Dell Security Management Server

インストールおよび移行ガイド v10.2.12

August 2020
Rev. A01

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

目次

1

はじめに

Security Management Server について

Security Management Server の機能は、次のとおりです。

- デバイス、ユーザー、セキュリティポリシーの一元管理
- 一元的なコンプライアンス監査とレポート
- 管理者職務の分割
- 役割ベースのセキュリティポリシーの作成と管理
- クライアント接続時のセキュリティポリシー配布
- 管理者がサポートするデバイス復元
- コンポーネント間での通信のための信頼済みパス
- 固有暗号化キーの生成および自動かつセキュアなキーエスクロー

Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート (877-459-7304、内線 4310039) にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問 (FAQ)、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の各国の電話番号を記載したページを参照してください。

2

要件およびアーキテクチャ

この項では、Dell Security Management Server を実装する場合のハードウェアおよびソフトウェア要件、および推奨するアーキテクチャ設計について、詳細を説明します。

Security Management Server アーキテクチャの設計

Encryption Enterprise および Endpoint Security Suite Enterprise ソリューションは非常に拡張性の高い製品であり、組織内の暗号化の対象となるエンドポイントの数に基づいて拡張可能です。

アーキテクチャコンポーネント

以下に、ほとんどの環境に適した推奨ハードウェア構成を示します。

Security Management Server

- オペレーティングシステム：Windows Server 2012 R2（Standard、Datacenter 64 ビット）、Windows Server 2016（Standard、Datacenter 64 ビット）、Windows Server 2019（Standard、Datacenter）
- 仮想 / 物理マシン
- CPU：4 コア
- RAM：16.00 GB
- ドライブ C：ログおよびアプリケーションデータベース用に空きディスク容量 30 GB

  メモ: PostgreSQL 内に保存されているローカルイベントデータベースで最大 10 GB を消費することがあります。

プロキシサーバー

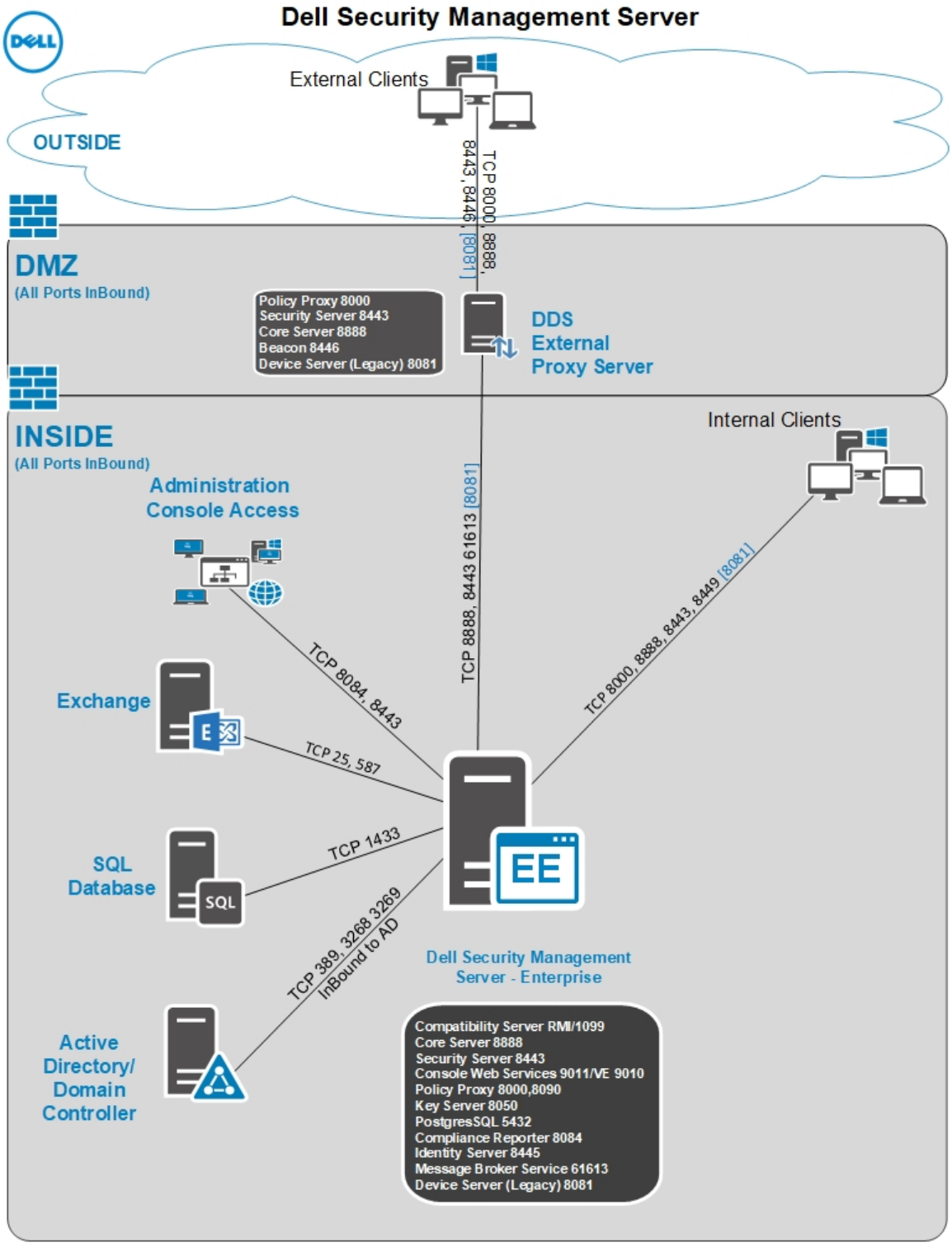
- オペレーティングシステム：Windows Server 2012 R2（Standard、Datacenter 64 ビット）、Windows Server 2016（Standard、Datacenter 64 ビット）、Windows Server 2019（Standard、Datacenter）
- 仮想 / 物理マシン
- CPU：2 コア
- RAM：8.00 GB
- ドライブ C：ログ用に空きディスク容量 20 GB

SQL Server のハードウェア仕様

- CPU：4 コア
- RAM：24.00 GB
- データドライブ：空きディスク容量 100 ~ 150 GB（環境によって異なる）
- ログドライブ：空きディスク容量 50 GB（環境によって異なる）

  メモ: ほとんどの環境で上記の情報が有効です。そうでない場合は、「SQL Server ベストプラクティス」を参照してください。

以下は、Dell Security Management Server の基本的な導入です。



メモ: 組織に 20,000 を超えるエンドポイントがある場合は、Dell ProSupport に問い合わせてサポートを受けてください。

要件

Security Management Server ソフトウェアをインストールするためのハードウェアおよびソフトウェアの前提条件は、次のとおりです。

インストールを開始する前に、すべてのパッチとアップデートがインストールに使用されるサーバーに適用されていることを確認します。

ハードウェア

次の表に、Security Management Server の*最小*ハードウェア要件の詳細を示します。導入環境のサイズに基づいて拡張を行う場合の詳細については、「Security Management Server のアーキテクチャの設計」を参照してください。

ハードウェア要件
プロセッサ 現行のクアッドコア CPU (1.5 GHz+)
RAM 16 GB
空きディスク容量 20 GB の空きディスク容量 メモ: PostgreSQL に保存されているローカルイベントデータベースは、最大 10 GB まで消費することがあります。
ネットワークカード 10/100/1000 またはそれ以上
その他 IPv4 または IPv6、またはハイブリッド IPv4/IPv6 環境が必要

次の表は、Security Management Server フロント - エンド / プロキシサーバの*最小*ハードウェア要件を示します。

ハードウェア要件
プロセッサ 最新デュアルコア CPU
RAM 8 GB
空きディスク容量 ログファイル用に空きディスク容量 20 GB
ネットワークカード 10/100/1000 またはそれ以上
その他 IPv4 または IPv6、またはハイブリッド IPv4/IPv6 環境が必要

仮想化

Security Management Server は、仮想環境にインストールできます。次の環境のみが推奨されます。

Security Management Server v10.2.11 は、以下のプラットフォームで動作確認済みです。

Hyper-V サーバーは、Windows Server 2012、Windows Server 2016、Windows Server 2019 の各環境でフルまたはコア インストールとして、あるいはロールとしてインストールされているものを指します。

- Hyper-V サーバー
  - 64 ビット x86 CPU (必須)
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM (推奨)

- ハードウェアは Hyper-V 最小要件を満たしている必要があります
- イメージ専用リソース用に最小 4 GB の RAM
- 第 1 世代の仮想マシンとして実行する必要があります
- 詳細については、https://technet.microsoft.com/en-us/library/hh923062.aspx を参照してください。

Security Management Server v10.2.11 は、VMware ESXi 6.0 および VMware ESXi 6.5 で動作確認済みです。

メモ: Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 のいずれかと VMware ESXi を実行する場合は、VMXNET3 Ethernet アダプターの使用をお勧めします。

- VMware ESXi 6.0
  - 64 ビット x86 CPU (必須)
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM (推奨)
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-60/index.jsp を参照してください。
- VMware ESXi 6.5
  - 64 ビット x86 CPU (必須)
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM (推奨)
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-65/index.jsp を参照してください。
- VMware ESXi 6.7
  - 64 ビット x86 CPU (必須)
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM (推奨)
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-65/index.jsp を参照してください。

メモ: Security Management Server をホストする SQL Server データベースは、パフォーマンス上の理由から、別のコンピュータで実行してください。

SQL Server

さらに大規模な環境では、SQL クラスタなどの冗長システム上で SQL データベースサーバを実行して、可用性とデータ継続性を確保することを強くお勧めします。また、トランザクションログを有効にして完全バックアップを毎日実行し、ユーザー / デバイスのアクティブ化によって新規に生成されたすべてのキーを回復可能にしておくこともお勧めします。

データベースのメンテナンスタスクには、データベースインデックスの再構築と統計の収集を含めるようにしてください。

ソフトウェア

次の表に、Security Management Server とプロキシサーバのソフトウェア要件の詳細を示します。

メモ: Security Management Server が保持するデータは機密性が高いため、また、最小権限ルールに合わせるために、Security Management Server は専用のオペレーティング システムにインストールするか、役割と権限が制限されたアプリケーション サーバーの一部としてインストールして、安全な環境を確保することをお勧めします。また、Security Management Server を特権インフラストラクチャ サーバーにインストールしないでください。最小権限ルールの実装の詳細については、「https://

docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models」を参照してください。

メモ: 保護されたディレクトリにインストールする場合は、ユニバーサルアカウント制御（UAC）を無効にする必要があります。UAC を無効化した後は、変更を有効にするためにサーバーを再起動する必要があります。

メモ: ポリシープロキシ（インストールされている場合）のレジストリの場所：HKLM\SOFTWARE\Wow6432Node\Dell

メモ: Windows Server のレジストリの場所：HKLM\SOFTWARE\Dell

前提条件
• **Visual C++ 2010 再頒布可能パッケージ** インストールされていない場合、インストーラーによってインストールされます。 • **Visual C++ 2013 再頒布可能パッケージ** インストールされていない場合、インストーラーによってインストールされます。 • **Visual C++ 2015 再頒布可能パッケージ** インストールされていない場合、インストーラーによってインストールされます。 • **.NET Framework バージョン 4.6.1** • **.NET Framework バージョン 4.5** Microsoft は、.NET Framework バージョン 4.6.1 および 4.5 のセキュリティ更新プログラムを公開しました。 • **.NET Framework バージョン 3.5 SP1** • **SQL Native Client 2012** SQL Server 2012 または SQL Server 2016 を使用している場合。 インストールされていない場合、インストーラーによってインストールされます。

Security Management Server - バックエンド サーバーおよびデル フロントエンド サーバー
• **Windows Server 2012 R2** - Standard Edition - Datacenter Edition • **Windows Server 2016** - Standard Edition - Datacenter Edition • **Windows Server 2019** - Standard Edition - Datacenter Edition **メモ:** バックエンド構成またはフロントエンド構成にインストールされているデルの Security Management Server では現在、Windows Server オペレーティング システムの OS アップグレードはサポートされていません。
LDAP リポジトリ
• Active Directory 2008 R2 • Active Directory 2012 R2 • Active Directory 2016 **メモ:** Security Management Server は、Active Directory 使用時に LDAP チャネル バインディングおよび LDAP 署名を行うための Microsoft 要件と互換性があります。

管理コンソールおよび Compliance Reporter

- Mozilla Firefox 41.x 以降
- Google Chrome 46.x 以降
- Microsoft Edge（Chromium 版）
- Microsoft Edge

メモ: お使いのブラウザで cookie を受け入れる必要があります。

Security Management Server コンポーネントの推奨仮想環境

Security Management Server は、仮想環境にインストールできます。

デルは現在、Amazon Web Services、Azure などの複数のベンダーが提供しているようなクラウドホスト IaaS（Infrastructure as a Service）環境での、Dell Security Management Server または Dell Security Management Server Virtual のホスティングをサポートしています。こうした環境のサポートは、Security Management Server の機能に限定されます。これらの仮想マシンの管理とセキュリティは、IaaS ソリューションの管理者が担当します。

