;) で区切ります。

19. [Next >] をクリックします。

    [Review Settings] 画面が表示されます。

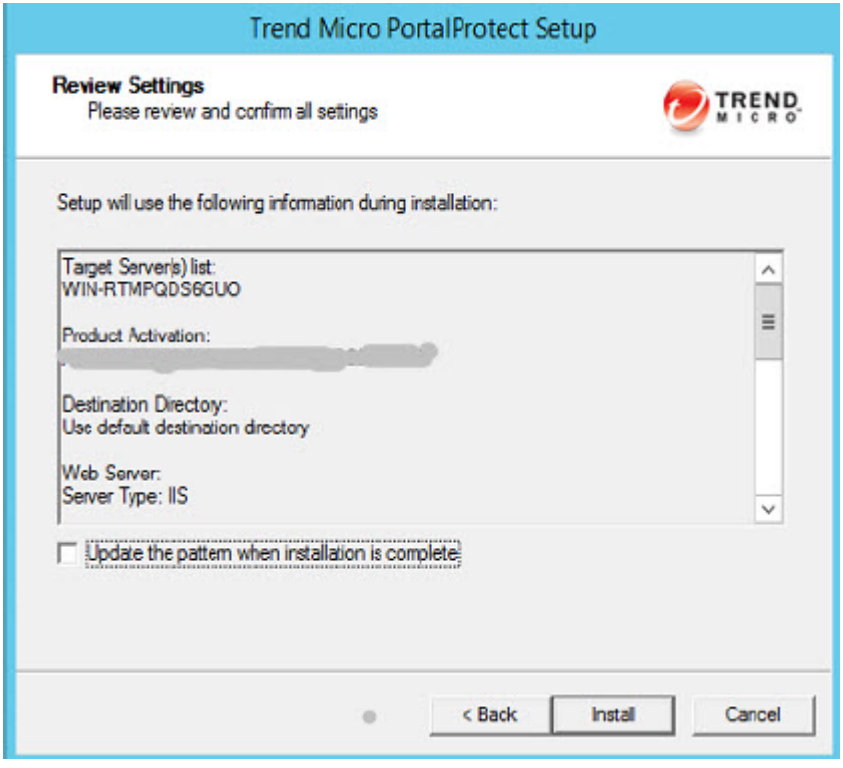

図 2-15. [Review Settings] 画面

20. 画面に表示された設定を確認し、変更が必要な場合には前の手順に戻ります。インストールの完了時にパターンファイルをアップデートする場合は、[Update the pattern when installation is complete] をクリックします。[Install] をクリックします。

[Installation Progress] 画面が表示されます。

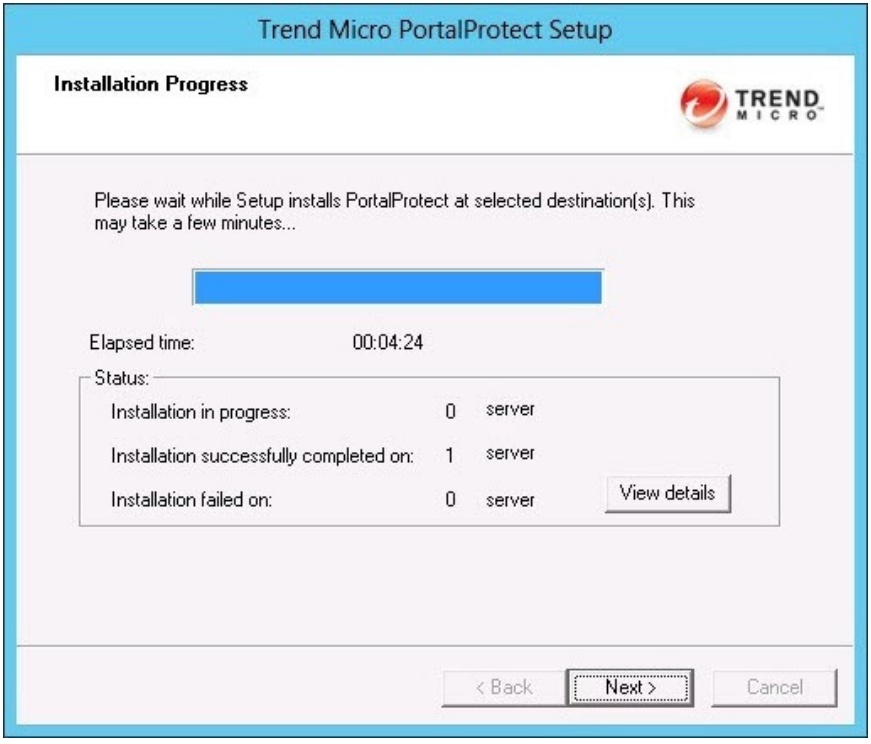

図 2-16. [Installation Progress] 画面

21. インストールの間は、[View details] をクリックしてステータスを確認します。

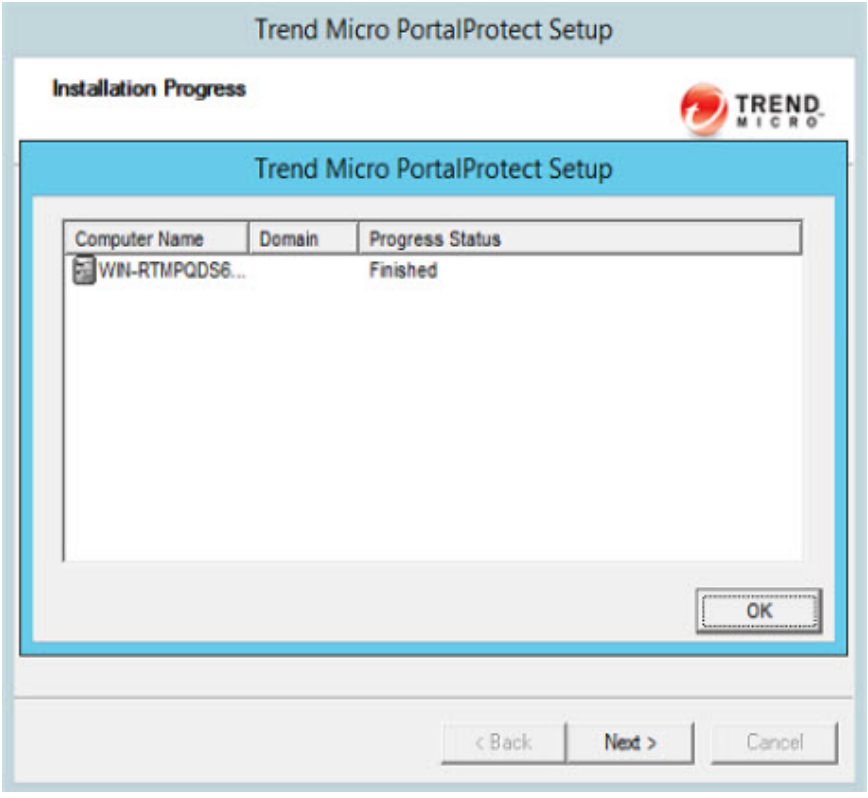

図 2-17. インストールの進行状況 (終了時)

22. インストールの進行状況が [Finished] と表示されたら、[Next >] をクリックします。

[Installation Complete] 画面が表示されます。

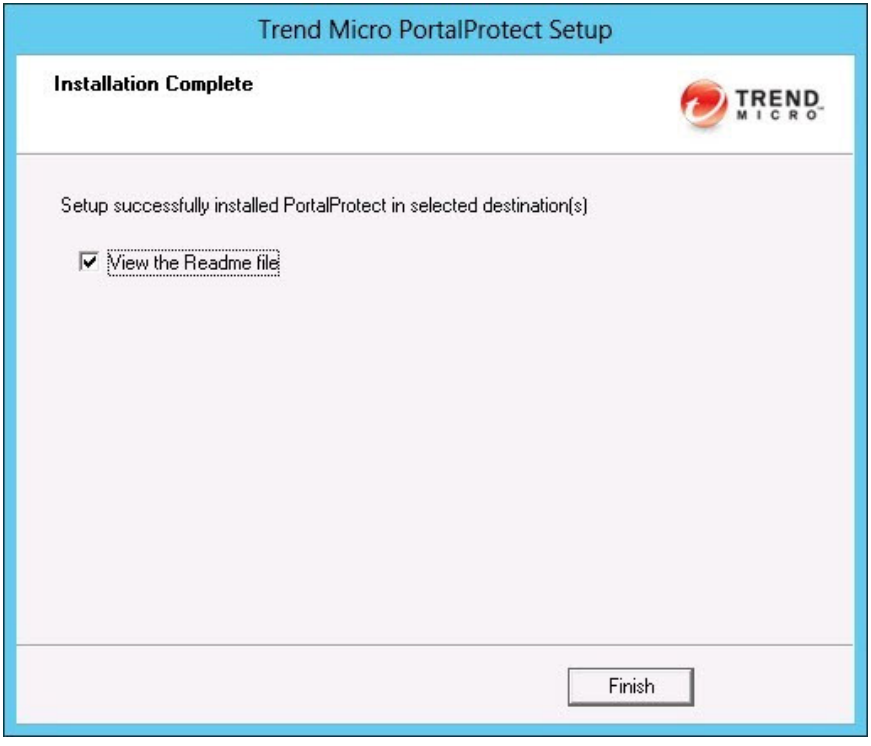

図 2-18. [Installation Complete] 画面

23. Readme ファイルを表示する場合は [View the Readme file] を選択し、[Finish] をクリックしてインストールを完了します。

新規サイレントインストール

新規サイレントインストールでは、INI ファイルにインストールパラメータを事前に指定することで、管理者による操作なしに PortalProtect がインストールされます。サイレントインストールを実行するには、PortalProtect のセットアップパッケージまたはビルドを取得する必要があります。

手順

1. PortalProtect のセットアップパッケージに移動して、実行可能ファイルの一覧を表示します。
2. PortalProtect のセットアップパッケージのすべてのファイルを、`SilentSetup.bat` ツールとともに PortalProtect のサイレントインストールを実行する場所にコピーします。
3. ファイルをコピーしたら、コマンドプロンプトを開いて、指定された場所に現在のディレクトリを変更します。

警告!

サイレントインストールには silentsetup.bat を使用する必要があります。setup.exe は使用しないでください。

4. 「SilentSetup.bat /?」と入力し、サイレントインストールの手順で使用できるオプションの一覧を表示します。

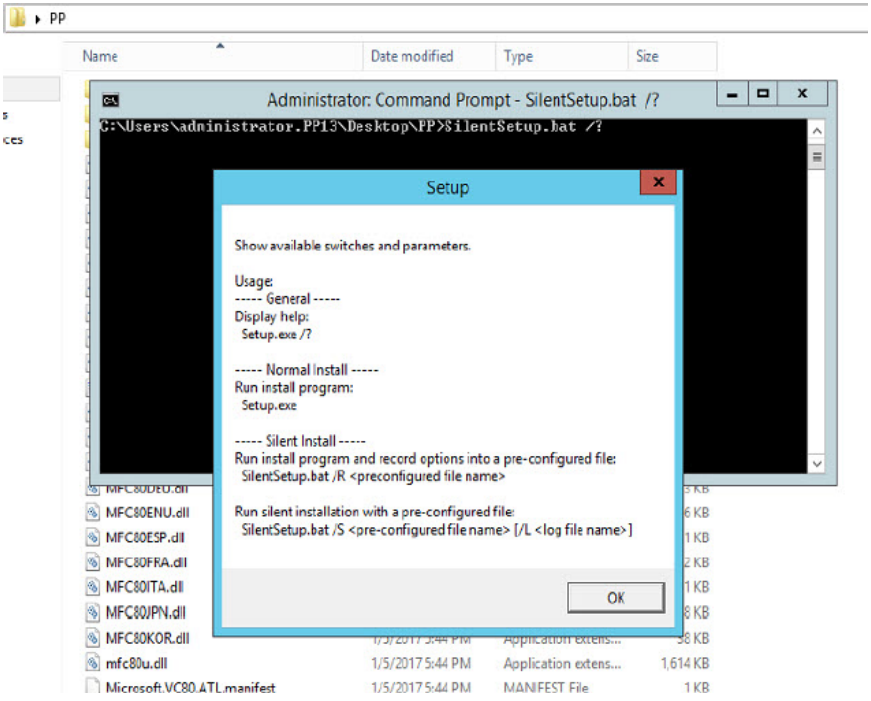

図 2-19. サイレントセットアップのヘルプ

5. 「`SilentSetup /R`」と入力してサイレントインストールの手順を開始します。[Trend Micro PortalProtect Setup] 画面が表示されます。