その他のインフラストラクチャ要件。適切に機能するためには、Active Directory や SQL Server など、その他のインフラストラクチャ要件も必要です。

メモ: Security Management Server をホストする SQL Server データベースは、別のコンピュータ上で実行する必要があります。

データベース

- **SQL Server 2012 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2014 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2016 -** Standard Edition / Enterprise Edition
- **SQL Server 2017 -** Standard Edition / Enterprise Edition
- **SQL Server 2019 -** Standard Edition / Enterprise Edition

メモ: Express Edition は、実稼働環境ではサポートされません。Express Edition は、POC および評価でのみ使用できます。

SQL Server のバージョンに応じて、Security Management Server で次のいずれかが有効になっている**必要があります**。

- フル テキスト インデックス作成
- フルテキスト フィルター
- フルテストおよび検索用のセマンティック抽出

上記の機能が使用中の SQL Server で有効になっていない場合に発生したエラーの詳細については、KB 記事 SLN308557 を参照してください。

Security Management Server に対応した Microsoft SQL Server のアクセス許可および機能の設定の詳細については、KB 記事 SLN307771 を参照してください。

メモ: SQL のアクセス許可の要件を次に示します。インストールとサービスを実行するユーザーは、ローカル管理者権限を持っている必要があります。また、Dell Security Management Server サービスを管理するサービス アカウントにも、ローカル管理者権限が必要です。

タイプ	アクション	シナリオ	必要な SQL 特権
バックエンド	アップグレード	定義によって、アップグレードにはすでに DB とログイン/ユーザーが確立されています。	db_owner
バックエンド	インストールの復元	復元には、既存の DB とログインが含まれます。	db_owner
バックエンド	新規インストール	既存の DB を使用	db_owner
バックエンド	新規インストール	新しい DB の作成	dbcreator、db_owner
バックエンド	新規インストール	既存のログインを使用	db_owner

タイプ	アクション	シナリオ	必要な SQL 特権
バックエンド	新規インストール	新規のログインを作成	securityadmin
バックエンド	アンインストール	該当なし	該当なし
プロキシのフロントエンド	任意	該当なし	該当なし

メモ: ユーザー アカウント制御（UAC）が有効になっている場合、`C:\Program Files` にインストールする際は、Windows Server 2012 R2 にインストールする前に UAC を無効にしておく必要があります。変更を有効にするためにはサーバーを再起動する必要があります。

インストール中にデータベースを設定するために Windows または SQL 認証資格情報が必要です。使用された認証資格情報の種類にかかわらず、アカウントには処置を実行するための適切な権限が必要です。上の表には、インストールのタイプ別に必要な権限が記載されています。また、データベースの作成とセットアップに使用するアカウントでは、デフォルト スキーマを dbo に設定する必要があります。

これらの権限は、インストール時にデータベースをセットアップするためにのみ必要になります。Security Management Server がインストールされると、SQL アクセスの管理に使用するアカウントは db_owner および public ロールに制限できます。

アクセス権限の有無またはデータベースへのアクセスの可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

管理コンソールの言語サポート

管理コンソールは、多言語ユーザーインタフェース（MUI）に対応しており、次の言語をサポートします。

言語サポート	
EN - 英語	JA - 日本語
ES - スペイン語	KO - 韓国語
FR - フランス語	PT-BR - ポルトガル語（ブラジル）
IT - イタリア語	PT-PT - ポルトガル語（ポルトガル（イベリア））
DE - ドイツ語	

3

インストール前の設定

作業を開始する前に、Security Management Server に関連する最新の回避策または既知の問題について *Security Management Server テクニカルアドバイザリー*をお読みください。

Security Management Server をインストールするサーバのインストール前の設定は非常に重要です。Security Management Server を円滑にインストールするためにこの項を特に注意してお読みください。

設定

管理コンソールへのアクセス

Internet Explorer はサポートされなくなったため、サード パーティー製のブラウザーをインストールして、管理コンソールに適切にアクセスできるようにする必要があります。

管理コンソールの検証に Internet Explorer が必要な場合は、ログインしている管理者に対応するアカウント タイプに対して、Internet Explorer のセキュリティ強化の構成を無効にする必要があります。

ポートとファイアウォールの構成

クライアントとサーバーのパブリック (アウトバウンド) 通信

Dell サーバーが管理対象エンドポイントと通信するには、次のサービスとポートが必要です。これらのポートとサービスは、アウトバウンド通信に対応している必要があります。SSL インスペクションとプロキシ サービスが使用されている場合、URL はそれらから除外される必要があります。

- オンザボックス利用資格検証
  - 宛先 URL
    - cloud.dell.com
  - ポート
    - 443
  - アウトバウンド デバイス
    - バックエンド構成の Security Management Server または Security Management Server Virtual
  - 発信元サービス
    - Dell Security Server
  - 発信元ポート
    - 8443
- Advanced Threat Prevention クライアント通信
  - 宛先 URL
    - 北アメリカ
      - login.cylance.com
      - protect.cylance.com
      - data.cylance.com
      - update.cylance.com
      - api.cylance.com
      - protect-api.cylance.com
      - download.cylance.com
    - 南アメリカ
      - login-sae1.cylance.com
      - protect-sae1.cylance.com
      - data-sae1.cylance.com
      - update-sae1.cylance.com
      - api-sae1.cylance.com

- protect-api-sae1.cylance.com
- download-sae1.cylance.com

▪ ヨーロッパ

- login-euc1.cylance.com
- protect-euc1.cylance.com
- data-euc1.cylance.com
- update-euc1.cylance.com
- api-euc1.cylance.com
- protect-api-euc1.cylance.com
- download-euc1.cylance.com

▪ 中東およびアジア

- login-au.cylance.com
- protect-au.cylance.com
- data-au.cylance.com
- update-au.cylance.com
- api-au.cylance.com
- protect-api-au.cylance.com
- download-au.cylance.com

▪ 日本、オーストラリア、ニュージーランド

- login-apne1.cylance.com
- protect-apne1.cylance.com
- data-apne1.cylance.com
- update-apne1.cylance.com
- api-apne1.cylance.com
- protect-api-apne1.cylance.com
- download-apne1.cylance.com

○ ポート

▪ 443

○ アウトバウンド デバイス

▪ すべての管理対象エンドポイント

○ アウトバウンド サービス

▪ CylanceSVC

○ 発信元ポート

▪ 443

フロントエンド サーバーへのパブリック通信 (必要な場合)

インターネット経由でフロントエンド サーバーに情報を転送する場合です。ファイアウォールまたはルーティングの構成で、パブリックまたはインターネット接続から 1 つ以上のフロントエンド サーバーまたは 1 つのロード バランサーへのインバウンドとして、ポートが設定されている必要があります。

- Dell Core Server Proxy：HTTPS/8888
- Dell Device Server：HTTPS/8081
- Dell Policy Proxy：TCP/8000
- Dell Security Server：HTTPS/8443

バックエンド サーバーへの DMZ またはフロントエンド通信 (必要な場合)

次のサービスとポートは、フロントエンド モードで構成したすべての Security Management Server と、バックエンド モードで構成した Security Management Server との間の通信を行います。ファイアウォールまたはルーティングの構成で、1 つ以上のフロントエンド サーバーまたはロード バランサーからバックエンド サーバーへのインバウンドとして、ポートが設定されている必要があります。

- フロントエンド Dell Policy Proxy および Dell Beacon Server からバックエンド Dell Message Broker：STOMP/61613
- フロントエンド Dell Security Server Proxy からバックエンド Dell Security Server：HTTPS/8443
- フロントエンド Dell Core Server Proxy からバックエンド Dell Core Server：HTTPS/8888
- フロントエンド Dell Device Server からバックエンド Dell Security Server：HTTPS/8443

バックエンド サーバーから内部ネットワークへ

次のサービスとポートは、ドメイン上に存在するか VPN を介して接続されているクライアントによって、各サービスとの内部的な通信に使用されます。Dell Technologies では、これらのサービスの一部をネットワーク外に転送しないことを、またはフロントエンド サーバー構成でサービスをデフォルトでフィルタリングすることをお勧めしています。ファイアウォールまたはルーティングの構成で、内部ネットワークからバックエンド Security Management Server へのインバウンドとして、ポートが設定されている必要があります。

- Dell Security Server でホストされている管理コンソール：HTTPS/8443
- Dell Compliance Reporter から送信されてくるレポート：HTTP(S)/8084

  メモ: このサービスは、デフォルトで無効になっています。代わりに、Dell Security Server によってホストされている管理コンソールで使用可能な管理対象レポートを使用します。Dell Compliance Reporter の履歴レポートを有効にする方法については、KB 記事 SLN314792 を参照してください。
- Dell Core Server：HTTPS/8888
- Dell Device Server：HTTP(S)/8081

  メモ: この従来のサービスは、8.x より前のバージョンの Dell Encryption クライアントでのみ必要です。すべてのクライアントが 8.0 以降の環境では、サービスを無効にしてもかまいません。
- キーサーバ：TCP/8050
- Dell Policy Proxy：TCP/8000
- Dell Security Server：HTTPS/8443
- Dell Security Server でホストされている証明書ベースの認証：HTTPS/8449

  メモ: Windows Server オペレーティング システムにインストールされた Dell Encryption クライアント、またはサーバー モードでインストールされたクライアントで、この機能が使用されます。このサーバー モードでのクライアントのインストールに関する詳細については、『Dell Encryption Enterprise 詳細インストール ガイド』を参照してください。

インフラストラクチャ通信

- Active Directory、Dell Encryption TCP/389/636（ローカル ドメイン コントローラー）、TCP/3268/3269（グローバル カタログ）、TCP/135/49125+（RPC）によるユーザー認証に使用
- E メール通信（オプション）: 25/587
- Microsoft SQL Server：1433（デフォルト ポート）

Microsoft SQL データベースの作成と管理

Dell サーバー データベースの作成：

次の手順はオプションです。データベースが存在しない場合、インストーラーはデフォルトでデータベースを作成します。Security Management Server をインストールする前にデータベースをセットアップする場合は、次の手順に従って、SQL Management Studio に SQL データベースと SQL ユーザーを作成してください。Security Management Server のインストール時に自動的に作成されたものでない場合、SQL データベースに対して適切な権限を設定するようにします。必要な権限のリストについては、ソフトウェア要件に関する項を参照してください。

データベースを事前に作成する場合は、「既存データベースでのバックエンド サーバーのインストール」の手順に従ってください。

Security Management Server は、SQL 認証と Windows 認証の両方に対応しています。

メモ: SQL データベースまたは SQL インスタンスでサポートされているデフォルト以外の想定照合は、「SQL_Latin1_General_CP1_CI_AS」照合です。照合では、大文字と小文字を区別し、アクセントを区別する必要があります。

インストールの前提条件

前提条件は、Security Management Server のインストール時にデフォルトで、Windows Server オペレーティング システムにインストールされます。次の前提条件は、再起動の必要性を回避するため、Security Management Server をインストールする前にインストールしておくこともできます。

Visual C++再頒布可能パッケージのインストール

インストールされていない場合は、Visual C++ 2010、2013、2015（以降）の再頒布可能パッケージをインストールしてください。オプションで、Security Management Server インストーラーにこれらのコンポーネントのインストールを許可することができます。

メモ: Microsoft Visual C++再頒布可能パッケージをインストールすると、再起動が必要になる場合があります。

Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 - https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads

.NET Framework 4.5 のインストール

.NET Framework 4.5 は、Windows Server 2012 R2 以降では Server Manager の機能の一部としてプリインストールされています。

SQL Native Client 2012 のインストール

SQL Server 2012 または SQL Server 2016 を使用している場合は、SQL Native Client 2012 をインストールしてください。オプションで、Security Management Server インストーラーにこのコンポーネントのインストールを許可することができます。http://www.microsoft.com/en-us/download/details.aspx?id=35580

サーバー インストール ライセンスのインポート

新規インストールの場合 - プロダクト キー(ファイルの名前は *EnterpriseServerInstallKey.ini*)を `C:\Windows` にコピーして、Security Management Server インストーラーで 32 文字のプロダクト キーが自動的に入力されるようにします。

メモ: EnterpriseServerInstallKey.ini は、Security Management Server のダウンロード パッケージに収録されています。このパッケージはこちらから入手できます。

サーバーのプリインストールの設定が完了しました。「インストールまたはアップグレード / 移行」に進みます。

4

インストールまたはアップグレード / 移行

本章では、次の操作に対する手順を説明します。

- 新規インストール - 新しい Security Management Server をインストールします。
- アップグレード / 移行 - 既存の Enterprise Server v9.2 以降からアップグレードします。
- Security Management Server のアンインストール - 必要に応じて、現在のインストールを削除します。

  メインサーバ (バックエンド) を複数インストールする必要がある場合は、Dell ProSupport の担当者にお問い合わせください。

インストールまたはアップグレード / 移行を開始する前に

作業を開始する前に、該当する「インストール前の設定」の手順が完了していることを確認します。

Security Management Server のインストールに関連する最新の回避策または既知の問題については、『*Security Management Server テクニカルアドバイザリー*』をお読みください。