注意

この手順によって、PortalProtect のサイレントインストールで使用する設定が記録されます。

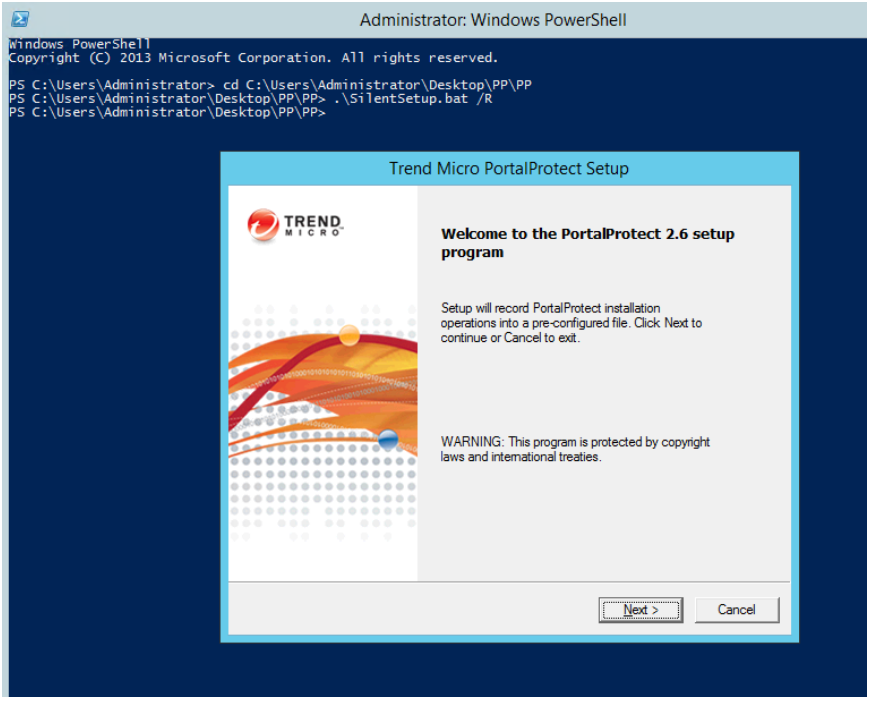

図 2-20. サイレントインストールの開始画面

注意

事前設定ファイルは、「SilentSetup /R <事前設定ファイル>」コマンドを使用して特定のパスに保存できます。事前設定ファイルを指定しない場合、事前設定ファイルは`%Windir%¥temp` の `Setup-PortalProtect.iss` に設定されます。

ツールによって事前設定ファイル Setup-PortalProtect.iss が生成されます。初期設定のファイルパスは、フォルダ%windir%¥temp になります。

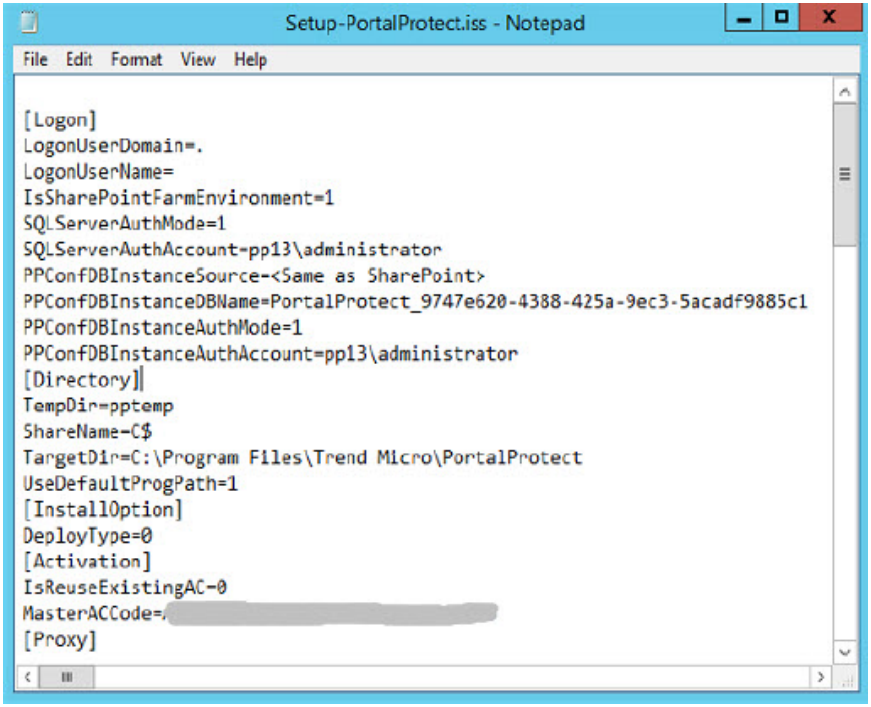

図 2-21. Setup-PortalProtect.iss ファイル

警告!

すべてのパスワードはセキュリティのために暗号化されます。ConsoleGroup または ServerManagementGroupSid は変更しないでください。

6. SilentSetup /S <*事前設定ファイル*> を実行して、PortalProtect の無人インストールを実行するサイレントインストールを有効にします。

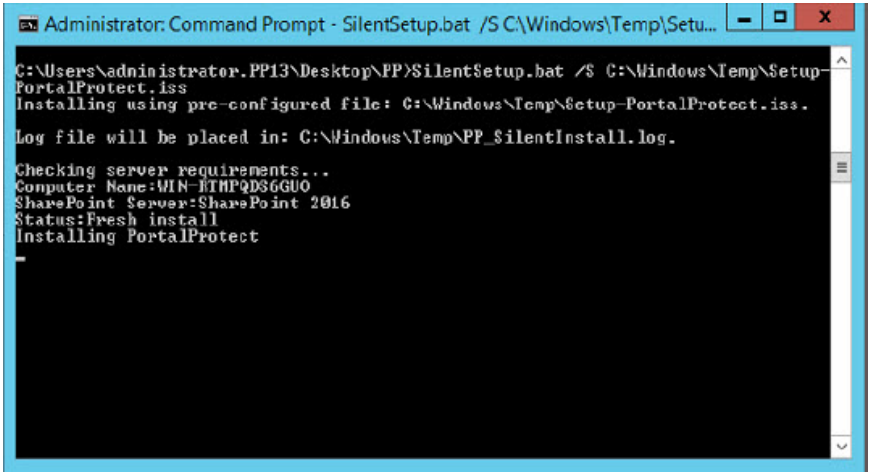

図 2-22. インストール画面

Setup によってコンピュータに PortalProtect がインストールされると、`%windir%¥temp` フォルダにセットアップログファイルが作成されます。

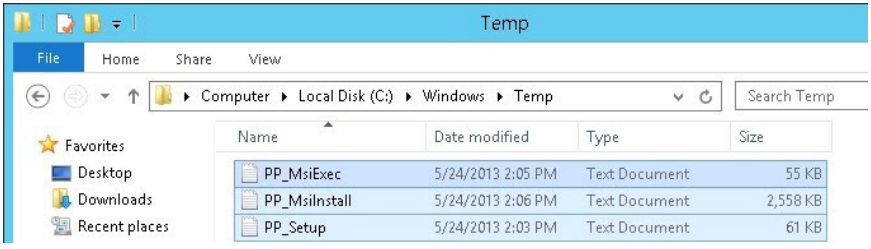

図 2-23. セットアップログファイル

注意

サイレントインストールでは、選択した任意のパスに PortalProtect をインストールできます。これは、`%ProgramFiles%¥Trend Micro ¥PortalProtect` のように、初期設定のシステムの Program Files フォルダに PortalProtect をインストールするセットアッププログラムとは異なります。

インストール後の作業

重要

PortalProtect のインストール後、[SharePoint サーバーの全体管理] のウイルス対策設定と、PortalProtect 管理コンソールの Web コンテンツ検索設定を行います。これにより、PortalProtect が正しく機能します。

手順

1. SharePoint Server のウイルス対策設定を有効にします。
   a. SharePoint から、[SharePoint サーバーの全体管理] > [セキュリティ] > [一般的なセキュリティ] > [ウイルス対策設定の管理] の順に選択します。
   b. 次のオプションを有効にしてください。
      - アップロード時にドキュメントをスキャンする
      - ダウンロード時にドキュメントをスキャンする
      - 感染したドキュメントを正常な状態に戻す
2. PortalProtect で Web コンテンツ検索設定を有効にします。
   a. PortalProtect から、[PortalProtect Management Console] > [Summary] > [System] > [Microsoft SharePoint Services] の順に選択します。
   b. 次のオプションを有効にしてください。
      - Scan Web content

      注意

      ウイルス検索とウイルスシグネチャについて PortalProtect のステータスの更新を定期的にチェックする SharePoint Administration サービスが開始されていることを確認します。サービスのステータスは、[スタート] > [プログラム] > [管理ツール] > [サービス] の順に選択して確認できます。

PortalProtect サーバにウイルス対策製品がインストールされている場合は、次のフォルダを検索しないように設定します。

- 仮定するインストールフォルダ: `C:¥Program Files¥Trend Micro ¥PortalProtect`
- 一時フォルダ: `C:¥Program Files¥Trend Micro¥PortalProtect¥temp`
- バックアップフォルダ (初期設定の場所): `C:¥Program Files¥Trend Micro¥PortalProtect¥storage¥Backup`
- 共有リソースプールフォルダ (初期設定の場所): `C:¥Program Files ¥Trend Micro¥PortalProtect¥SharedResPool`

  たとえば、Trend Micro ServerProtect を使用している場合、これらのフォルダを除外フォルダリストに追加します。

PortalProtect のアップグレード

PortalProtect は、次の 2 種類の方法でアップグレードできます。

- インストールプログラム (`setup.exe`) を使用する (47 ページの「セットアッププログラムを使用したアップグレード」を参照)
- サイレントインストールプログラム (`SilentSetup.bat`) を使用する (40 ページの「新規サイレントインストール」を参照)

セットアッププログラムを使用したアップグレード

手順

1. アップグレードパッケージから Setup.exe を実行します。

開始画面が表示されます。

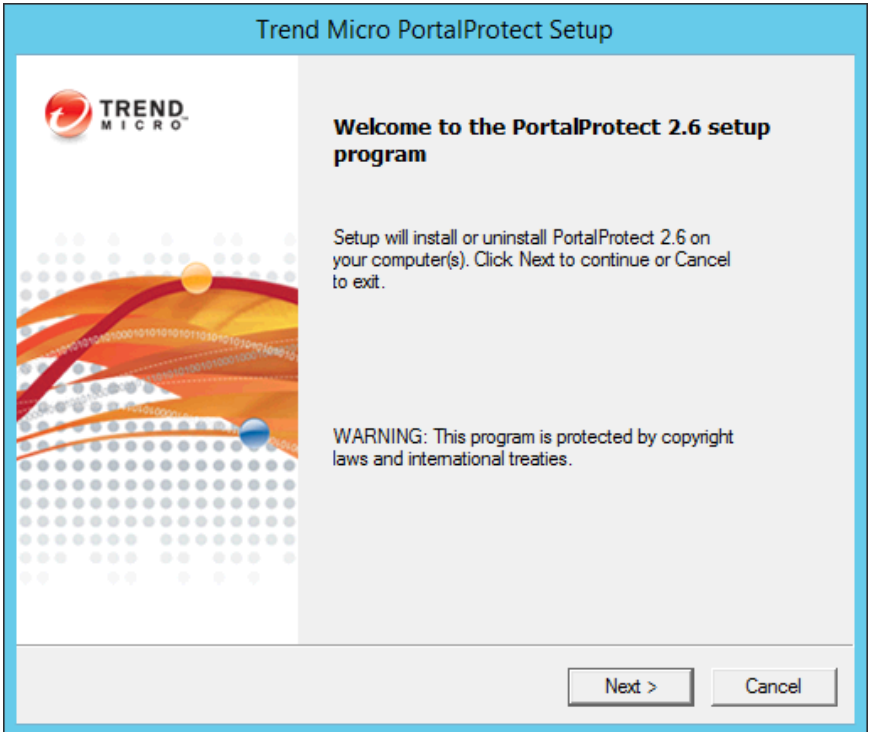

図 2-24. PortalProtect アップグレードの開始画面

2. [Next >] をクリックします。

[License Agreement] 画面が表示されます。

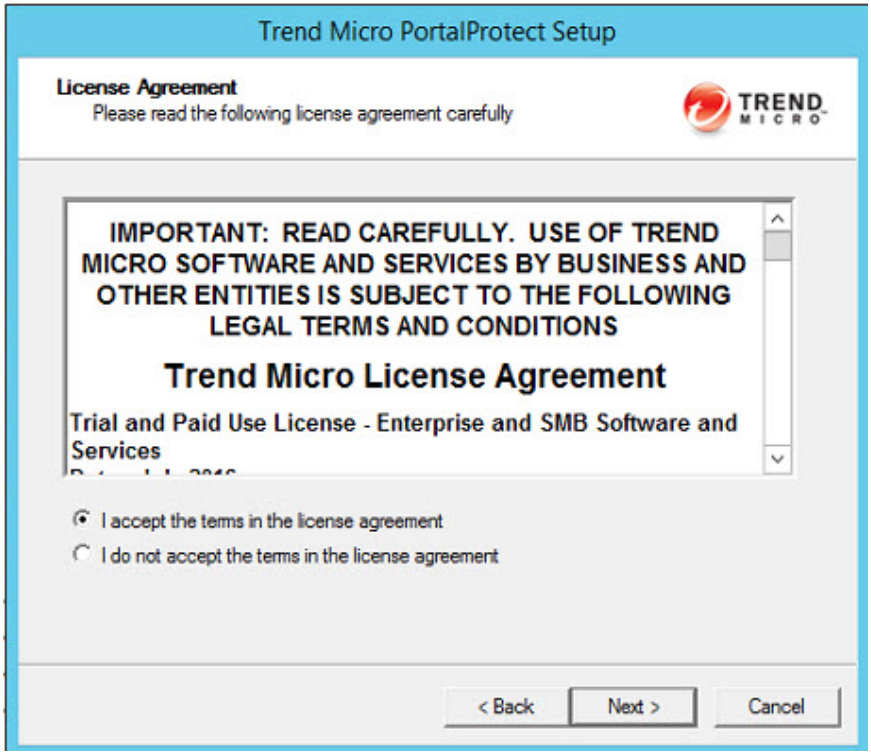

図 2-25. [License Agreement] 画面

3. 使用許諾契約書を確認します。契約に同意する場合は、[I accept the terms in the license agreement] を選択して [Next >] をクリックします。セットアッププログラムによって、システムが要件を満たしているかどうかのチェックが開始されます。契約に同意できない場合は、[Cancel] をクリックしてセットアッププログラムを終了します。