Security Management Server のインストールまたはアップグレード中は、Microsoft C++ランタイム インストーラー、Java の動作 (証明書の作成と操作)、および PostgreSQL の作成/変更処理に影響を与えないように、アンチウイルス ソフトウェアおよびマルウェア対策ソフトウェアを無効にする必要があります。これらの項目はすべて、実行可能ファイルまたはスクリプトによってトリガーされます。

回避策として、次を除外します。

- [INSTALLATION PATH]:\Dell\Enterprise Edition
- C:\Windows\Installer
- インストーラーの実行元であるファイル パス

デルでは、データベースのベストプラクティスをデルサーバのデータベースに使用し、組織の災害復旧計画にデルソフトウェアを含めることを推奨しています。

DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

本番稼働の場合、デルでは、専用サーバーに SQL Server をインストールすることを強く推奨します。

フロントエンドサーバをインストールして設定する前に、バックエンドサーバをインストールすることがベストプラクティスです。

インストールのログファイルは次のディレクトリに保存されます。`C:\Users\<LoggedOnUser>\AppData\Local\Temp`

新規インストール

バックエンドサーバのインストールでは、次の 2 つのオプションのどちらかを選択します。

- バックエンドサーバと新規データベースのインストール - Security Management Server と、新規データベースをインストールします。
- 既存データベースでのバックエンドサーバのインストール - 新しい Security Management Server をインストールして、インストール前の設定中に作成された SQL データベースまたは v9.x 以降の既存の SQL データベースに接続します (スキーマバージョンがインストールする Security Management Server のバージョンに一致する場合)。v9.2 以降のデータベースは、最新バージョンのサーバ設定ツールを使用して最新のスキーマに移行する必要があります。サーバー設定ツールを使用したデータベース移行の手順については、「データベースの移行」を参照してください。最新のサーバ設定ツールを入手するには、または v9.2 より前のデータベースを移行する場合は、Dell ProSupport に問い合わせてサポートを受けてください。

メモ:

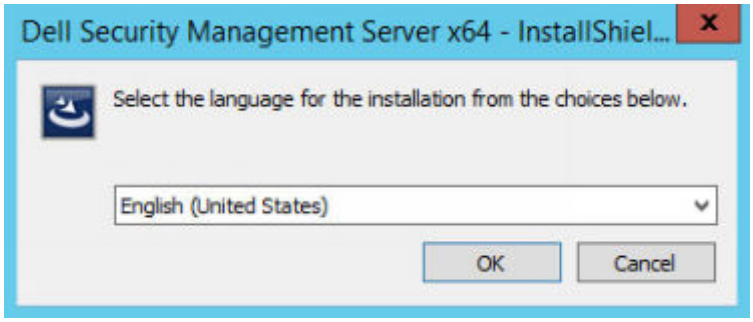
Enterprise Server v9.2 以降を実行している場合は、「**バックエンドサーバのアップグレード / 移行**」の手順を参照してください。

フロントエンドサーバをインストールする場合は、バックエンドサーバのインストールを行ってからこのインストールを実行します。

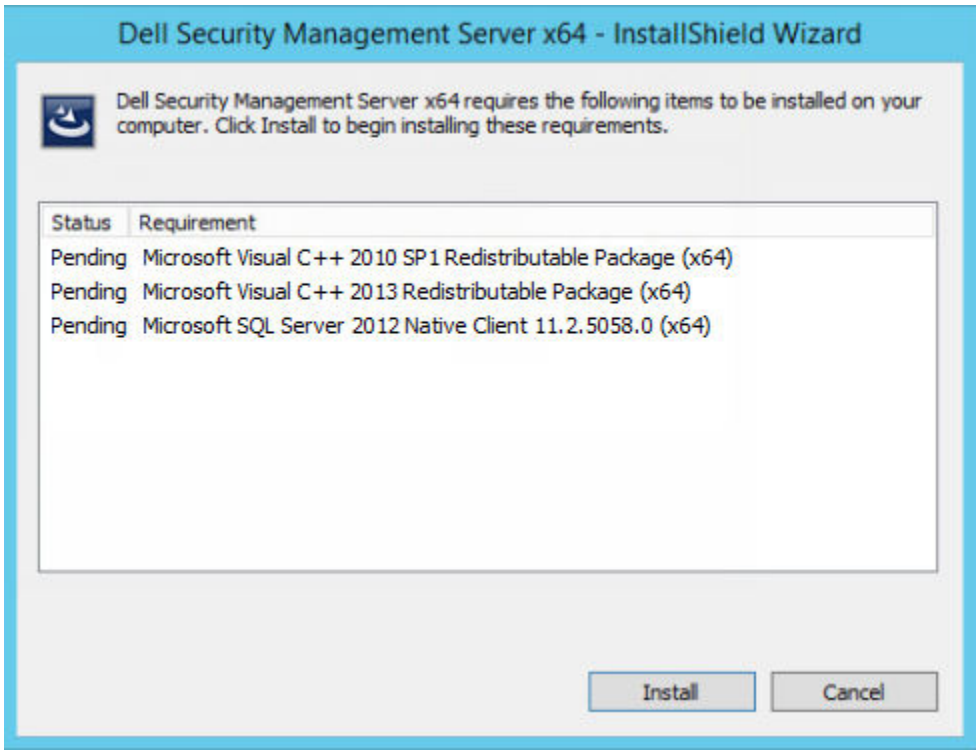
- フロントエンドサーバのインストール - バックエンドサーバと通信するようにフロントエンドサーバをインストールします。

バックエンドサーバーと新規データベースのインストール

1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。***コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. インストール用言語を選択して **OK** をクリックします。

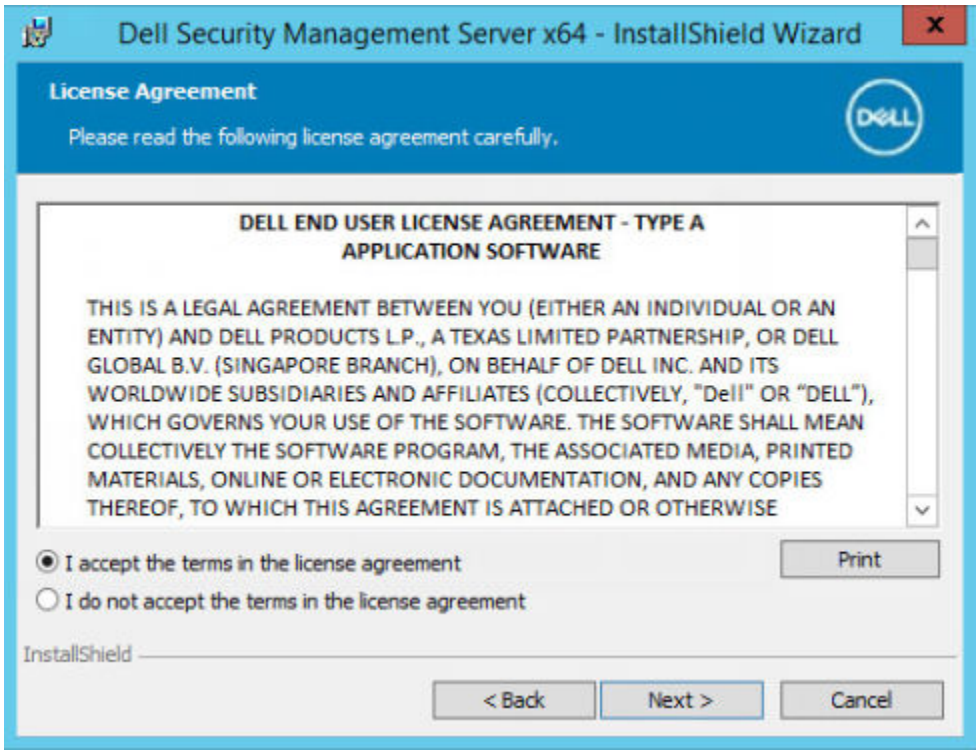


4. 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

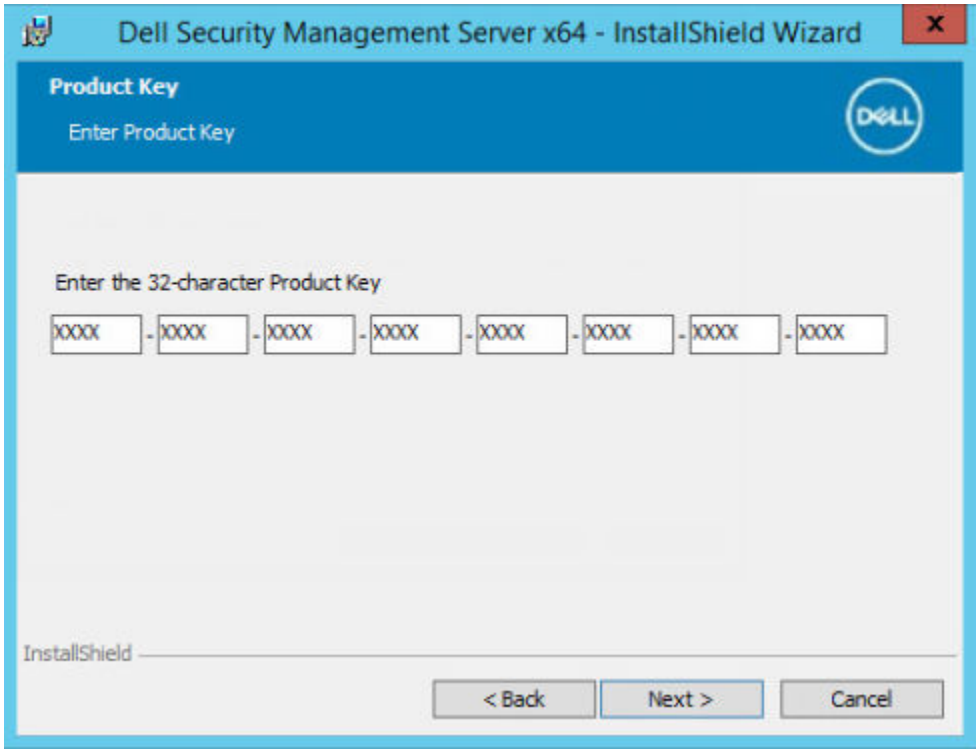


5. *ようこそ*ダイアログで **次へ** をクリックします。

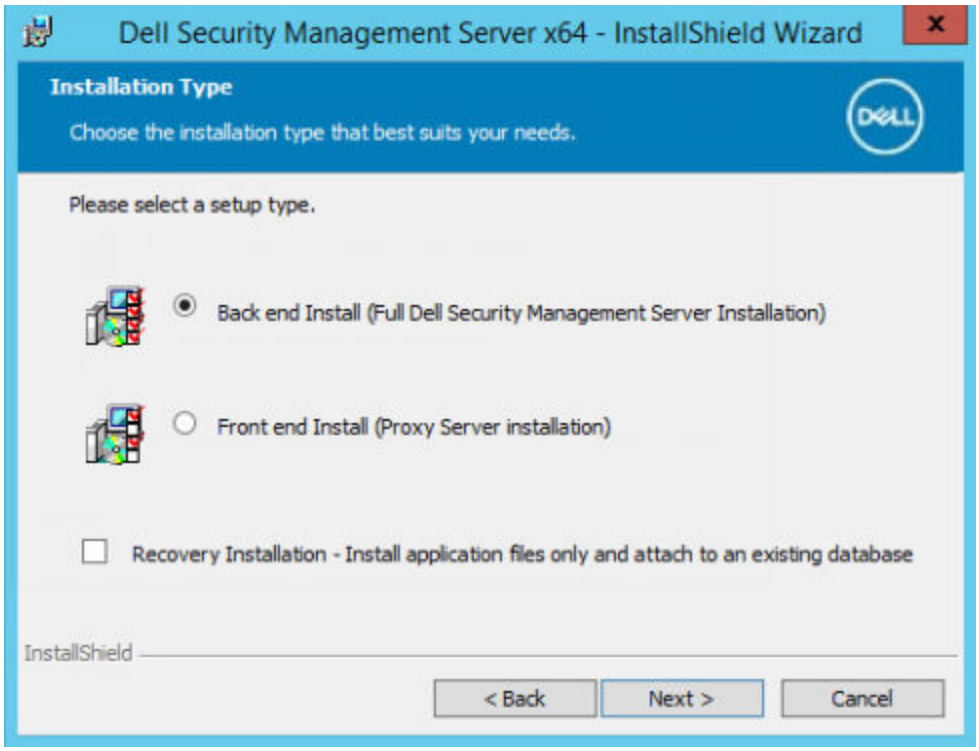
6. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。