[Select an Action] 画面 (1) が表示されます。

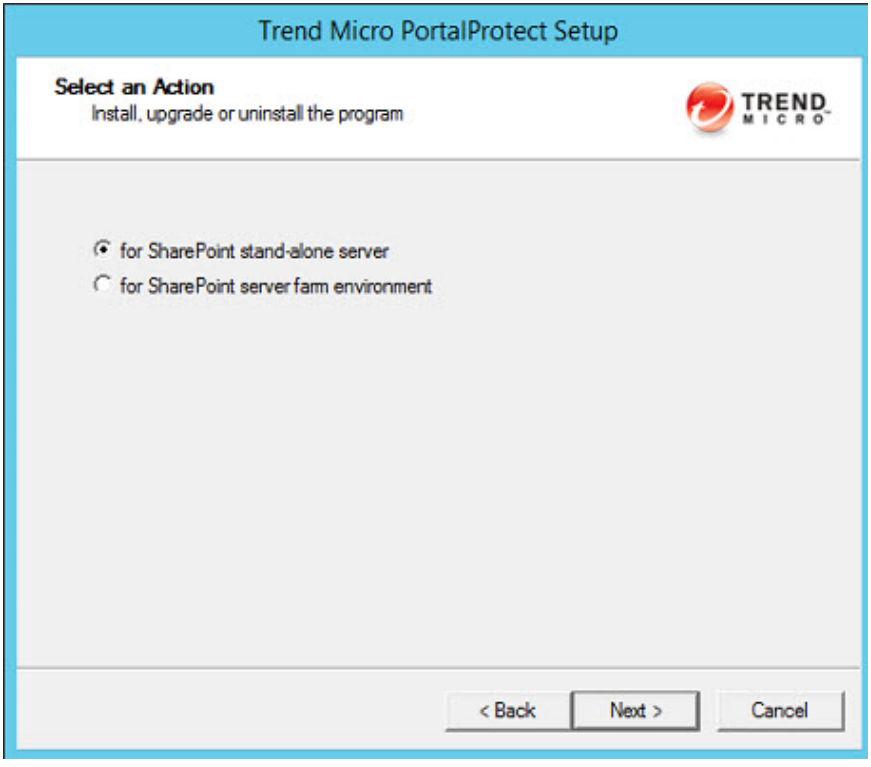

図 2-26. [Select an Action] 画面 (1)

4. 次のいずれかのインストールオプションを選択します。
   - for SharePoint stand-alone server
   - for SharePoint server farm environment
5. 適切なオプションを選択したら、[Next >] をクリックします。

注意

SharePoint の配置モードに応じて、SharePoint スタンドアロンサーバへのインストール ([for SharePoint stand-alone server]) を選択するか、SharePoint サーバファーム環境へのインストール ([for SharePoint server farm environment]) を選択します。SharePoint をファームモードで配置する場合は、[for SharePoint server farm environment] を選択する必要があります。一方、SharePoint をスタンドアロンモード (基本的な配置) で配置する場合は、[for SharePoint stand-alone server] を選択する必要があります。

[Select an Action] 画面 (2) が表示されます。

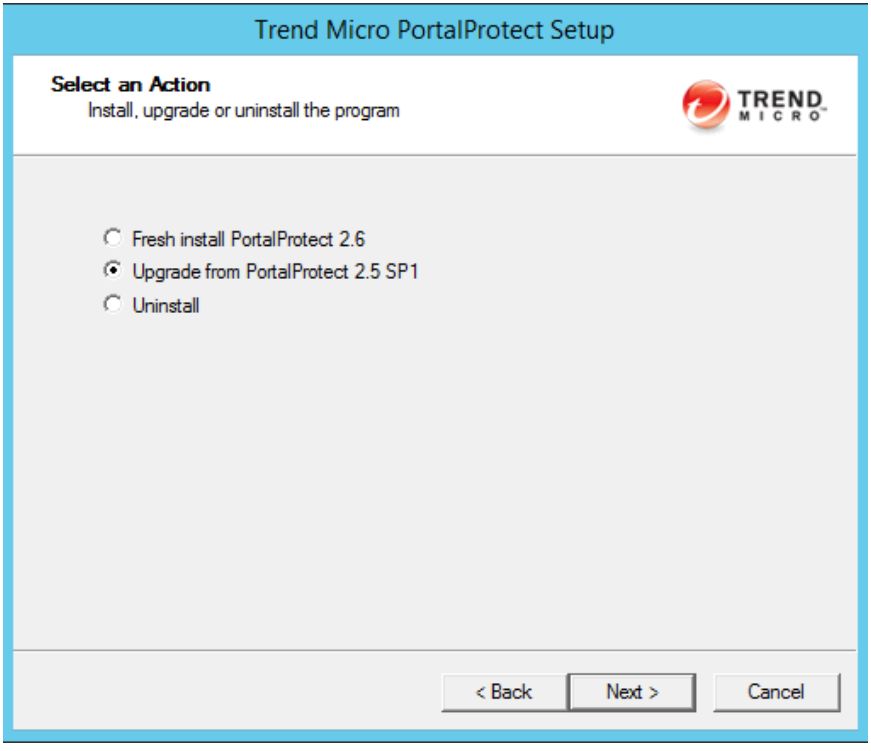

図 2-27. [Select an Action] 画面 (2)

6. [Upgrade from PortalProtect 2.5 SP1] を選択して [Next >] をクリックします。

[Product Activation] 画面が表示されます。

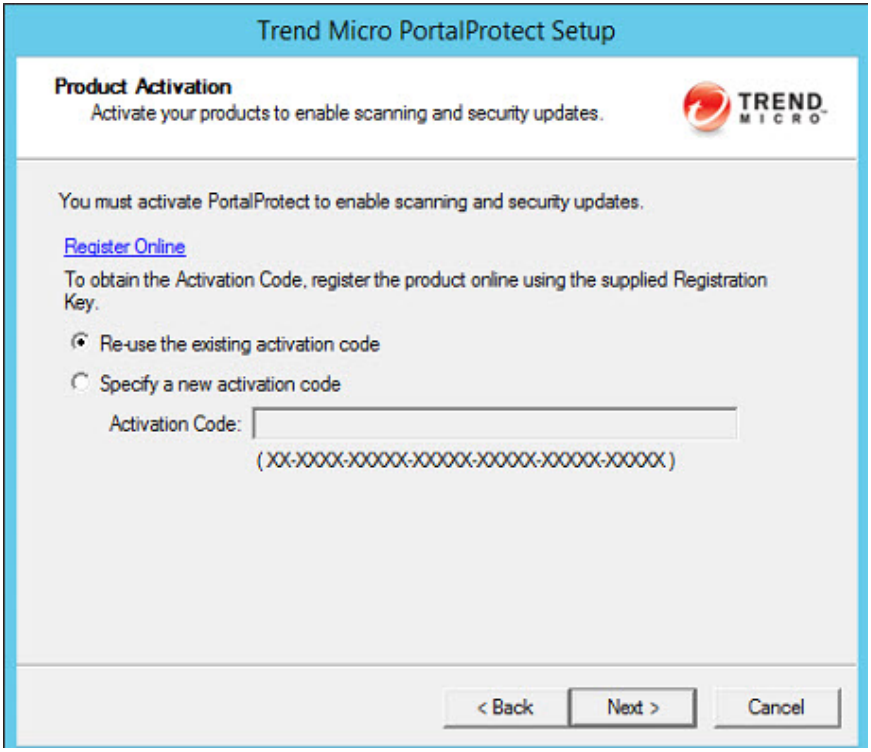

図 2-28. [Product Activation] 画面

7. アクティベーションコードを入力します。既存のアクティベーションコードを使用することも、新しく指定することもできます。[Next >] をクリックします。

[Select Target Server(s)] 画面が表示されます。

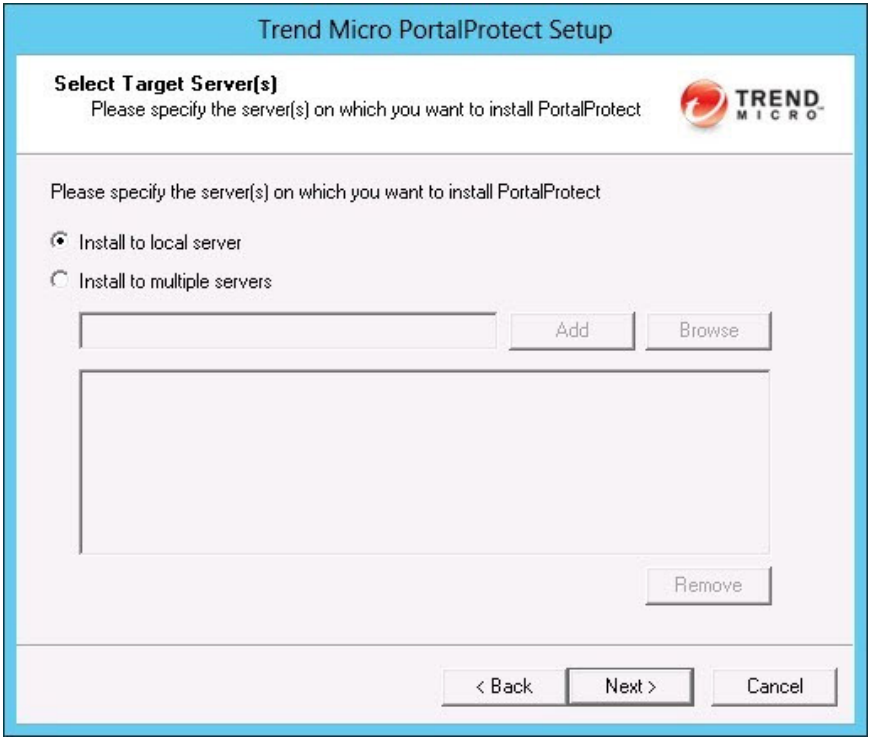

図 2-29. [Select Target Server(s)] 画面

8. 次のオプションから選択します。

   - Install to local server (推奨) — ローカルサーバにインストールします。選択したら、[Next >] をクリックしてインストールを続行します。
   - Install to multiple servers (リモートインストール) — PortalProtect をインストールするインストール先サーバを選択します。コンピュータ名を入力するか [Computer name] の [Browse] をクリックしてコンピュータを参照し、1 つまたは複数のサーバを [Add] をクリックして追加します。すべてのインストール先サーバをリストに追加したら、[Next >] をクリックしてインストールを続行します。リ

モートサーバのログオンアカウント情報を入力するように求められます。

[Configure Shared/Target Directory] 画面が表示されます。

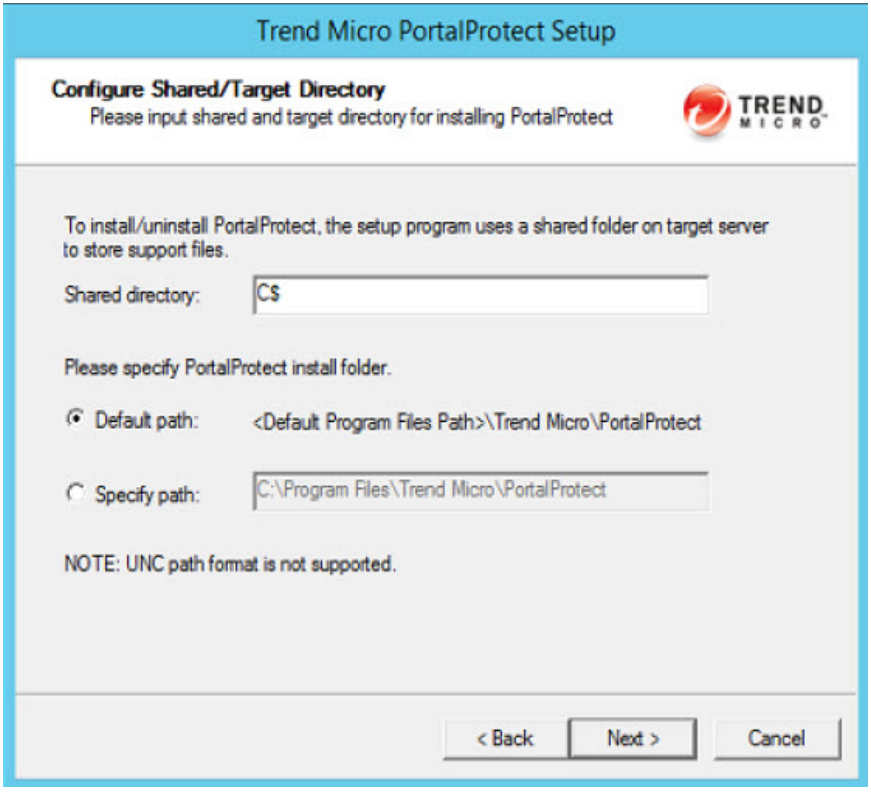

図 2-30. [Configure Shared/Target Directory] 画面

9. インストール先サーバの共有フォルダの初期設定パスをそのまま使用するか、[Specify path] に新しいパスを入力します。[Next >] をクリックします。

警告!