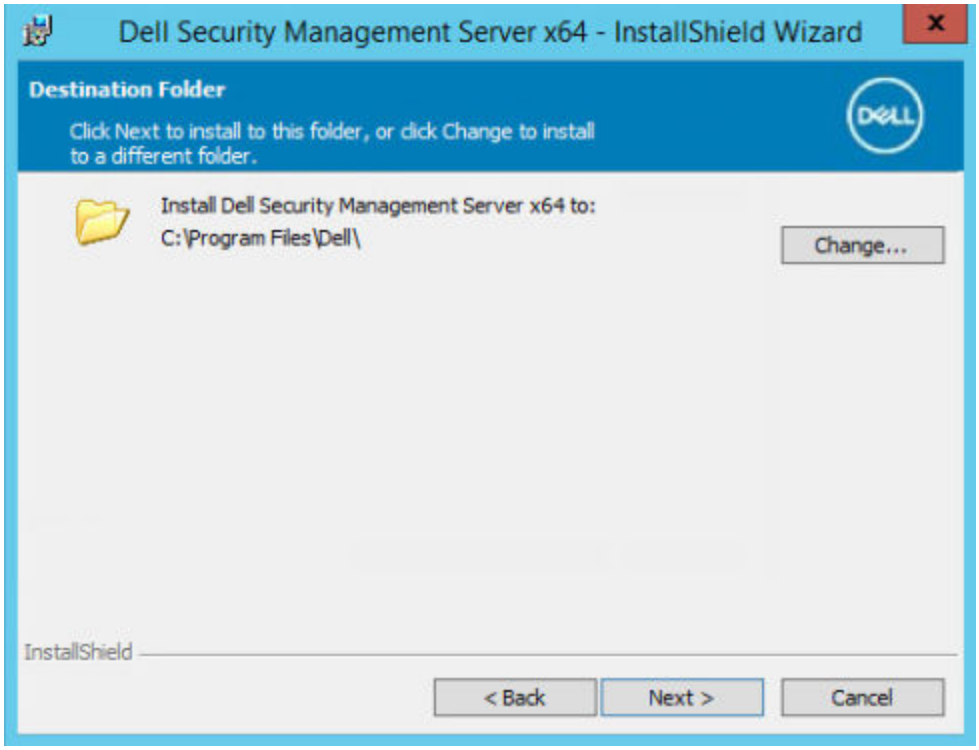
7. 「インストール前の設定」で説明したとおり、`EnterpriseServerInstallKey boot.ini` ファイルを `C: ¥ Windows` にコピーした場合は、**次へ** をクリックします。完了していない場合は、32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーはファイル「`EnterpriseServerInstallKey.ini`」にあります。



8. **バックエンドインストール** を選択し、**次へ** をクリックします。

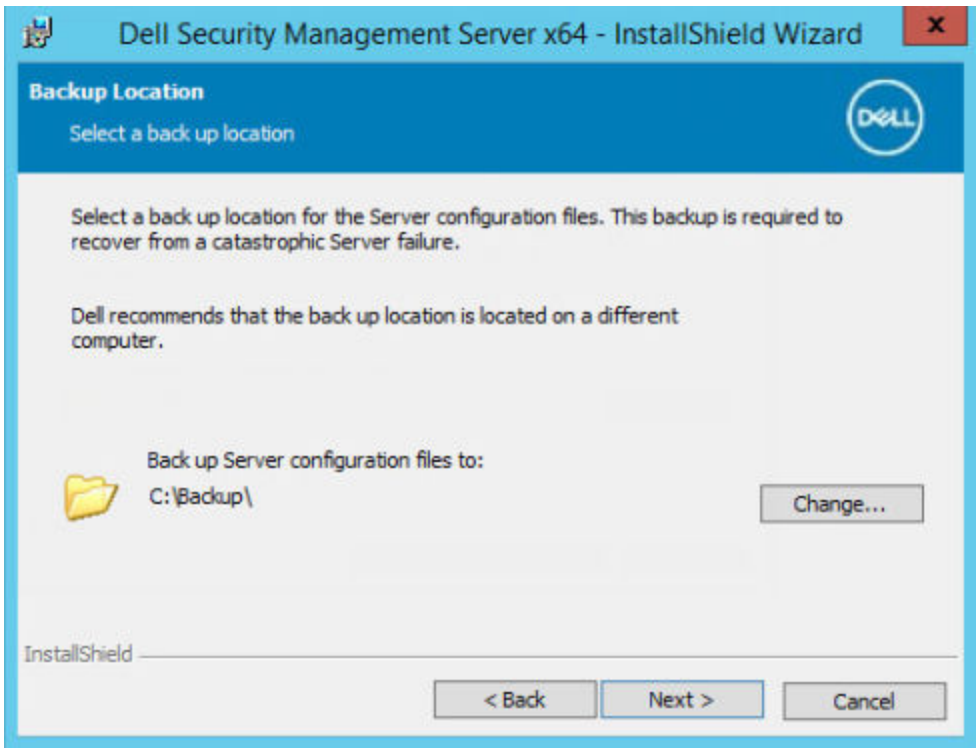


9. Security Management Server をデフォルトの `C:\Program Files\Dell` にインストールする場合は、**次へ** をクリックします。
それ以外の場所にインストールする場合は、**変更** をクリックして別の場所を選択し、**次へ** をクリックします。



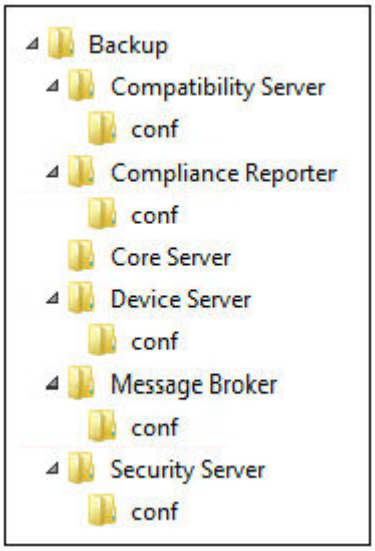
10. バックアップ設定ファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。

    デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。



サーバー設定ツールで行われた変更を含む、インストール後に設定ファイルに対して行われた変更は、これらのフォルダに手動でバックアップする必要があります。設定ファイルは、デルサーバを手動で復元するときに必要に応じて使用する、全情報の中でも重要な要素です。

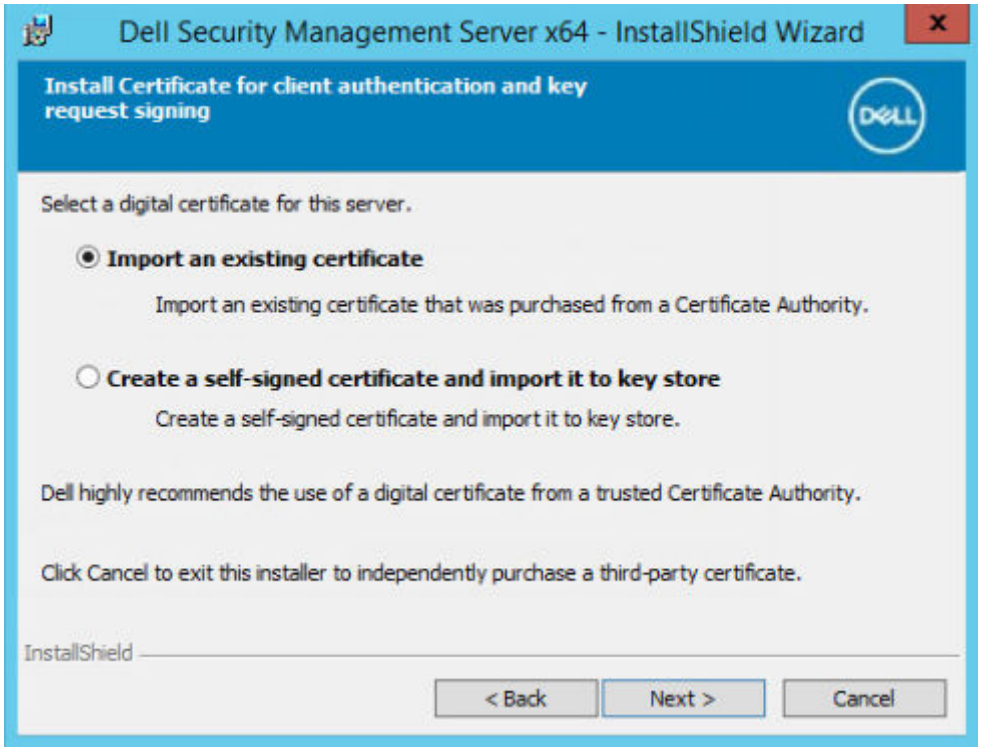
メモ: このインストール中にインストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



11. 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**

    以下のオプション「a」または「b」を選択します。

    a. CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。



    参照 をクリックして、証明書のパスを入力します。

    この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

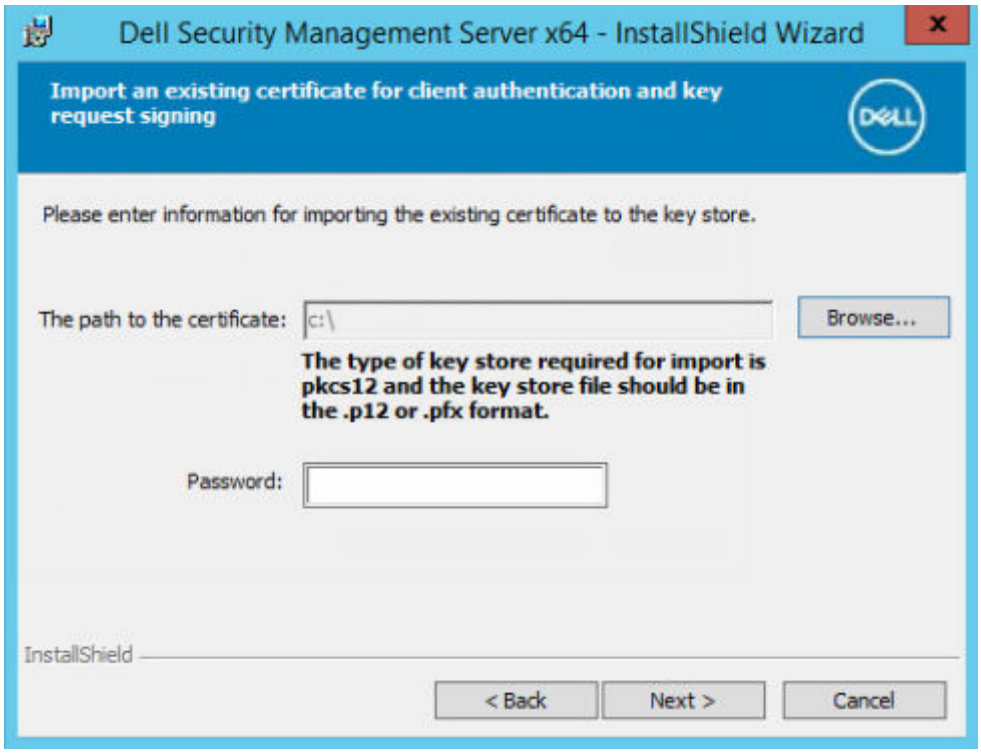
    次へ をクリックします。

    メモ:

    この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

    - Personal Information Exchange - PKCS#12 (.PFX)

- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする



または

b. 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする** を選択し、**次へ** をクリックします。