[Specify path] フィールドには英字のみを入力してください。そうしないと、インストールが正常に実行されません。

注意

PortalProtect では、共有ディレクトリに C$、D$などの Windows の初期設定の共有のみを使用できます。

[Web Server Information] 画面が表示されます。

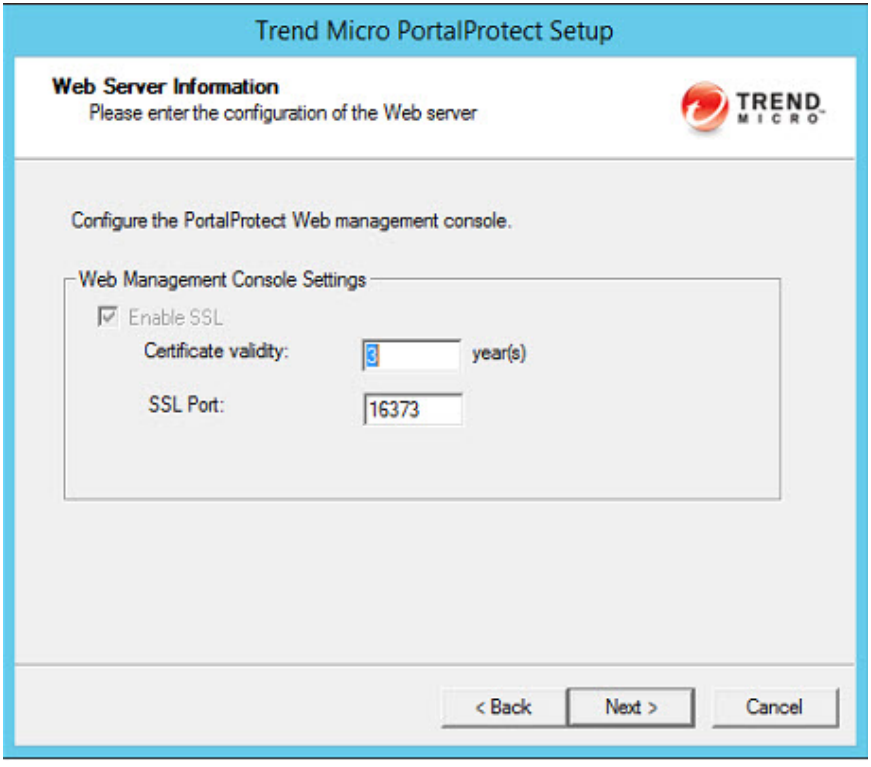

図 2-31. [Web Server Information] 画面

10. [SSL Port] に、Web 管理コンソールの SSL ポート番号を入力します。[Next >] をクリックします。

[PortalProtect Configuration Database] 画面が表示されます。

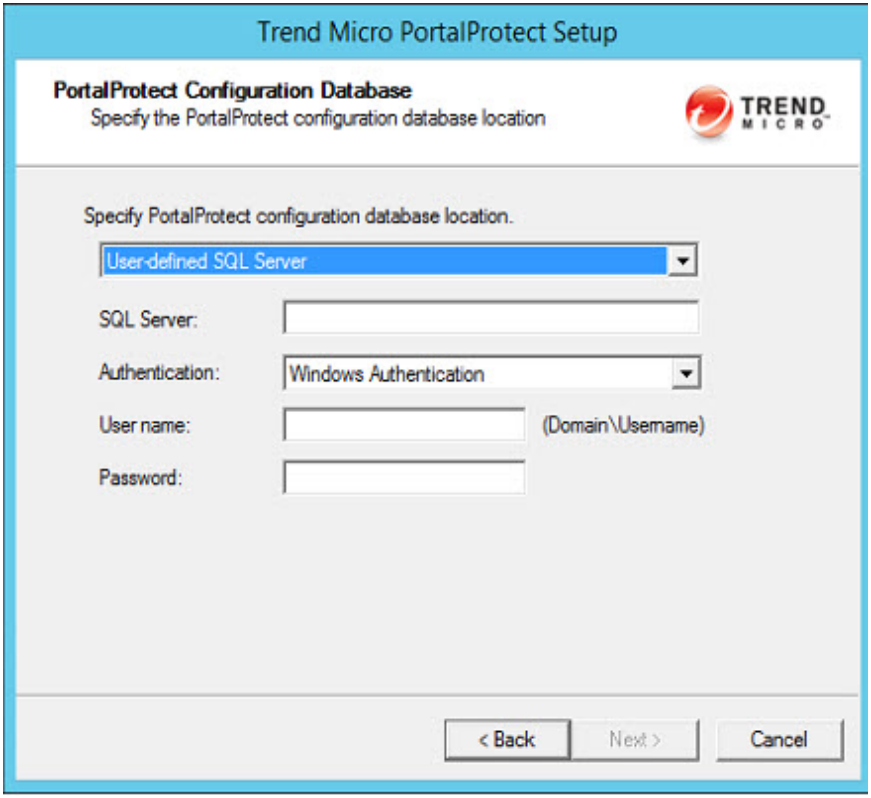

図 2-32. [PortalProtect Configuration Database] 画面

注意

前のバージョンと同じデータベース設定を使用してください。

11. 次のオプションから選択します。
    - Specify PortalProtect configuration database location:
        - SharePoint SQL Server — PortalProtect を SharePoint SQL Server にインストールします。

- User-defined SQL Server — PortalProtect をユーザ定義 SQL Server にインストールします。

注意

PortalProtect 設定データベースを自動作成するか既存の PortalProtect 設定データベースを使用するには、dbcreator 権限を持つアカウントでインストールを実行する必要があります。dbcreator の役割が使用できない場合は、93 ページの「データベース権限の要件」を参照してください。

- Authentication — [Windows Authentication] と [SQL Server Authentication] のいずれかを選択します。

注意

[Windows Authentication] を使用することを強くお勧めします。

- User name — 必要に応じて入力します。
- Password — 必要に応じて入力します。

12. [Next >] をクリックします。

[Checking Target Server System Requirements] 画面が表示されます。

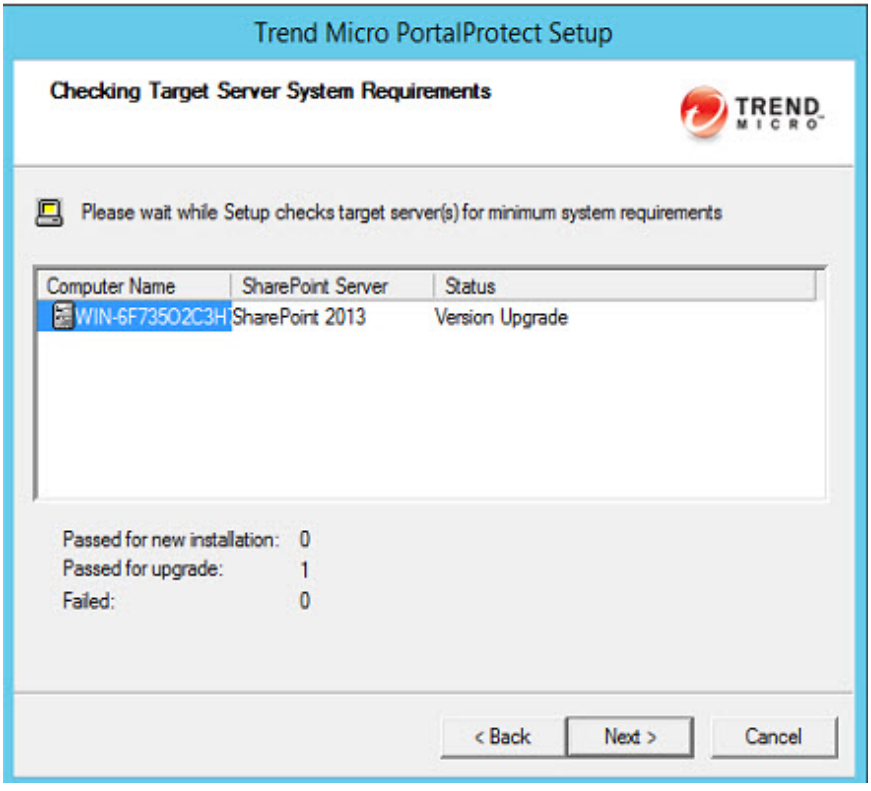

図 2-33. [Checking Target Server System Requirements] 画面

PortalProtect をインストールする各インストール先サーバで、インストールプログラムによって次の項目についてシステムが分析されます。

PortalProtect がインストールされているかどうか

- PortalProtect 2.5 SP1 がインストールされているかどうか
- インストール先サーバで正しいバージョンの Windows が実行されているかどうか

- インストール先サーバで正しい SharePoint のバージョンによって Web アプリケーションが実行されているかどうか
- インストール先サーバにログオンするための適切な権限が与えられているかどうか
- SharePoint データベースのアクセスアカウントが PortalProtect 2.5 SP1 と同じかどうか
- PortalProtect データベースのアクセスアカウントが PortalProtect 2.5 SP1 と同じかどうか

13. [Status] に [Fresh Install] と表示されていることを確認して、[Next >] をクリックします。

[Management Group Selection] 画面が表示されます。

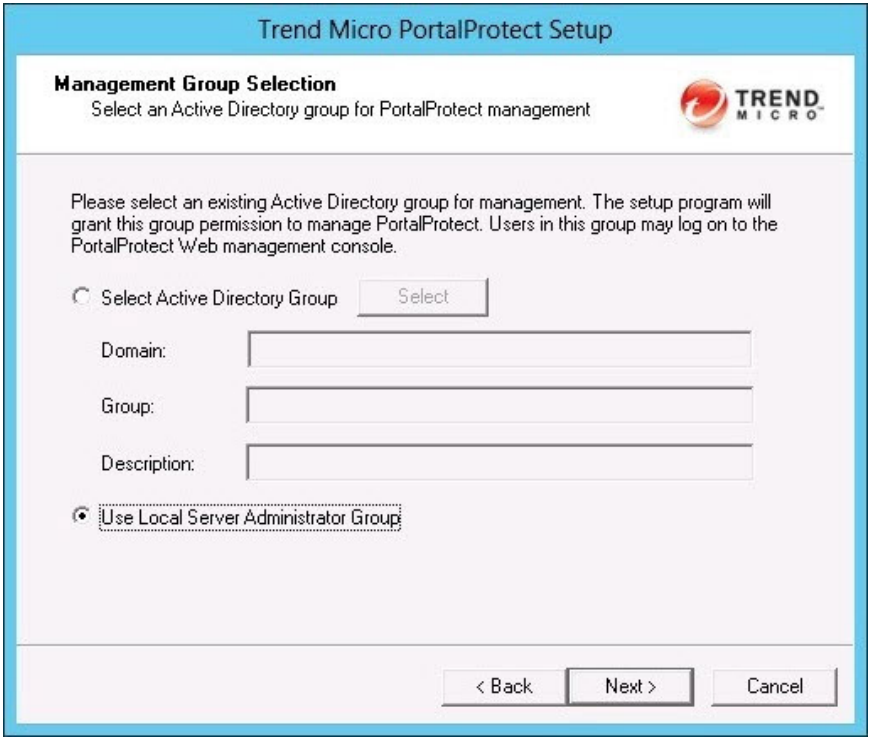

図 2-34. [Management Group Selection] 画面

注意

既存の Active Directory グループを使用するか、この手順を完了する前に新しいグループを作成する必要があります。[Use Local Server Administrator Group] を選択した場合、各インストール先サーバの管理者権限を持つアカウントは、ローカルの PortalProtect 管理コンソールにログオンできます。

14. ここで Active Directory グループを選択しない場合は [Use Local Server Administrator Group] を選択します。または、次の手順で Active Directory グループを選択します。

[Select Active Directory Group] を選択し、[Select] をクリックして既存グループを選択します。[Domain]、[Group]、[Description] の順に入力します。

15. [Next >] をクリックします。

    [Review Settings] 画面が表示されます。

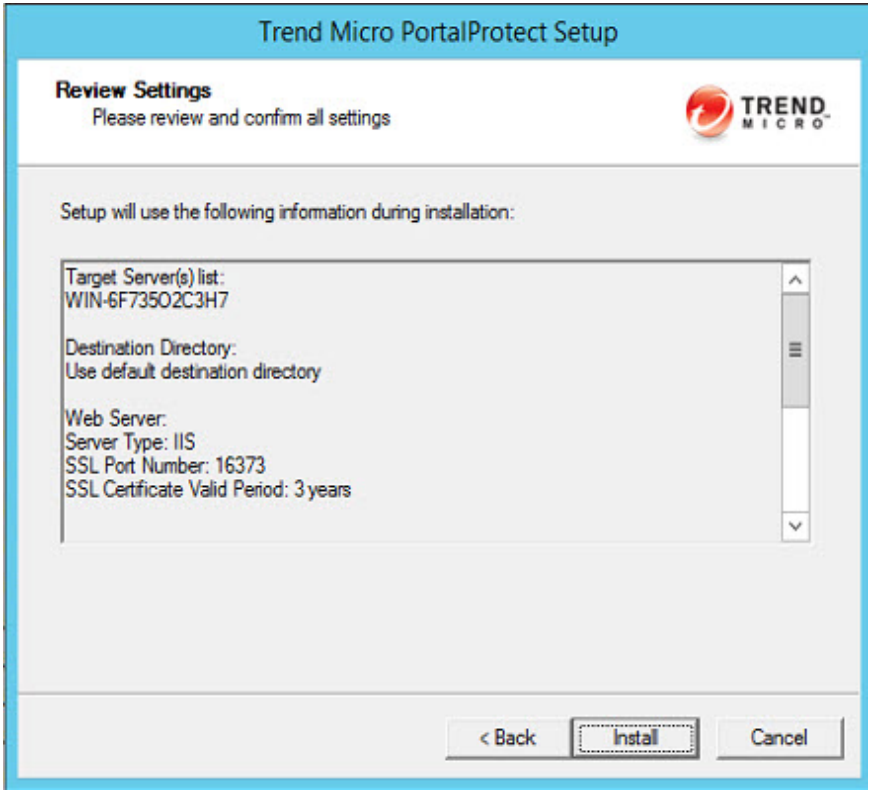

図 2-35. [Review Settings] 画面

16. 画面に表示された設定を確認し、変更が必要な場合には前の手順に戻ります。インストールの完了時にパターンファイルをアップデートする場合は、[Update the pattern when installation is complete] をクリックします。[Install] をクリックします。

[Installation Progress] 画面が表示されます。

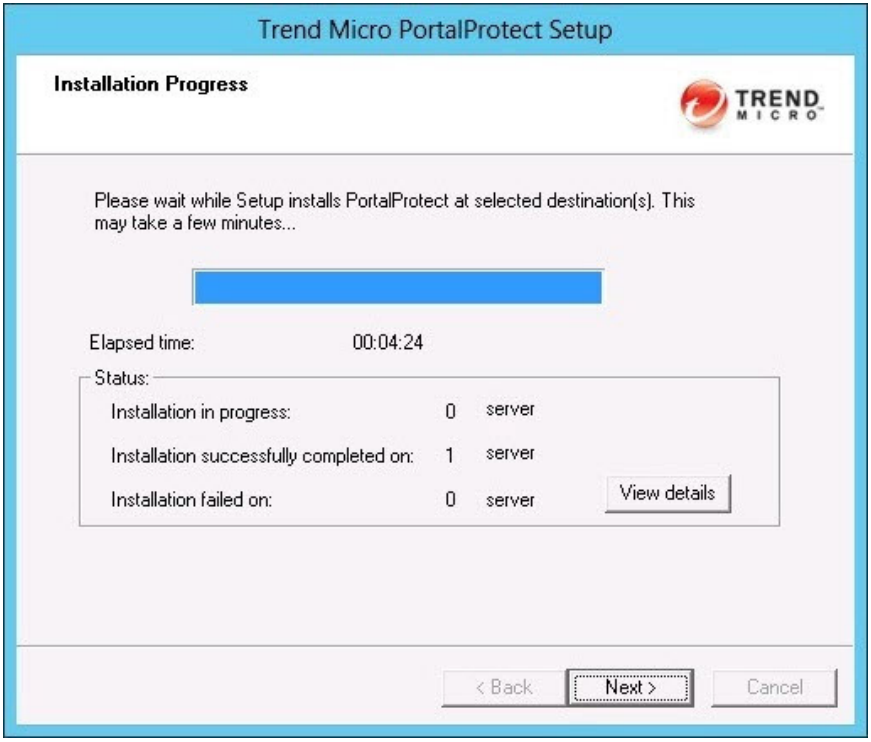

図 2-36. [Installation Progress] 画面

17. インストールの間は、[View details] をクリックしてステータスを確認します。

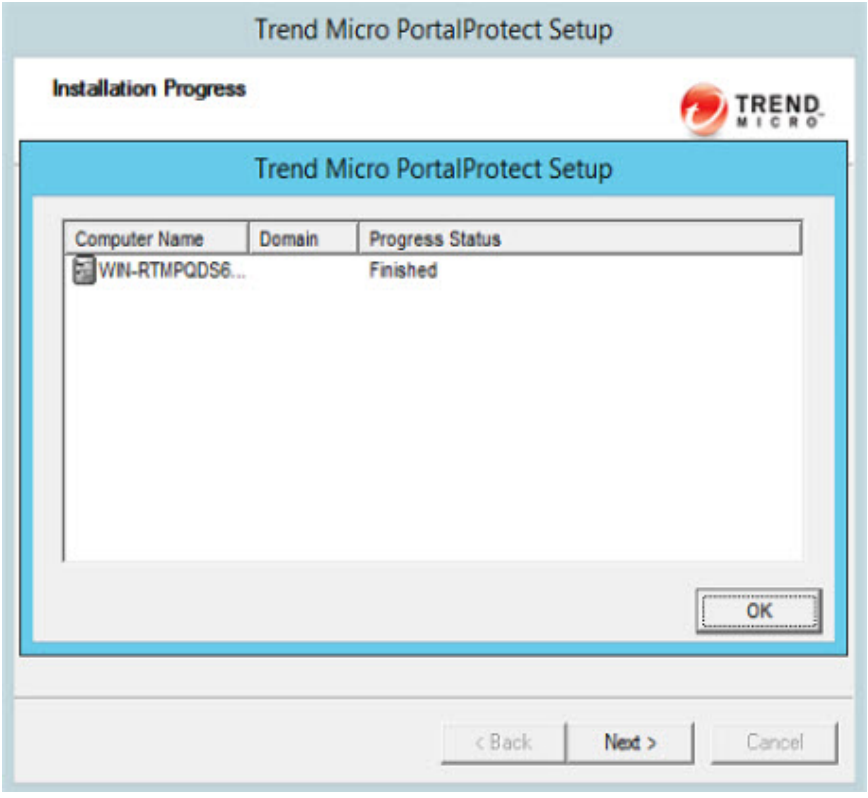

図 2-37. インストールの進行状況 (終了時)

18. インストールの進行状況が [Finished] と表示されたら、[Next >] をクリックします。

[Installation Complete] 画面が表示されます。

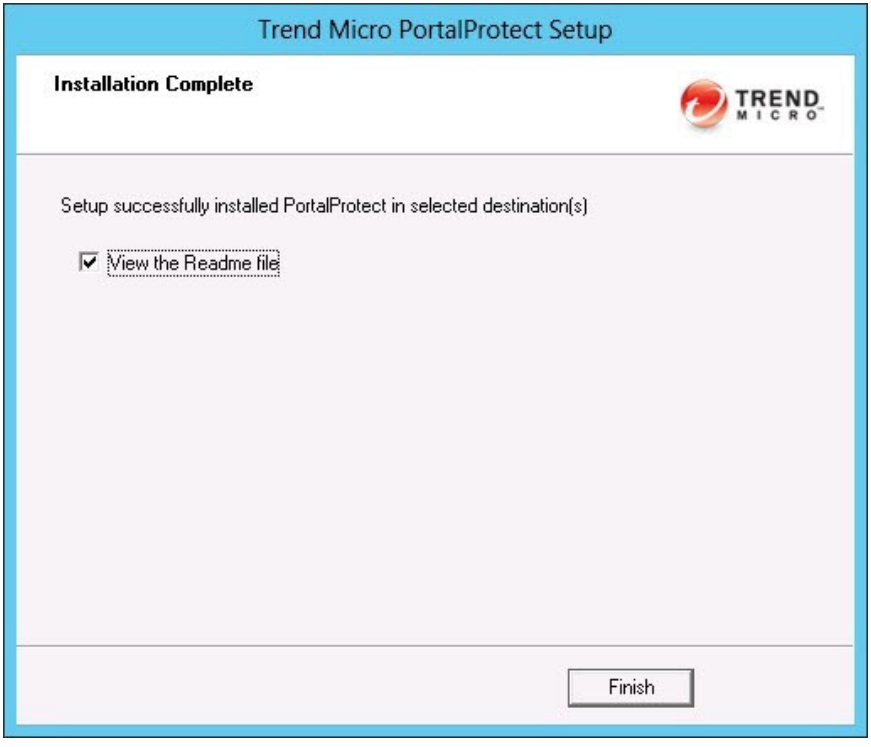

図 2-38. [Installation Complete] 画面

19. Readme ファイルを表示する場合は [View the Readme file] を選択し、[Finish] をクリックしてインストールを完了します。

インストール後のテスト

インストール状態は、EICAR テストスクリプトを使用して確認することをお勧めします。EICAR (European Institute for Computer Antivirus Research) は、ウイルス対策ソフトウェアが適切にインストールされ、設定されている

ことを確認するための安全な方法として、テキストスクリプトを開発しています。詳細については、EICAR の Web サイトを参照してください。

http://www.eicar.org

EICAR テストスクリプトは、.com 拡張子の付いた無害のテキストファイルです。これはウイルスではなく、ウイルスコードの断片も含まれていませんが、ほとんどのウイルス対策ソフトウェアはウイルスが存在するものとして反応します。このファイルを使用してウイルス感染を実行し、メール通知、HTTP 検索、およびウイルスログが適切に動作していることを確認します。

警告!

ウイルス対策のソフトウェアをテストする目的で実際のウイルスを使用しないでください。

手順

1. ASCII テキストファイルを開いて、次の 68 文字の文字列をコピーします。

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

2. ファイルを EICAR.com の名前で temp ディレクトリに保存します。コンピュータにウイルス対策ソフトウェアがインストールされている場合は、このファイルがただちに検出されます。

3. ネットワークに配置されている SharePoint が PortalProtect によって現在保護されていることをテストするには、`EICAR.com` ファイルを SharePoint サイトにアップロードします。

   注意

   ZIP 圧縮された EICAR ファイルをテストすることもお勧めします。圧縮ソフトウェアを使用して、テストスクリプトを ZIP 圧縮し、上記の手順を実行します。

PortalProtect のアンインストール

PortalProtect をアンインストールする方法には、次の 2 つがあります。

- Windows のコントロールパネルから [プログラムのアンインストール] を使用する (推奨)
- `Setup.exe` プログラムを使用する

PortalProtect のローカルまたはリモートでのアンインストールは、簡単なアンインストールプログラムを使用して実行できます。このプログラムによって、1 つまたは複数のサーバから PortalProtect を容易に削除できます。

これらのサーバはネットワーク内に存在する必要があり、設定するユーザには管理者権限が必要です。

注意

ローカルサーバの場合は、Windows のコントロールパネルにあるプログラムの削除機能を使用することもできます。ただし、PortalProtect をリモートのサーバから削除するには、`setup.exe` プログラムを使用する必要があります。