Create Self-Signed Certificate（自己署名証明書の作成）ダイアログで、次の情報を入力します。

完全修飾コンピュータ名（例：computername.domain.com）

組織

組織単位（例：Security）

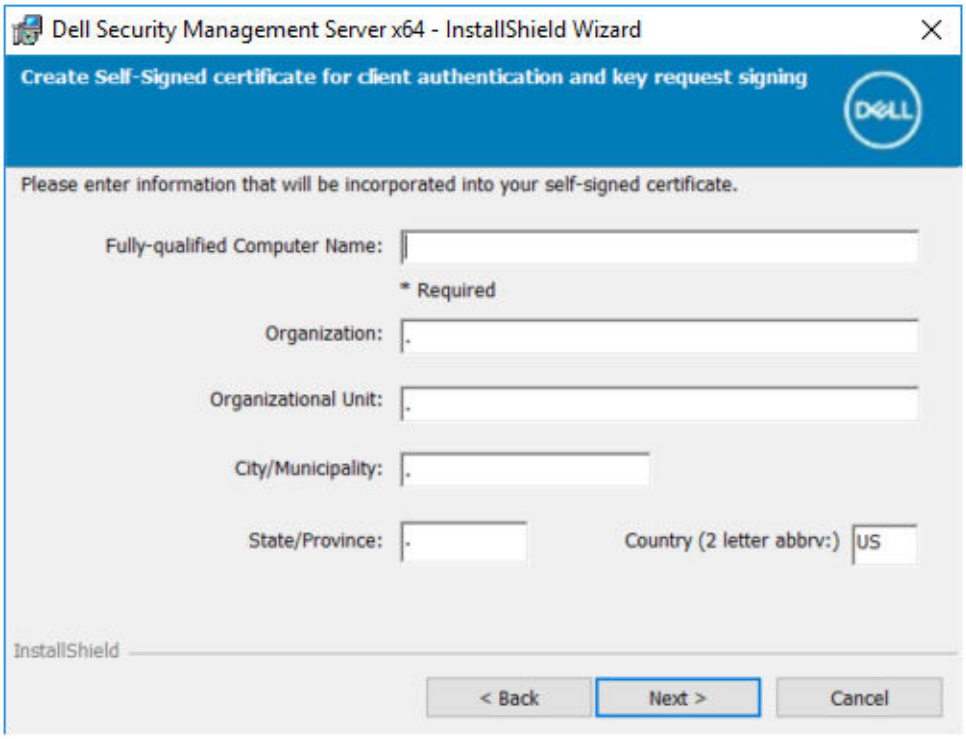
都市

州（正式名）

国：国を表す 2 文字の略語

次へ をクリックします。

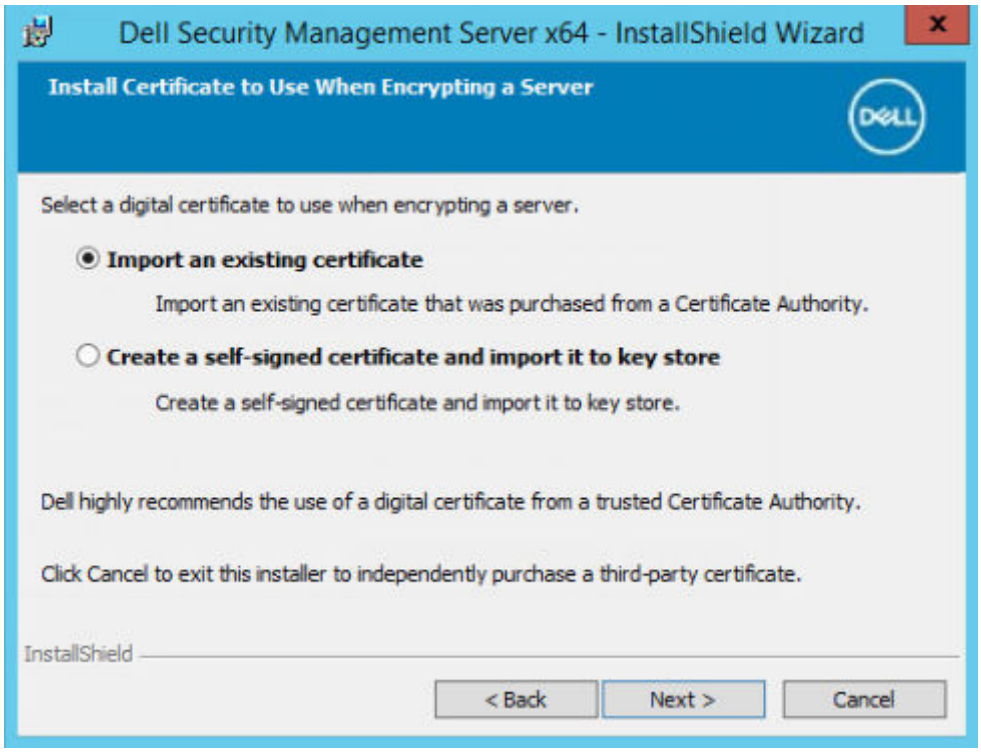
メモ: デフォルトでは、証明書は 10 年で期限切れになります。



12. サーバ暗号化では、使用するデジタル証明書のタイプを選択することができます。デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。

    以下のオプション「a」または「b」を選択します。

    a. CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。



    参照 をクリックして、証明書のパスを入力します。

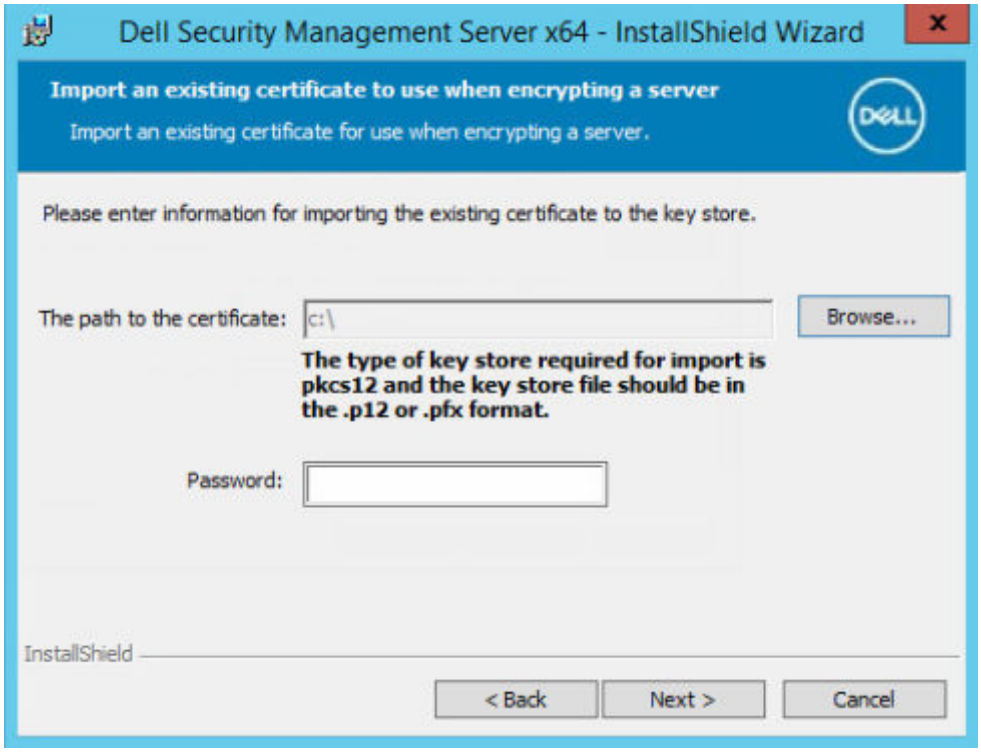
    この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

    次へ をクリックします。

メモ:

この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12 (.PFX)
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする



または

b. 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。

自己署名証明書の作成 ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

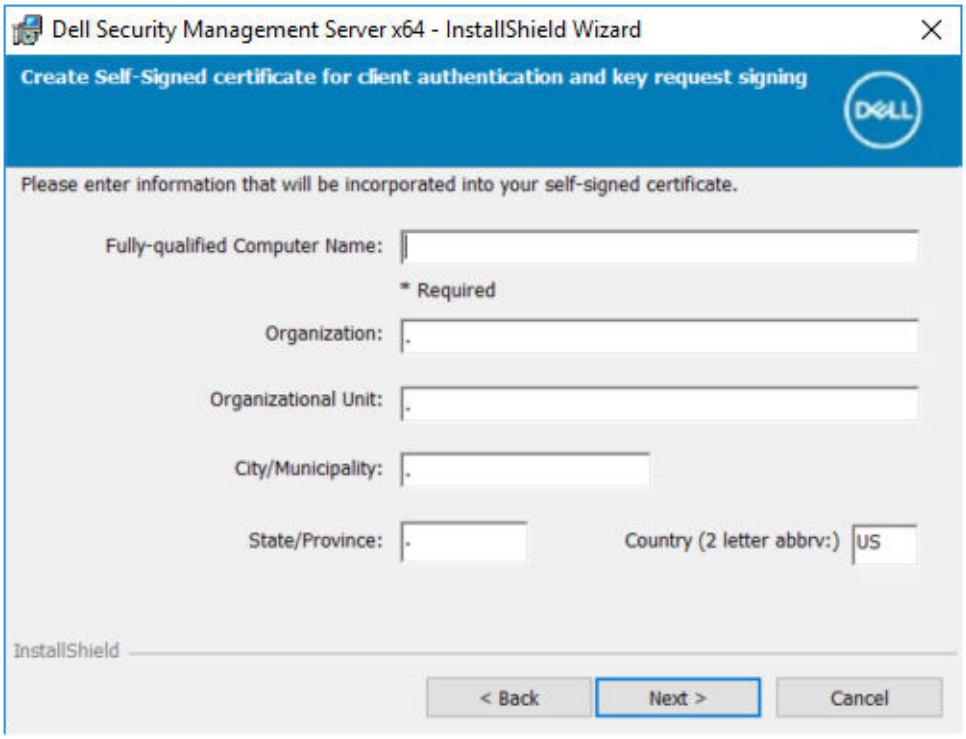
都市

州 (正式名)

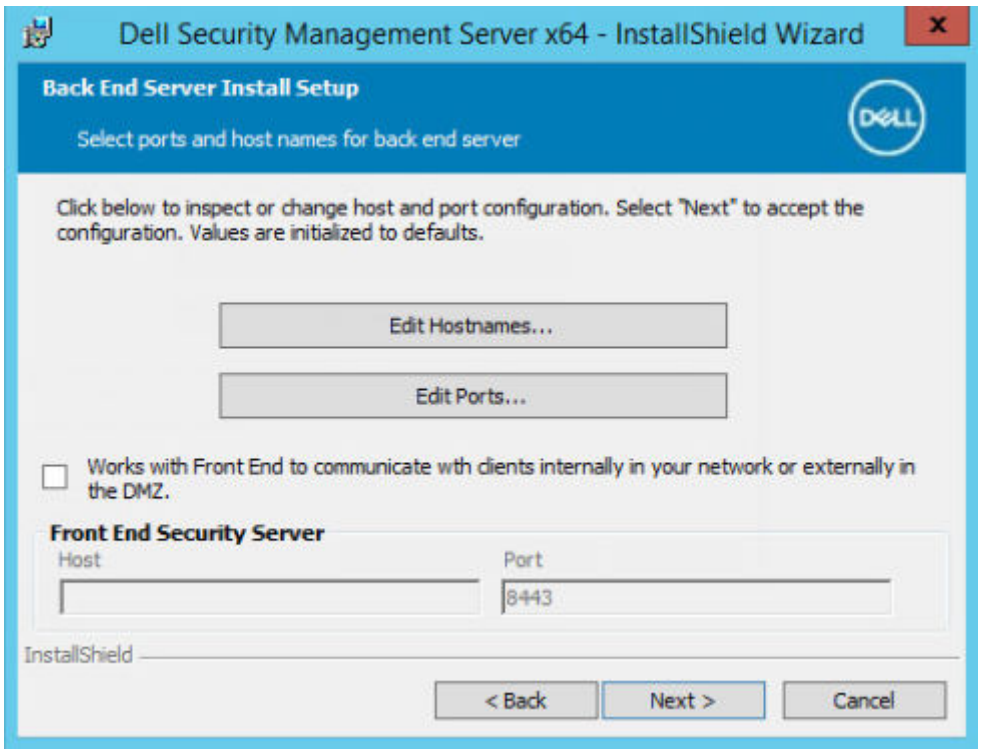
国 : 国を表す 2 文字の略語

次へ をクリックします。

メモ: デフォルトでは、証明書は 10 年で期限切れになります。



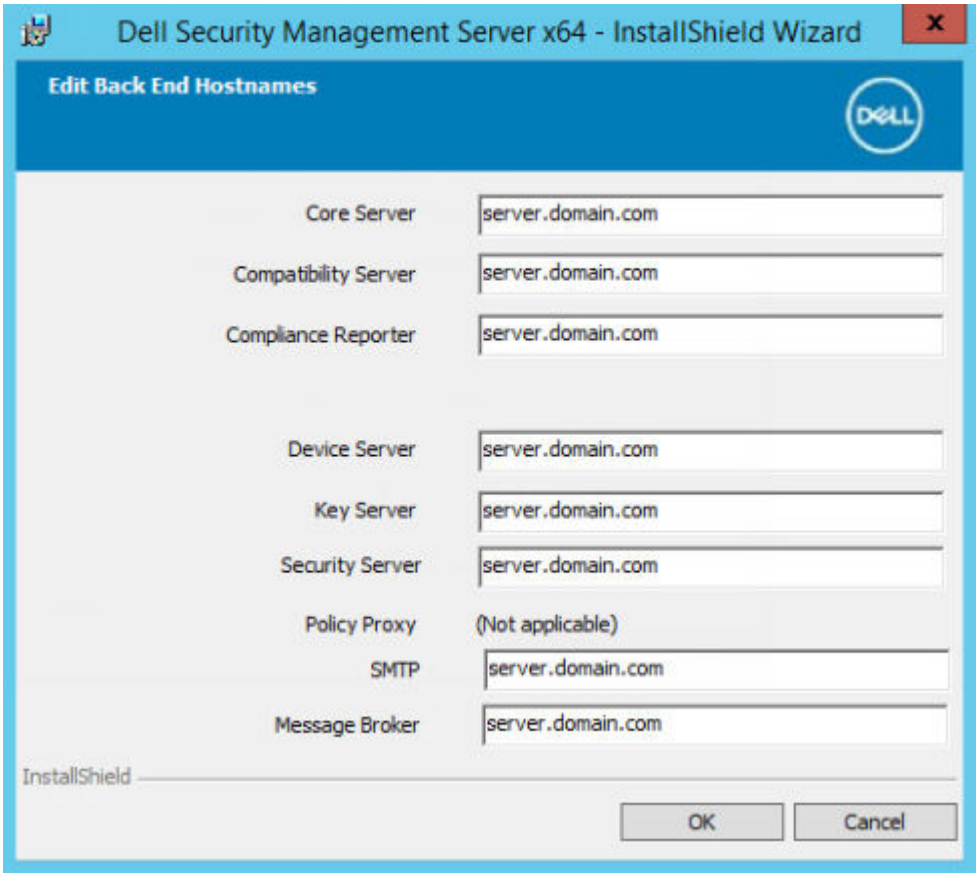
13. *バックエンドサーバーインストール設定*ダイアログから、ホスト名とポートを表示または編集できます。
    - デフォルトのホスト名とポートを使用する場合は、*バックエンドサーバーインストール設定*ダイアログで、**次へ** をクリックします。
    - フロントエンドサーバを使用している場合は、**ネットワークのクライアントとの内部通信、または DMZ のクライアントとの外部通信のために、フロントエンドと連携** を選択し、フロントエンドのセキュリティサーバのホスト名を入力します（server.domain.com など）。