手順

1. `Setup.exe` を参照して実行します。

PortalProtect のセットアッププログラム画面が表示されます。

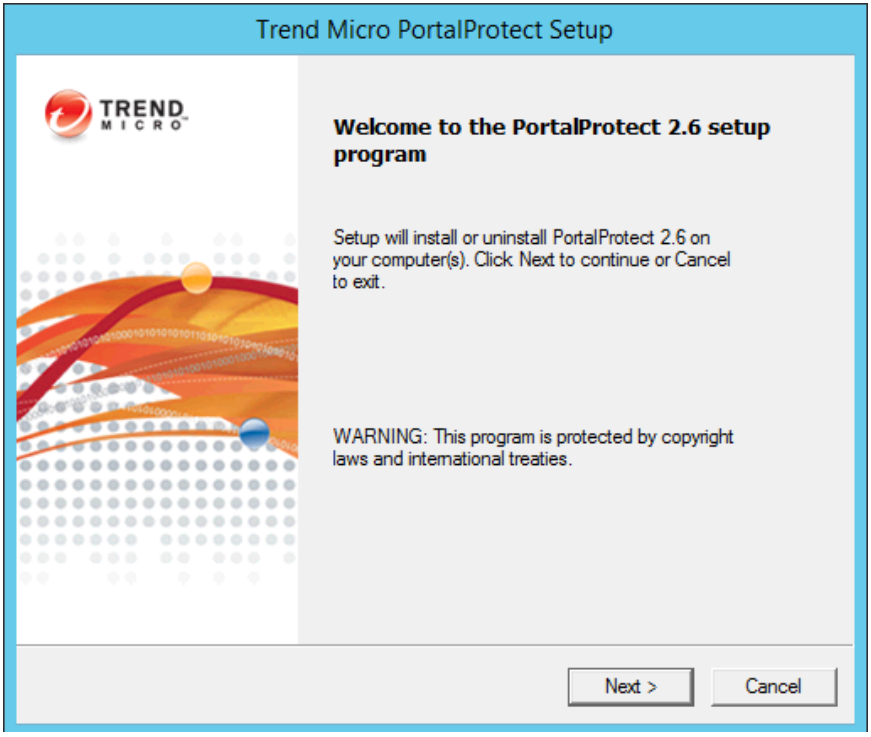

図 2-39. PortalProtect のセットアッププログラム画面

2. [Next >] をクリックします。

[License Agreement] 画面が表示されます。

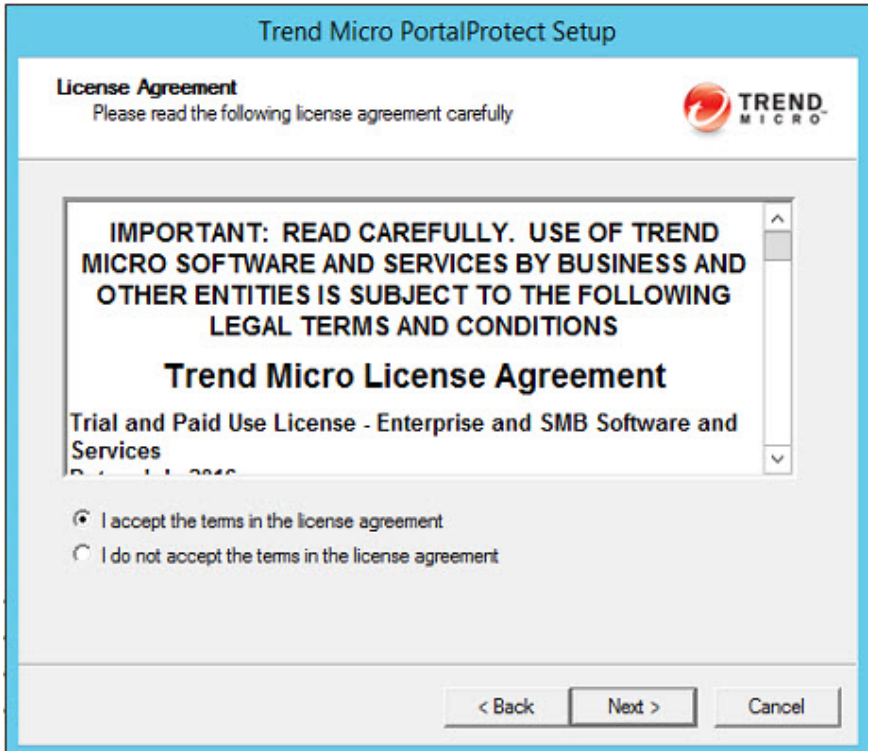

図 2-40. [License Agreement] 画面

3. [I accept the terms in the license agreement] を選択して [Next >] をクリックします。

[Select an Action] 画面 (1) が表示されます。

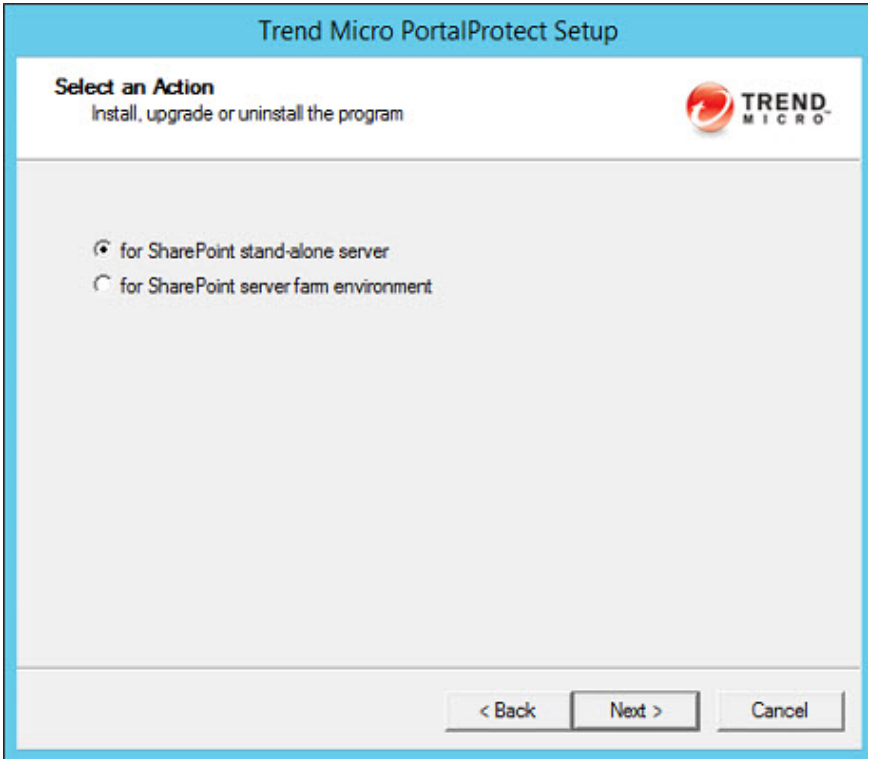

図 2-41. [Select an Action] 画面 (1)

4. 次のいずれかのインストールオプションを選択します。
   - for SharePoint stand-alone server
   - for SharePoint server farm environment
5. 適切なオプションを選択したら、[Next >] をクリックします。

[Select an Action - Install, upgrade or uninstall PortalProtect] 画面が表示されます。

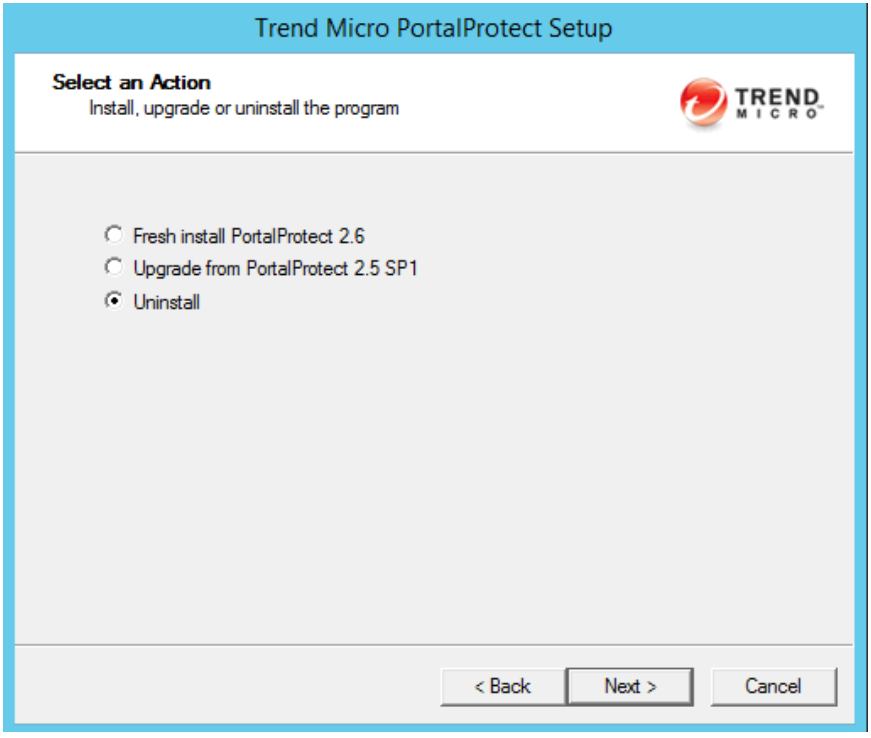

図 2-42. [Select an Action] 画面 (2)

6. [Uninstall] を選択し、[Next >] をクリックします。

[Select Target Server(s)] 画面が表示されます。

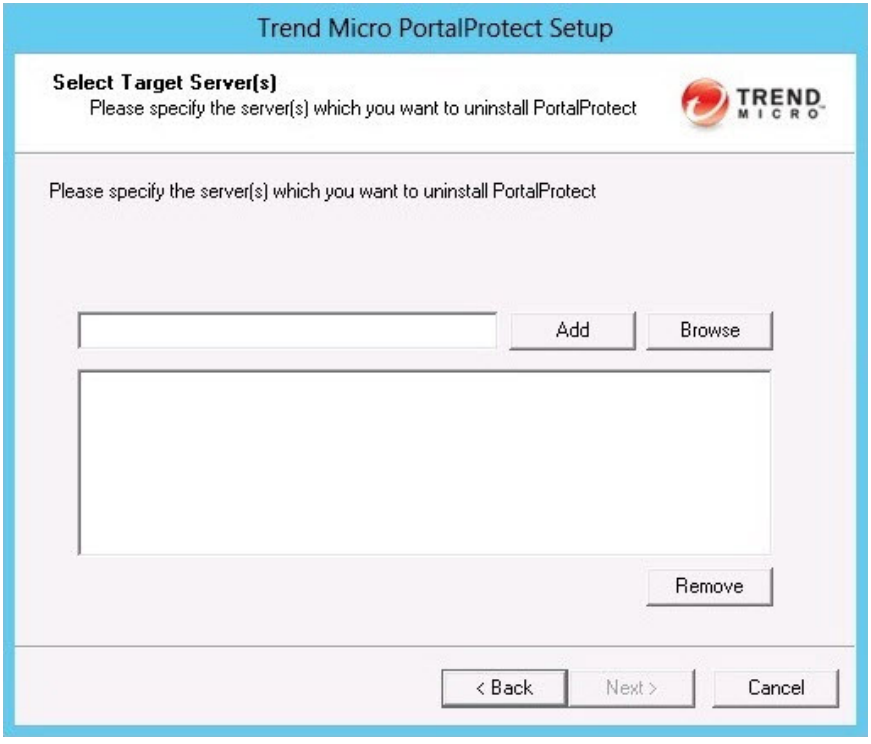

図 2-43. [Select Target Server(s)] 画面

7. PortalProtect をアンインストールするコンピュータ名を [Computer name] に入力するか、参照 ([Browse] をクリック) し、[Add] をクリックして追加します。追加したサーバを選択し、[Next >] をクリックします。

[Select Computers] ダイアログが表示されます。

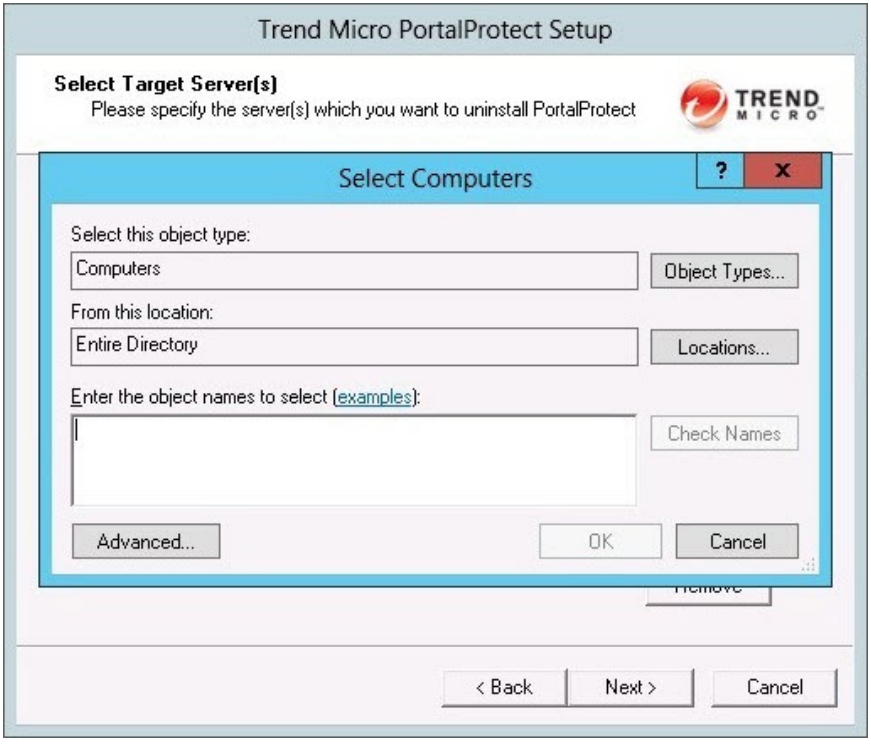

図 2-44. [Select Computers] ダイアログ

8. PortalProtect をアンインストールするコンピュータを選択し、[OK] をクリックします。

   [Select Target Server(s)] 画面が表示されます。

9. [Add] / [Browse] をクリックして、必要に応じて追加のサーバを選択し、[Next >] をクリックします。

[Log On] 画面が表示されます。

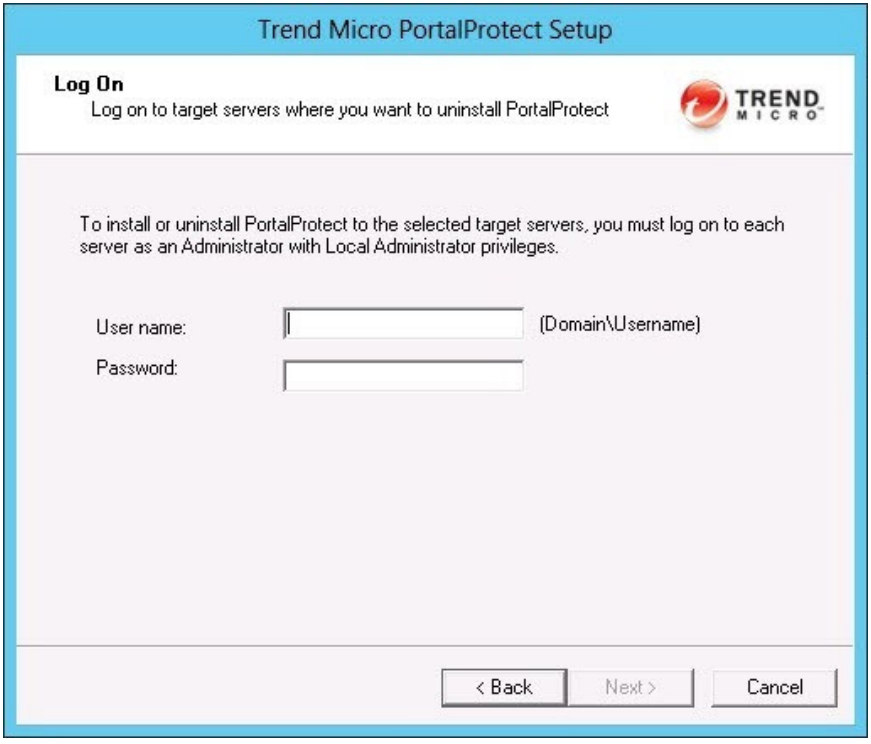

図 2-45. [Log On] 画面

10. [User name] に「ドメイン\ユーザ名」の形式でサーバのユーザ名を入力し、[Password] にパスワードを入力して [Next >] をクリックします。