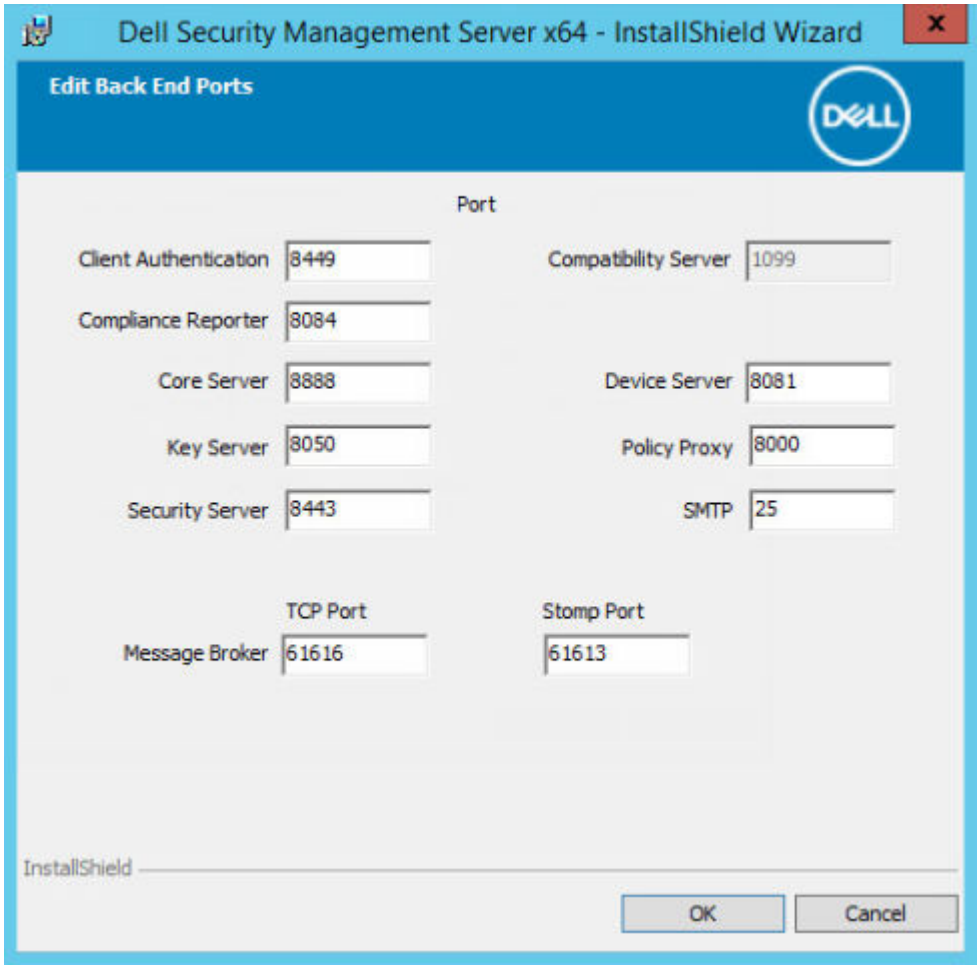
- ホスト名を表示または編集するには、**ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

  メモ: ホスト名に下線（「_」）は使用できません。

終了したら、**OK** をクリックします。

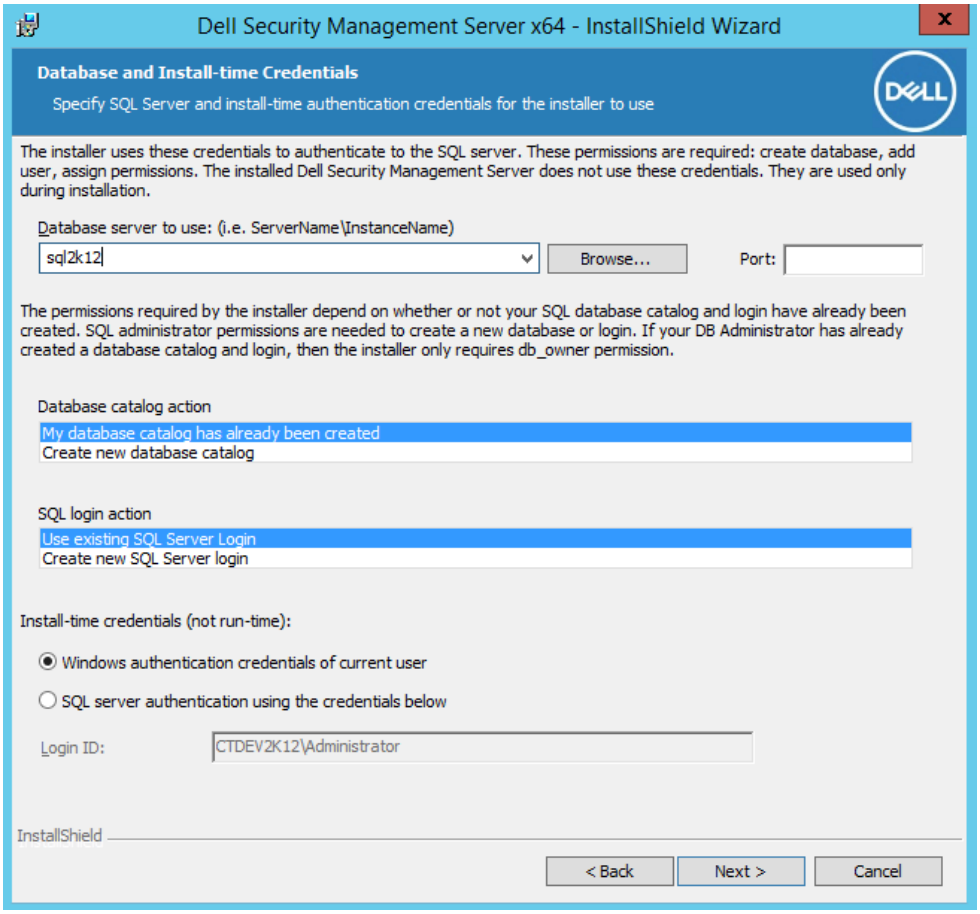


- ポートを表示または編集するには、**ポートの編集** をクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。終了したら、**OK** をクリックします。



14. 新規データベースを作成するには、次の手順に従います。
    a. **参照** をクリックして、データベースをインストールするサーバーを選択します。
    b. デルサーバデータベースのセットアップの際に使用される認証方法を選択します。製品がインストールされた後は、ここで指定された資格情報を使用することはありません。
        - **現在のユーザーの Windows 認証資格情報**

          Windows 認証を選択すると、Windows へのログイン時に使用されたのと同じ資格情報が認証に使用されます（*ユーザー名* フィールドと *パスワード* フィールドは編集できなくなります）。アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。



または

- **以下の資格情報を使った SQL server 認証**

  SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

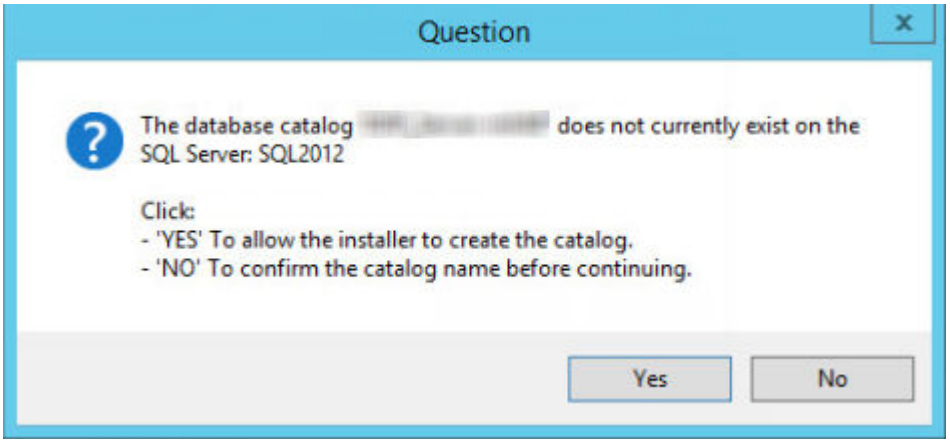
  インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

c. データベースカタログを指定します。

   新規データベースカタログの名前を入力します。次に表示されるダイアログで、新規カタログの作成を促すプロンプトが表示されます。

d. **次へ** をクリックします。

e. **はい** をクリックして、インストーラにデータベースを作成させることを確認します。前の画面に戻って設定を変更するには、**いいえ** をクリックします。



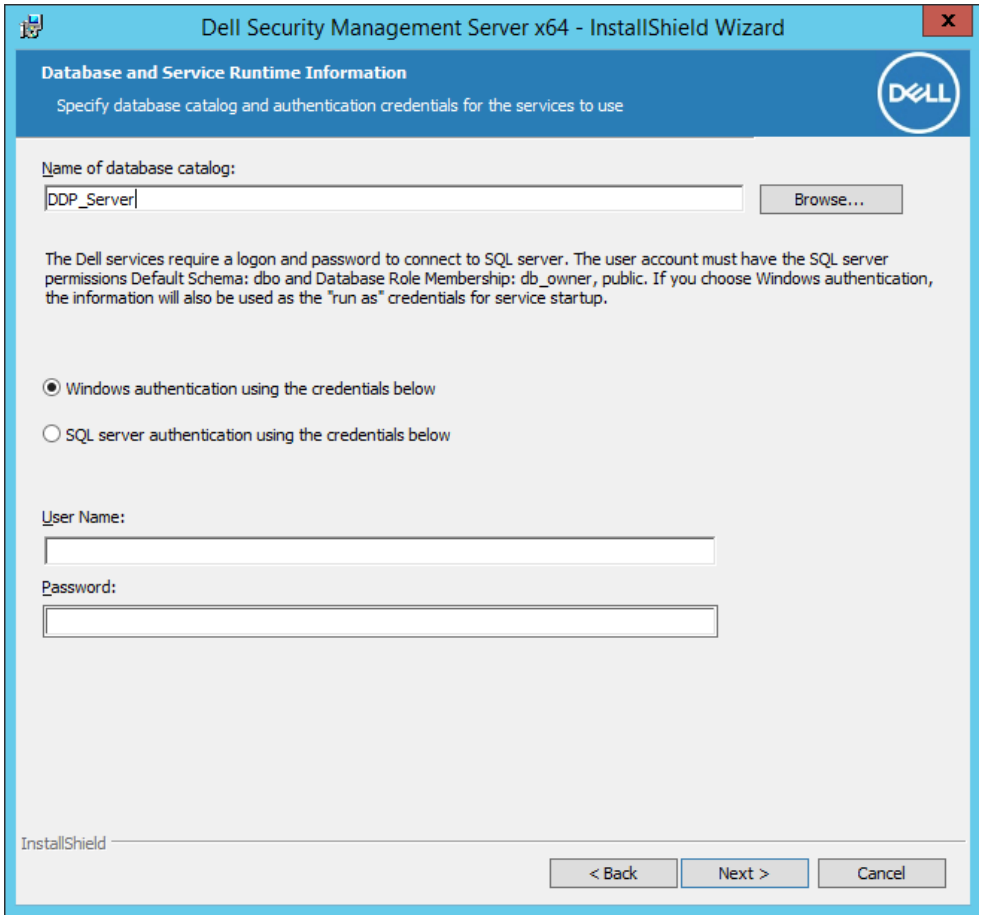
15. 製品が使用するための認証メソッドを選択します。このステップによりアカウントと製品が関連付けられます。

- **Windows 認証**

  以下の資格情報を使用した Windows 認証 を選択し、製品が使用する資格情報を入力してから、**次へ** をクリックします。

  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ： db_owner を public にする必要があります。