[Configure Shared Directory] 画面が表示されます。

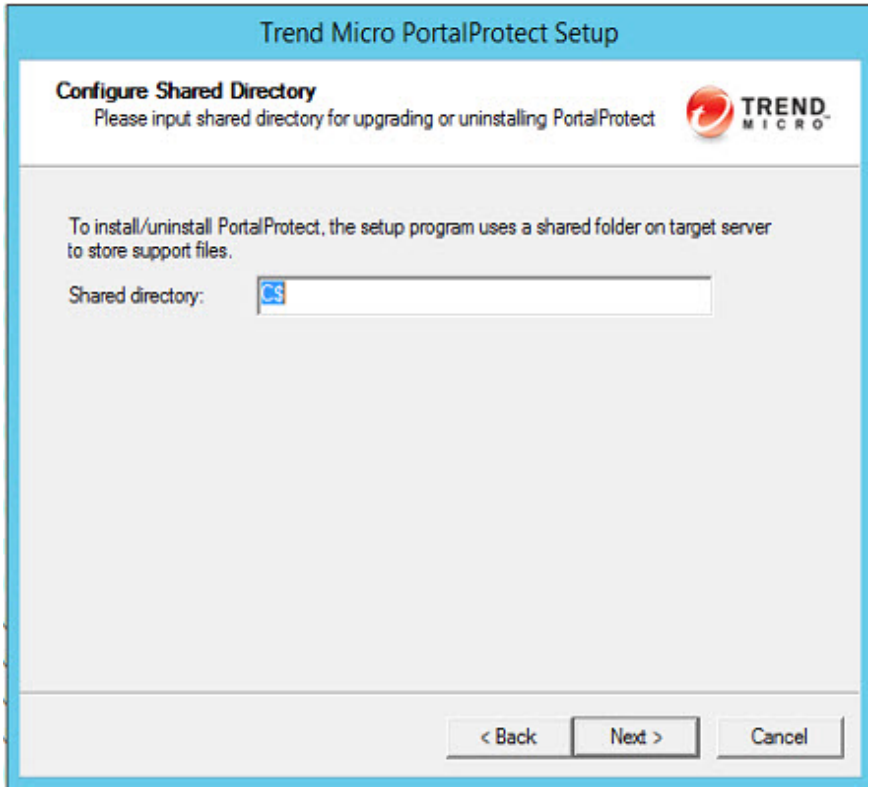

図 2-46. [Configure Shared Directory] 画面

11. [Shared directory] の共有ディレクトリを確認して、[Next >] をクリックします。

[Checking Target Server System Requirements] 画面が表示されます。

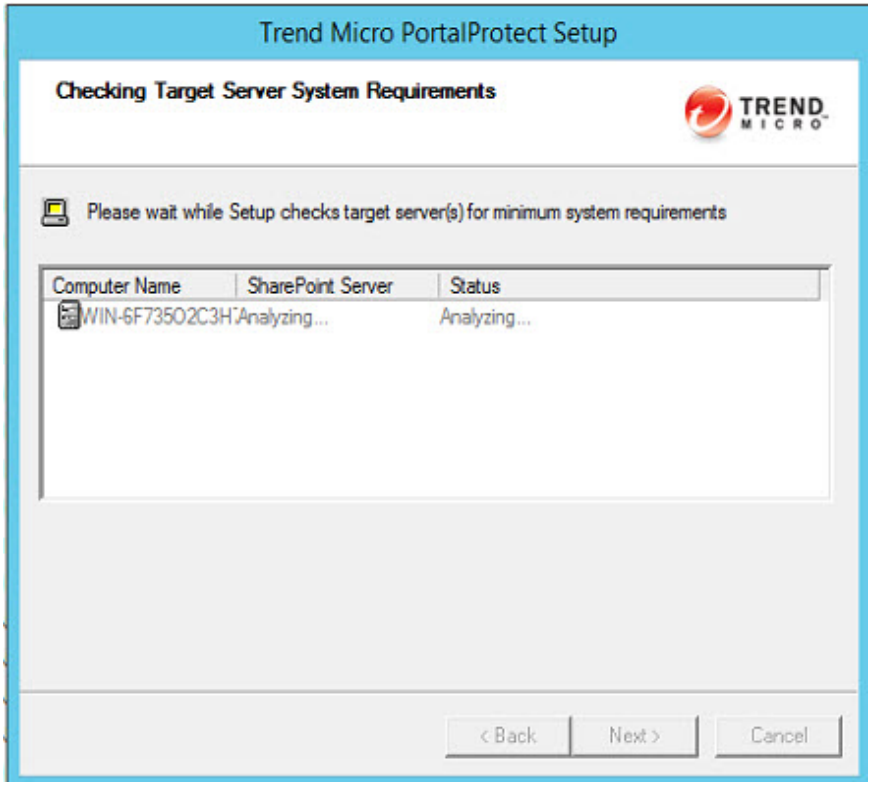

図 2-47. [Checking Target Server System Requirements] 画面

12. [Computer Name] および [SharePoint Server] を確認します。[Status] に [Uninstall] と表示されていることを確認して、[Next >] をクリックします。

[Uninstall Notice] 画面が表示されます。

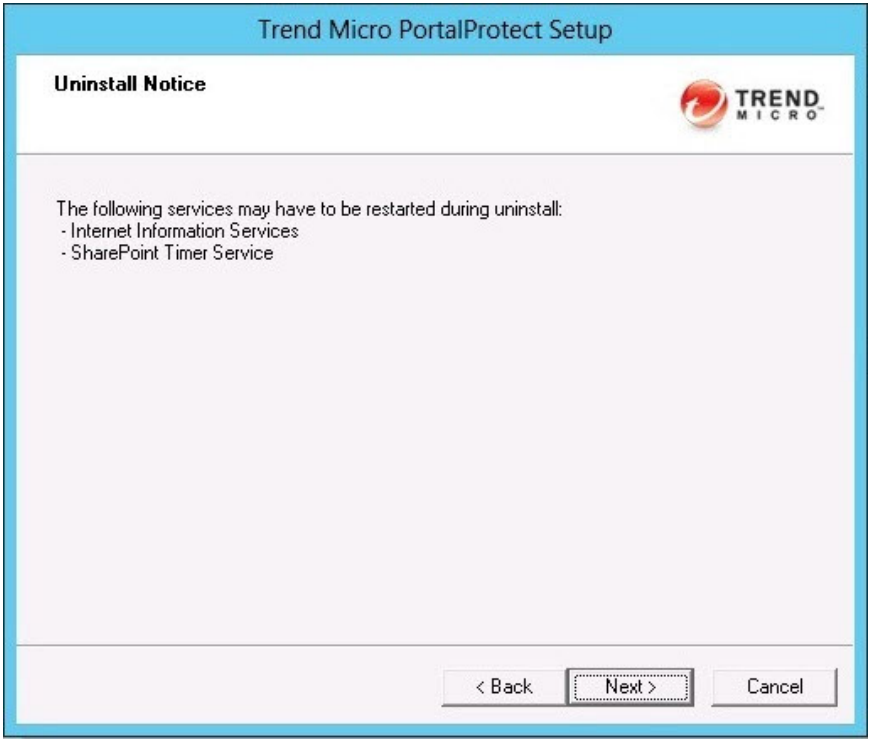

図 2-48. [Uninstall Notice] 画面

13. [Next >] をクリックします。

[Review Settings] 画面が表示されます。

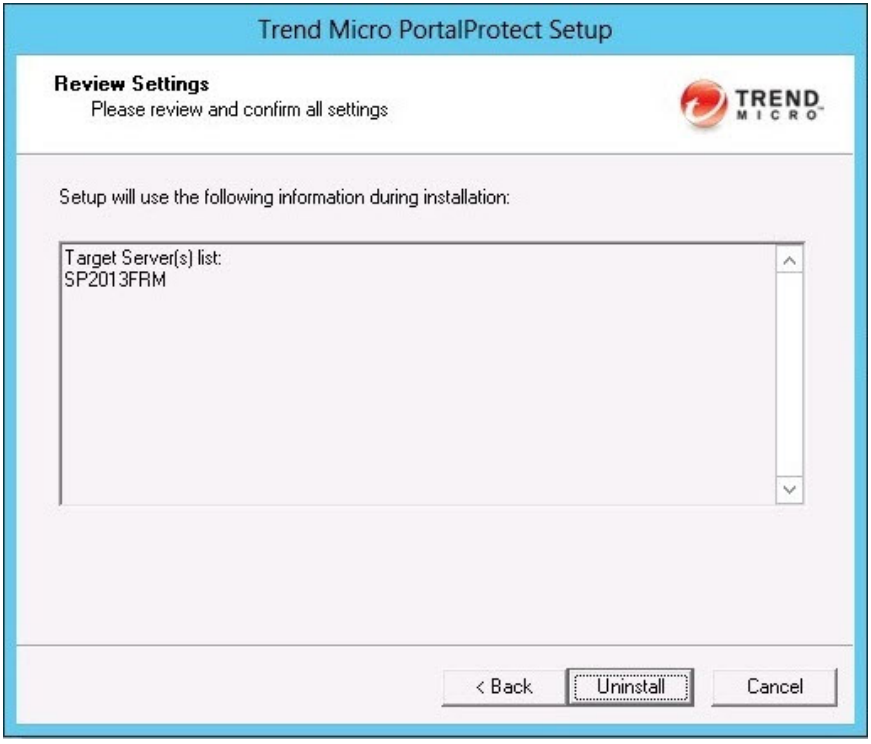

図 2-49. [Review Settings] 画面

14. 画面に表示された設定を確認します。変更が必要な場合には [< Back] をクリックして戻ります。設定内容が正しければ [Next >] をクリックします。