  これらの資格情報も Dell サービスが Security Management Server で作業する際に使用されます。

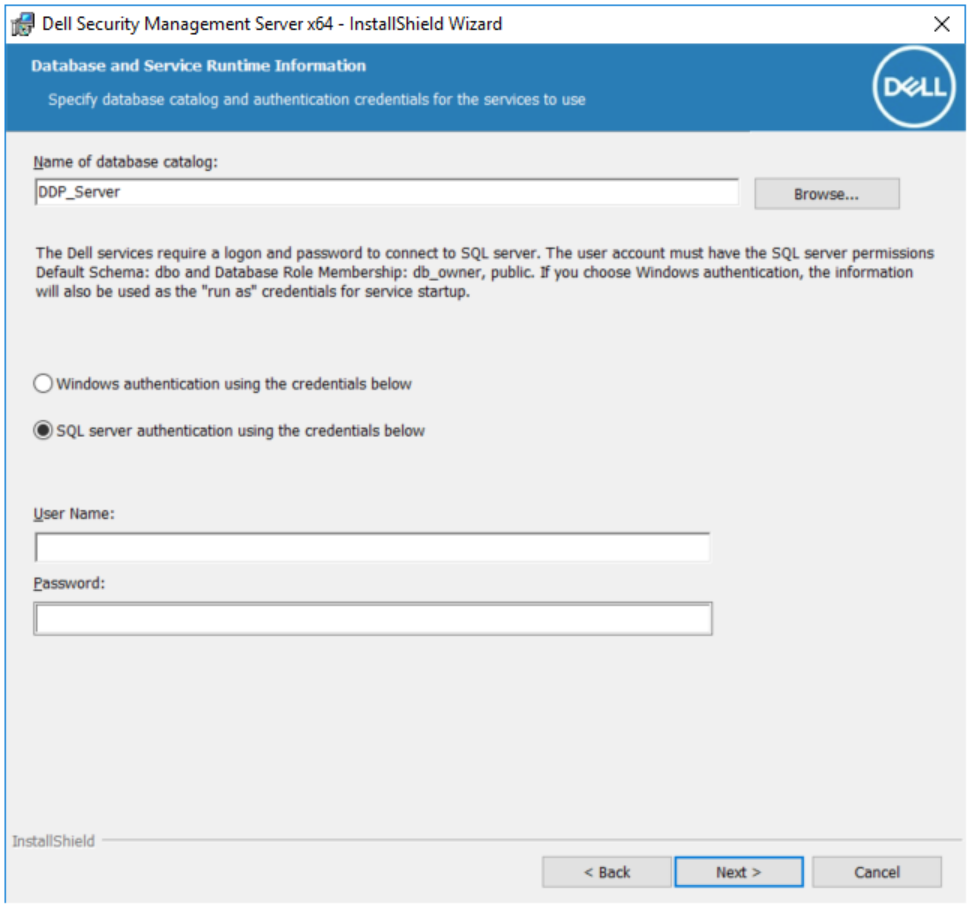


  または

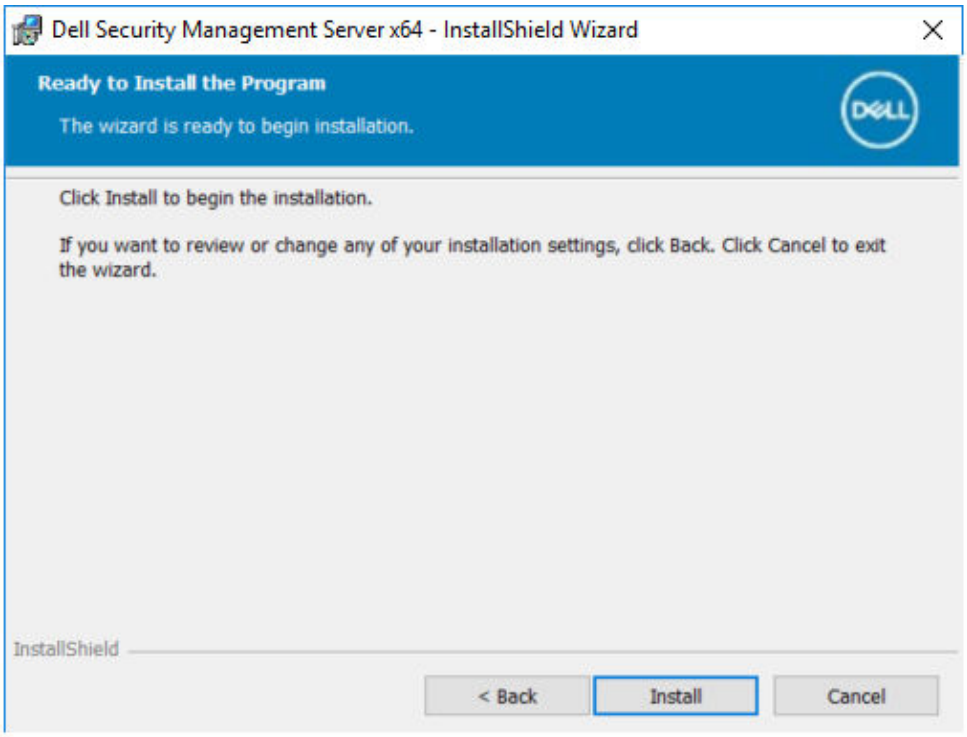
- **SQL Server 認証**

  以下の資格情報を使用した SQL サーバ認証 を選択し、Dell サービスが Security Management Server で動作する際に使用する SQL サーバ資格情報を入力して、**次へ** をクリックします。

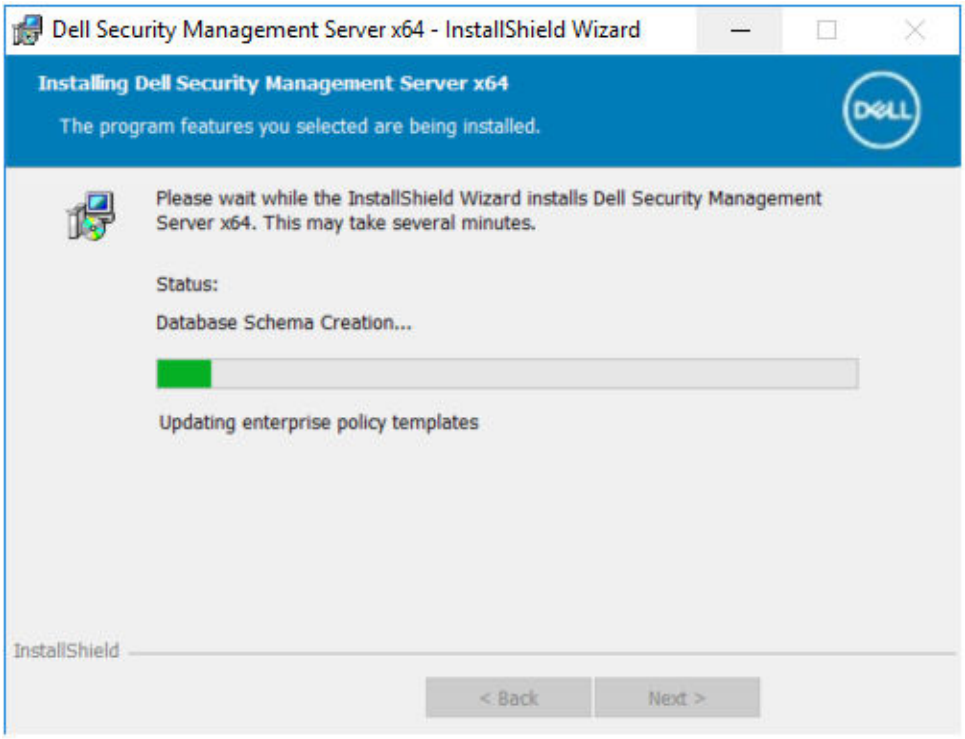
  ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ： db_owner を public にする必要があります。



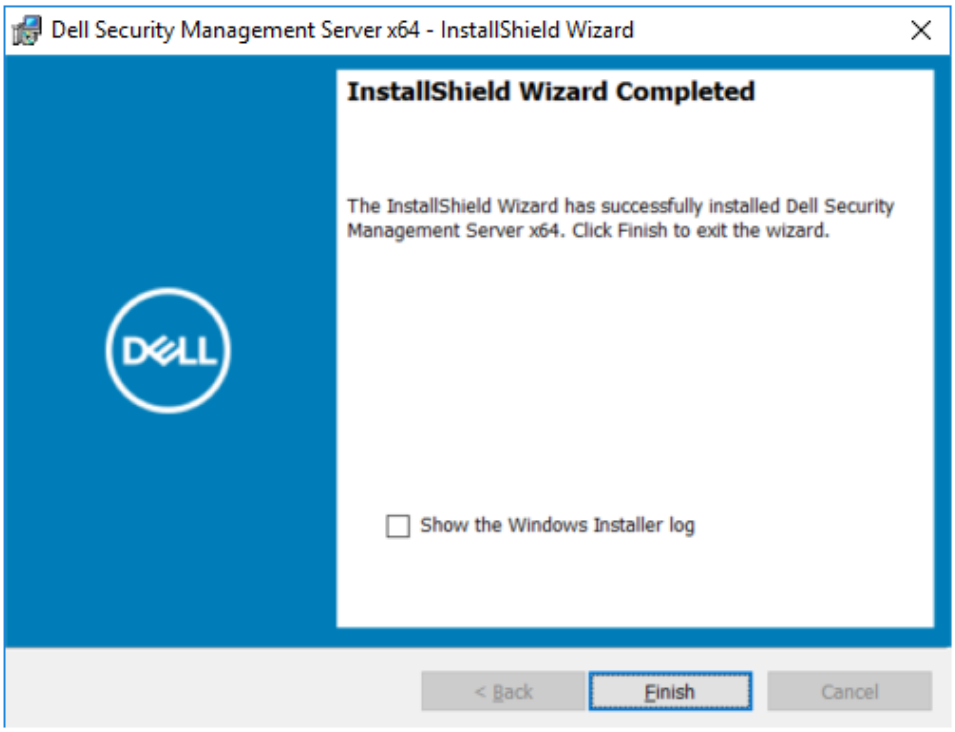
16. *プログラムインストールの準備完了*ダイアログで、**インストール** をクリックします。



ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。



17. インストールが完了したら、**終了** をクリックします。



これでバックエンドサーバーインストールタスクは完了です。

Dell サービスはインストール終了時に再起動されます。デルサーバを再起動する必要はありません。

既存データベースでのバックエンドサーバーのインストール

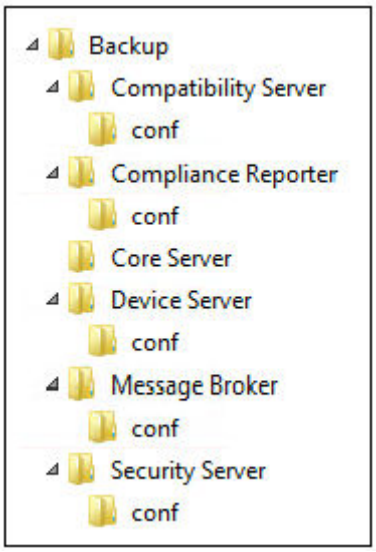
メモ:

デルサーバ v9.2 以降を実行している場合は、「バックエンドサーバのアップグレード / 移行」の手順を参照してください。

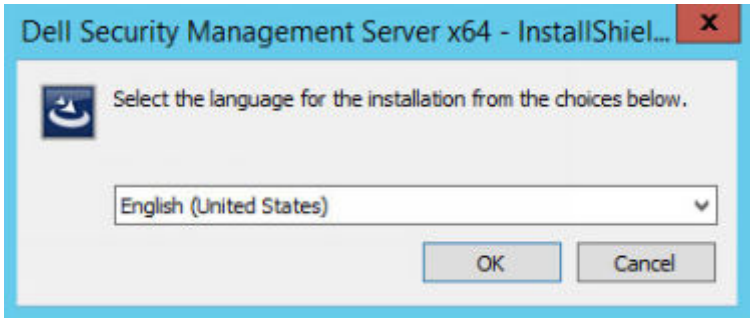
スキーマバージョンがインストールする Security Management Server のバージョンに一致する場合は、新しい Security Management Server をインストールして、インストール前の設定 で作成された SQL データベースまたは v9.x 以降の既存の SQL データベースに接続することができます。

インストールの実行元のユーザーアカウントには、SQL データベース用のデータベース所有者権限が必要です。アクセス権限の有無またはデータベースへのアクセス可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