[Uninstallation Progress] 画面が表示されます。

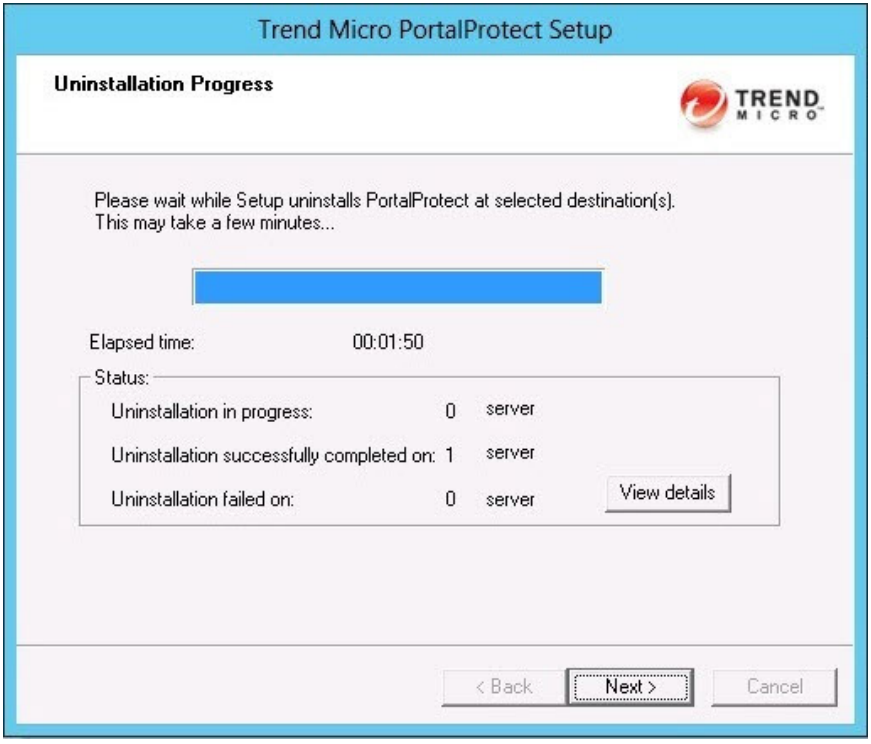

図 2-50. [Uninstallation Progress] 画面

15. [View details] をクリックすると、アンインストールの進行状況を確認できます。

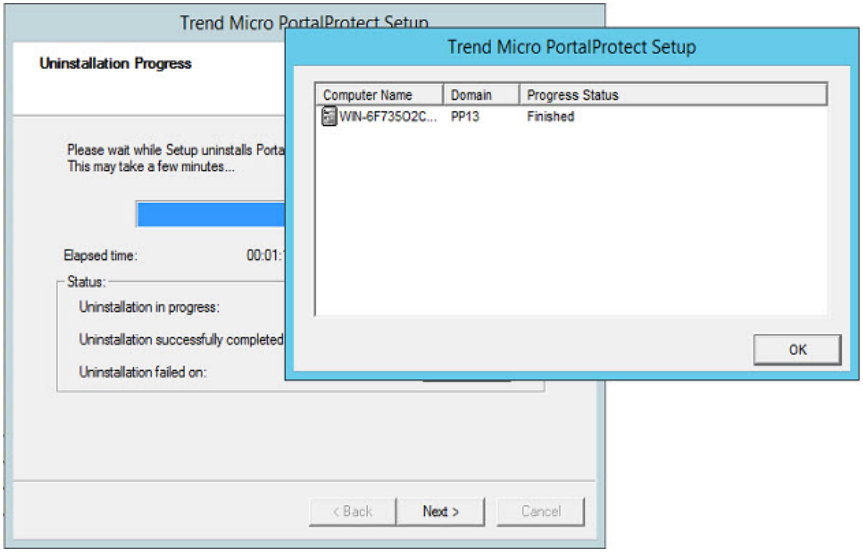

図 2-51. アンインストールの進捗状況

16. [Progress Status] が [Finished] と表示されたら、[OK]→[Next >] の順にクリックします。

[Uninstallation Complete] 画面が表示されます。

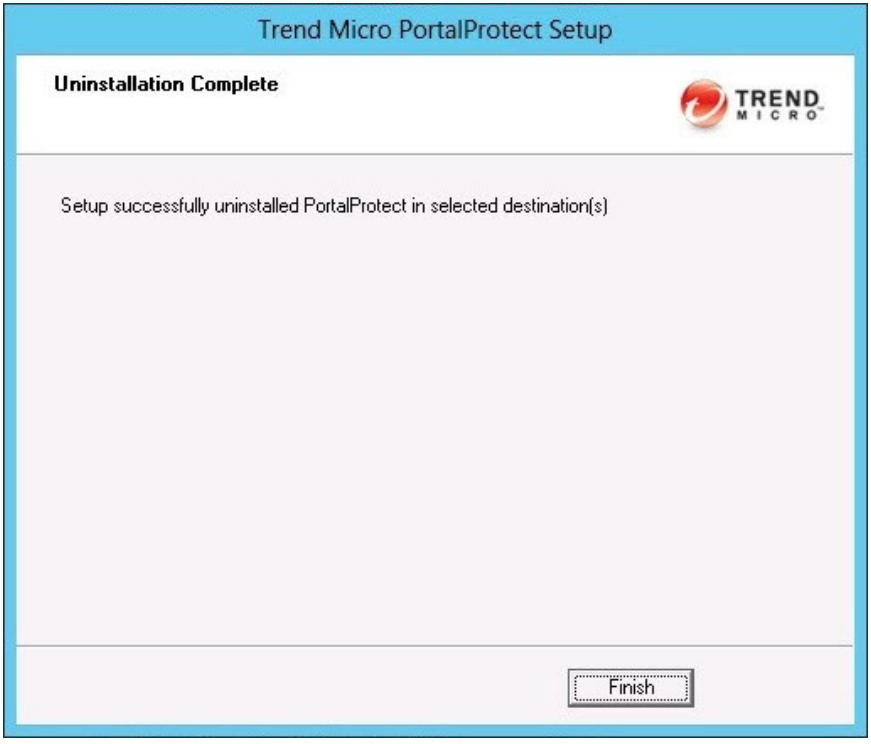

図 2-52. [Uninstallation Complete] 画面

第 3 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/ 駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

第 4 章

よくある質問

本章では、PortalProtect の機能に関してよくある質問とその回答について紹介します。

本章の内容は次のとおりです。

インストール

SharePoint 環境を保護するためには、どこに PortalProtect をインストールすればよいでしょうか。

SharePoint スタンドアロン配置モードの場合: スタンドアロンサーバで Web アプリケーションサーバ (サービス) が稼働しているため、PortalProtect はスタンドアロンサーバにインストールします。

SharePoint ファーム配置モードの場合: PortalProtect は Web アプリケーションサーバ (サービス) が稼働しているサーバ、つまり Web フロントエンドサーバにインストールします。

[install to farm] と [install to stand-alone] の違いは何ですか。

どちらを選択するかは SharePoint の配置モードによって異なります。SharePoint をファームモードで配置する場合は、[install to farm] を選択して PortalProtect をインストールする必要があります。SharePoint をスタンドアロンモードで配置する場合は (基本的な配置)、[install to stand-alone]を選択して PortalProtect をインストールする必要があります。

スタンドアロンサーバへのインストールを選択すると、SharePoint データベースがスタンドアロンサーバに配置されているため、ユーザに SharePoint データベースのアクセスアカウントの入力を求めることなく、スタンドアロンの SharePoint サーバに PortalProtect がインストールされます。

クラスタ環境への PortalProtect のインストール方法について教えてください。

PortalProtect はクラスタ環境を完全にはサポートしていません。クラスタサーバにインストールする場合、一度にインストールできるのはクラスタ内の 1 つのサーバ IP に対してのみです。

インストール後、PortalProtect 管理コンソールにログインできません。原因は何でしょうか。

次の点を確認してください。

1. [コントロールパネル] > [管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャ] を開きます。

2. PortalProtect アプリケーションプール、仮想サイト、および仮想ディレクトリが存在することを確認します。
3. IIS サイトが稼働していることを確認します。
4. IIS サイトプロパティが正しく設定されており、ブラウザからアクセスできることを確認します。
5. PortalProtect マスターサービスが稼働していることを確認します。
6. ログインアカウントがローカル管理者または管理グループ (インストール時に選択された PortalProtect 管理グループ) のメンバーであることを確認します。

データベースアクセスアカウントのパスワードを変更する場合や有効期限が切れた場合は、どのように処理すればよいですか。

1. SharePoint と PortalProtect がともに Windows 認証を使用してデータベースに接続している場合

   SharePoint データベースパスワードまたは PortalProtect データベースパスワードを変更するには

   a. [管理ツール] > [サービス] の順に選択します。
   b. Trend Micro PortalProtect for Microsoft SharePoint Master Service を見つけます。
   c. サービスログインアカウントのパスワードを変更して、サービスを再起動します。

2. PortalProtect が Windows 認証を使用してデータベースに接続し、PortalProtect は SQL 認証を使用してデータベースに接続している場合

   SharePoint データベースパスワードを変更するには

   a. [管理ツール] > [サービス] の順に選択します。
   b. Trend Micro PortalProtect for Microsoft SharePoint Master Service を見つけます。
   c. サービスログインアカウントのパスワードを変更して、サービスを再起動します。

   PortalProtect データベースパスワードを変更するには

a. レジストリを開き、次の項目を見つけます。

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion\PPConfDatabasePassword

b. パスワードを変更して、PortalProtect マスターサービスを再起動します。

注意

[PPConfDatabasePassword] フィールドにパスワードを入力できます。PortalProtect マスターサービスの再起動時に、パスワードは暗号化されます。

3. SharePoint が SQL 認証を使用してデータベースに接続し、PortalProtect は Windows 認証を使用してデータベースに接続している場合

SharePoint データベースパスワードを変更するには

a. レジストリを開き、次の項目を見つけます。

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion\SharePointDBAccessPassword

b. パスワードを変更して、PortalProtect マスターサービスを再起動します。

注意

[SharePointDBAccessPassword] フィールドにパスワードを入力できます。PortalProtect マスターサービスの再起動時に、パスワードは暗号化されます。

PortalProtect データベースパスワードを変更するには

a. [管理ツール] > [サービス] の順に選択します。

b. Trend Micro PortalProtect for Microsoft SharePoint Master Service を見つけます。

c. サービスログインアカウントのパスワードを変更して、サービスを再起動します。

4. SharePoint が SQL 認証を使用してデータベースに接続し、PortalProtect は Windows 認証を使用してデータベースに接続している場合

   SharePoint データベースパスワードを変更するには

   a. レジストリを開き、次の項目を見つけます。

      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect \CurrentVersion\SharePointDBAccessPassword

   b. パスワードを変更して、PortalProtect マスターサービスを再起動します。

   注意

   [SharePointDBAccessPassword] フィールドにパスワードを入力できます。PortalProtect マスターサービスの再起動時に、パスワードは暗号化されます。

   PortalProtect データベースパスワードを変更するには

   a. レジストリを開き、次の項目を見つけます。

      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect \CurrentVersion\PPConfDatabasePassword

   b. パスワードを変更して、PortalProtect マスターサービスを再起動します。

Windows Server 2016 の [スタート] メニューから PortalProtect 管理コンソールを開くことができないのはなぜでしょうか。

場合によって、Windows Server 2016 の [スタート] メニューに初期設定の Web 閲覧アプリケーションが含まれていないことがあります。Internet Explorer などの Web ブラウザを追加するには、[設定] > [既定のアプリ] の順に選択して、目的の Web ブラウザのリンクを追加します。

PortalProtect のインストール時にインストールされるサードパーティ製ソフトウェアには何がありますか。

PortalProtect のインストール時には次のサードパーティ製ソフトウェアがインストールされます。

- Microsoft Visual C++ 2015 再頒布可能パッケージ (x64)
- Microsoft Visual C++ 2010 再頒布可能パッケージ (x64)
- Microsoft SQL Server 2012 Native Client

注意

「Microsoft Visual C++ 2010 再頒布可能パッケージ (x64)」および「Microsoft SQL Server 2012 Native Client」のインストールでは、マイクロソフトによりシステムの再起動を求められることがあります。

付録 A

データベース権限の要件

ここでは、Trend Micro PortalProtect(以下、PortalProtect) 2.6 のデータベース権限で必要とされる技術的な詳細について説明します。

本章の内容は次のとおりです。

アプリケーション

ここでは、PortalProtect で使用されるアプリケーションについて説明します。

- PortalProtect
- SQL Server
- SharePoint

背景情報

PortalProtect は、次の SQL Server データベースソースにアクセスできる必要があります。

- PortalProtect 設定データベース
- SharePoint データベース

これらのデータベースにアクセスするために、PortalProtect は、次のデータベースアクセスアカウントを必要とします。

- PortalProtect 設定データベースアクセスアカウント
- SharePoint データベースアクセスアカウント

注意

これらのデータベースアクセスアカウントは、Windows 認証か SQL Server 認証のいずれかをサポートしている必要があります。

アクセスアカウントが SQL Server 認証に対して設定されている場合、アクセスアカウントのパスワードは暗号化されてレジストリに保存されます。

アクセスアカウントが Windows 認証に対して設定されている場合、PortalProtect サービスのログオンアカウントとして使用されます。

両方のアクセスアカウントで Windows 認証が使用される場合、それらは同じアカウントでなければならず、PortalProtect サービスのログオンアカウント

として使用されます。次の表は、PortalProtect サービスのログオンアカウントについて説明しています。

表 A-1. PortalProtect サービスのログオンアカウント

PortalProtect 設定データベースアクセスアカウント	SharePoint データベースアクセスアカウント	PortalProtect サービス起動アカウント
Windows 認証	Windows 認証	両方のアクセスアカウントは同じでなければなりません。PortalProtect は、サービス起動アカウントとしてこれらのアカウントを使用します。
Windows 認証	SQL Server 認証	PortalProtect 設定データベースアクセスアカウント
SQL Server 認証	Windows 認証	SharePoint データベースアクセスアカウント
SQL Server 認証	SQL Server 認証	Local System

アクセスアカウントが SQL Server 認証に対して設定されている場合、パスワードは次のレジストリキーに保存されます。

```
HKLM\Software\TrendMicro\PortalProtect\CurrentVersion
```

このレジストリキーには SharePoint の動作も含まれ、パスワードは暗号化されます。

注意

- - Windows 認証を使用することを強くお勧めします。Windows 認証では、より安定した環境が実現し、パスワードをなんらかの形式で保存する必要がありません。
- - PortalProtect と SharePoint の両方のデータベースで SQL Server 認証を使用する場合、機能制限により PortalProtect の Web コンテンツ検索と手動検索が機能しません。
- PortalProtect サービス起動アカウントには永続的なローカル管理者権限が必要です。権限がない場合、インストールが正常に実行されません。

PortalProtect 設定データベースアクセスアカウントに対する要件

認証の他に、これらのアクセスアカウントにはデータベース権限も必要です。ここでは、各データベースアクセスアカウントに必要な最小権限について説明します。

PortalProtect は、データ (設定、ログ、レポート、隔離されたデータなど) を PortalProtect 設定データベースに保存します。SharePoint 環境において、PortalProtect は新規インストール用のデータベースを必要とし、同じデータベースをアップグレードに使用します。

新規インストールで次のデータベースが作成されます。

- PortalProtect_{UUID}

PortalProtect 設定データベースアクセスアカウントに必要なデータベース権限は次のとおりです。

- アクセスアカウントは、サーバの役割 db_creator を持っている必要があります。

サーバの役割 db_creator は、PortalProtect のインストール時にのみ必要です。インストールの完了後、この権限を削除できます。

SharePoint データベースアクセスアカウントに対する要件

ここで説明する内容は、SharePoint ファーム環境のみに適用されます。SharePoint スタンドアロン環境では、データはローカルの SQL Server に保存されるため、アクセスアカウントを指定する必要はありません。

PortalProtect は、SharePoint データベース内のデータをフェッチまたは変更します。それに関連する権限を持つデータベースアクセスアカウントを指定する必要があります。必要なデータベース権限は次のとおりです。

- SharePoint_Config データベース: db_datareader および WSS_Content_Application_Pools の役割
- WSS_Content データベース: db_owner の役割

注意

WSS_Content データベースが複数ある場合は、この役割を各 WSS_Content データベースに指定します。

PortalProtect は、SharePoint 内部のストアドプロシージャを実行する必要があります。ストアドプロシージャの実行権限は、db_owner にのみ付与されます。このため、PortalProtect では、データベースの役割 db_owner が必要になります。PortalProtect は、SharePoint データベーススキーマを変更しません。