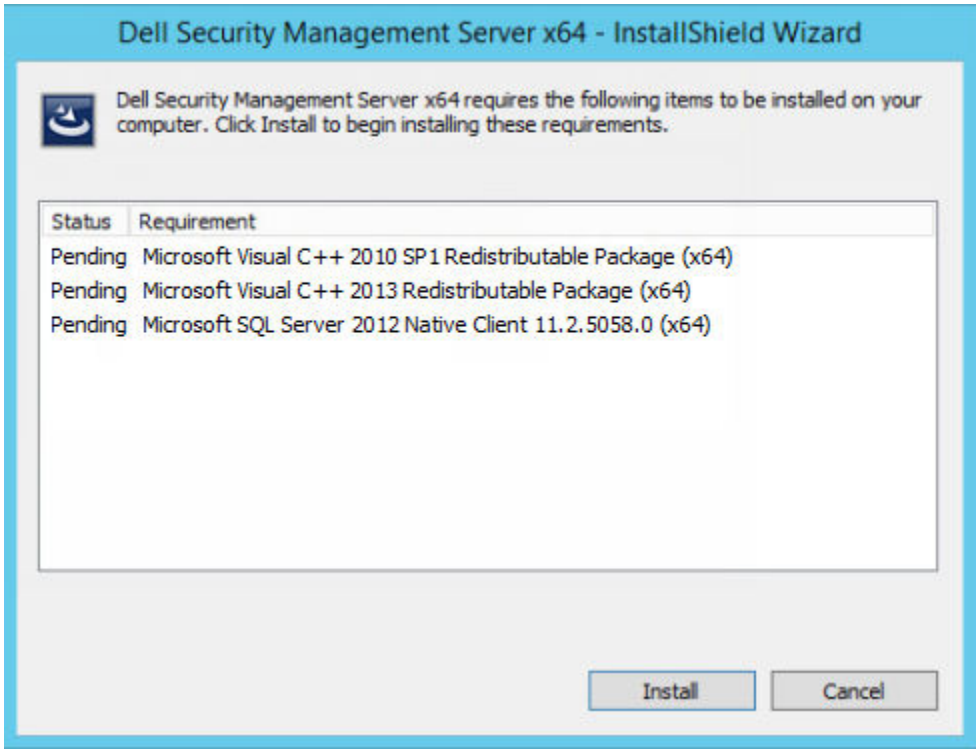
既存のデータベースが Security Management Server で事前にインストールされている場合は、インストールを開始する前に、データベース、設定ファイルおよび secretKeyStore がバックアップされていること、Security Management Server をインストールするサーバからアクセス可能であることを確認します。これらのファイルは、Security Management Server および既存のデータベースを設定するときに必要になります。インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。***コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. インストール用言語を選択して **OK** をクリックします。



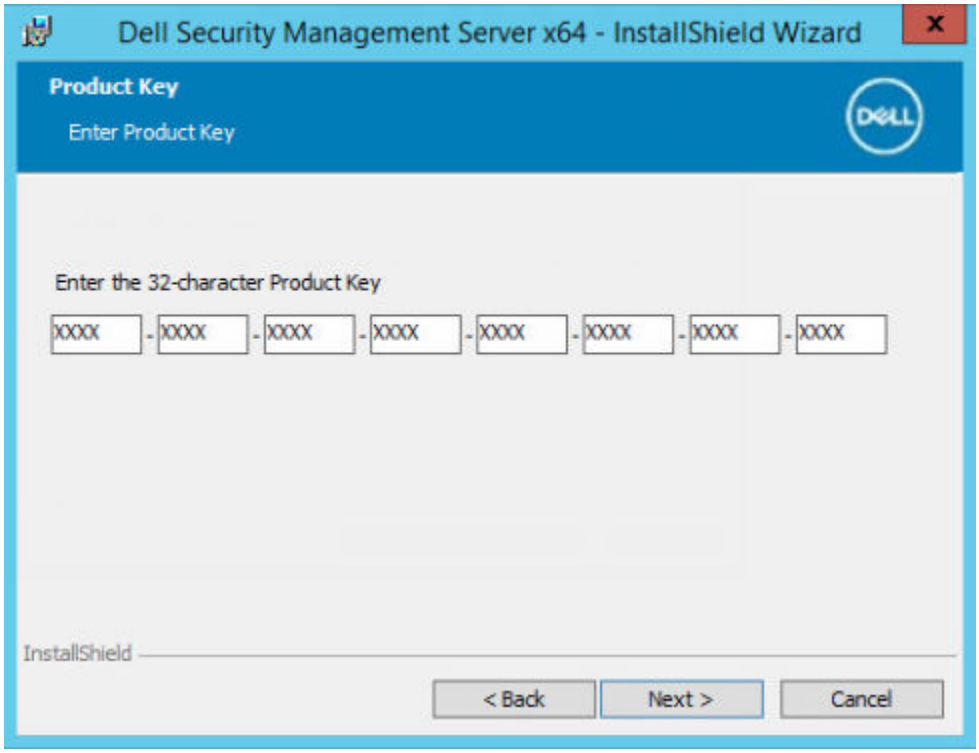
4. 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。



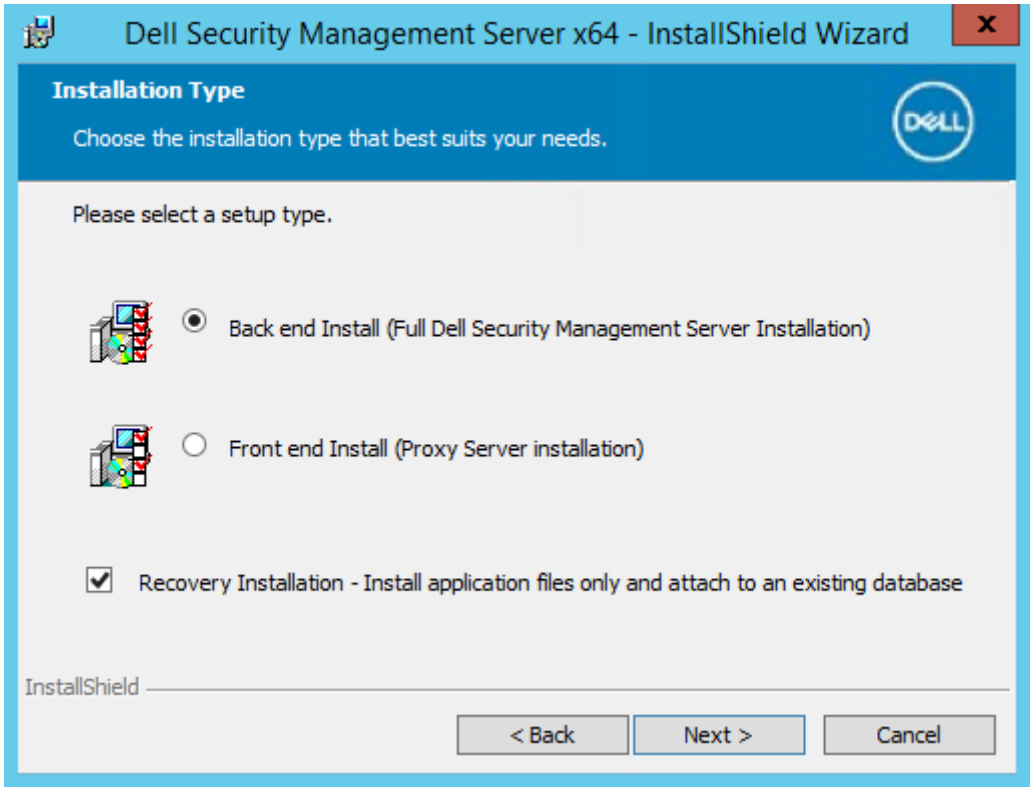
5. *ようこそ*ダイアログで **次へ** をクリックします。

6. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

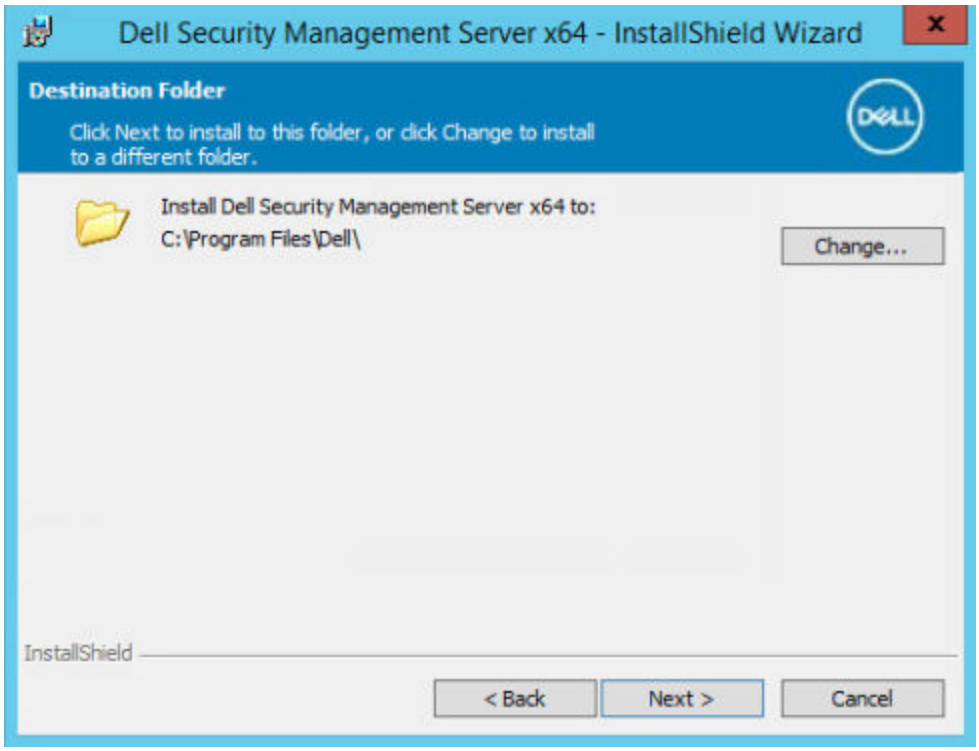
7. 「インストール前の設定」で説明したとおり、`EnterpriseServerInstallKey boot.ini` ファイルを `C: ¥ Windows` にコピーした場合は、**次へ** をクリックします。完了していない場合は、32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーはファイル「`EnterpriseServerInstallKey.ini`」にあります。



8. **バックエンドインストール** および **リカバリインストール** を選択し、**次へ** をクリックします。

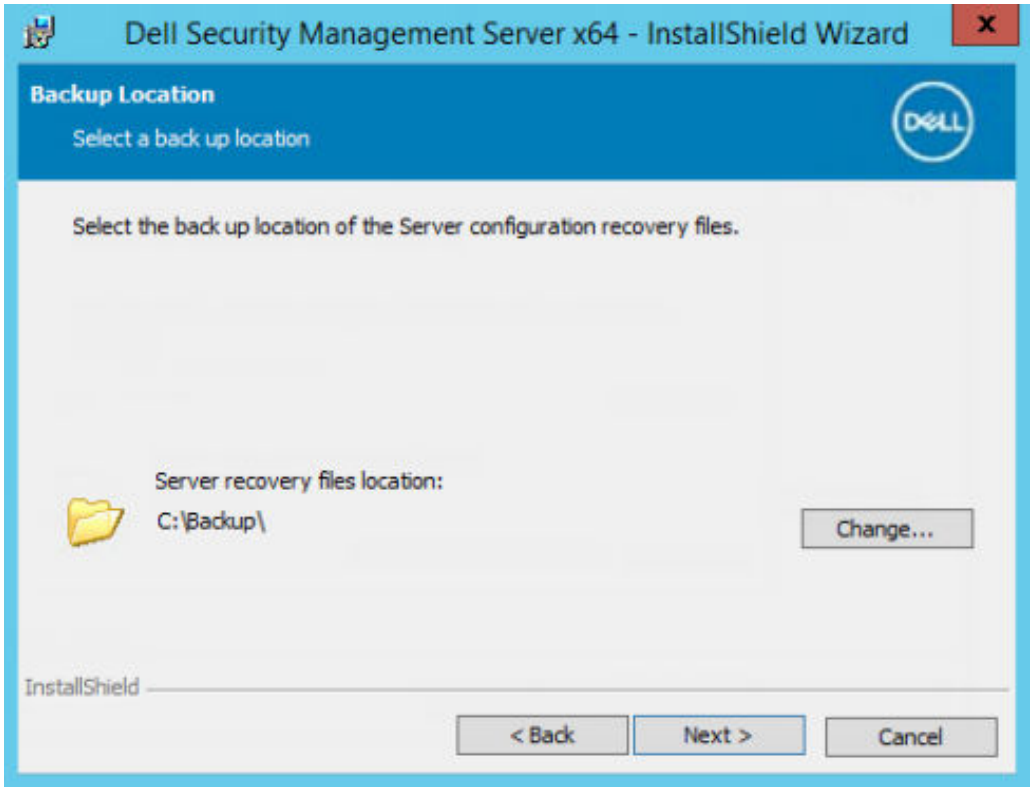


9. Security Management Server をデフォルトの `C:\Program Files\Dell` にインストールする場合は、**次へ** をクリックします。
それ以外の場所にインストールする場合は、**変更** をクリックして異なる場所を選択し、**次へ** をクリックします。



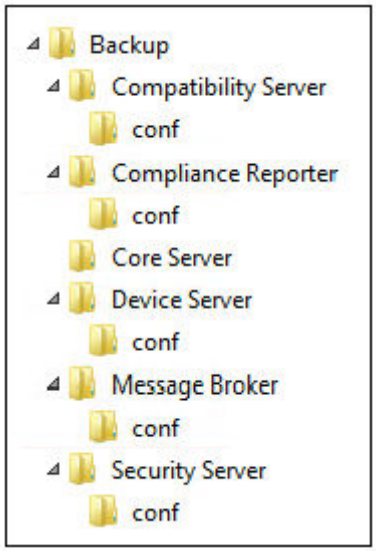
10. バックアップ設定リカバリファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。

デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。



サーバー設定ツールで行われた変更を含む、インストール後に設定ファイルに対して行われた変更は、これらのフォルダに手動でバックアップする必要があります。設定ファイルは、デルサーバを手動で復元するときに使用する情報全体の中でも重要な要素です。

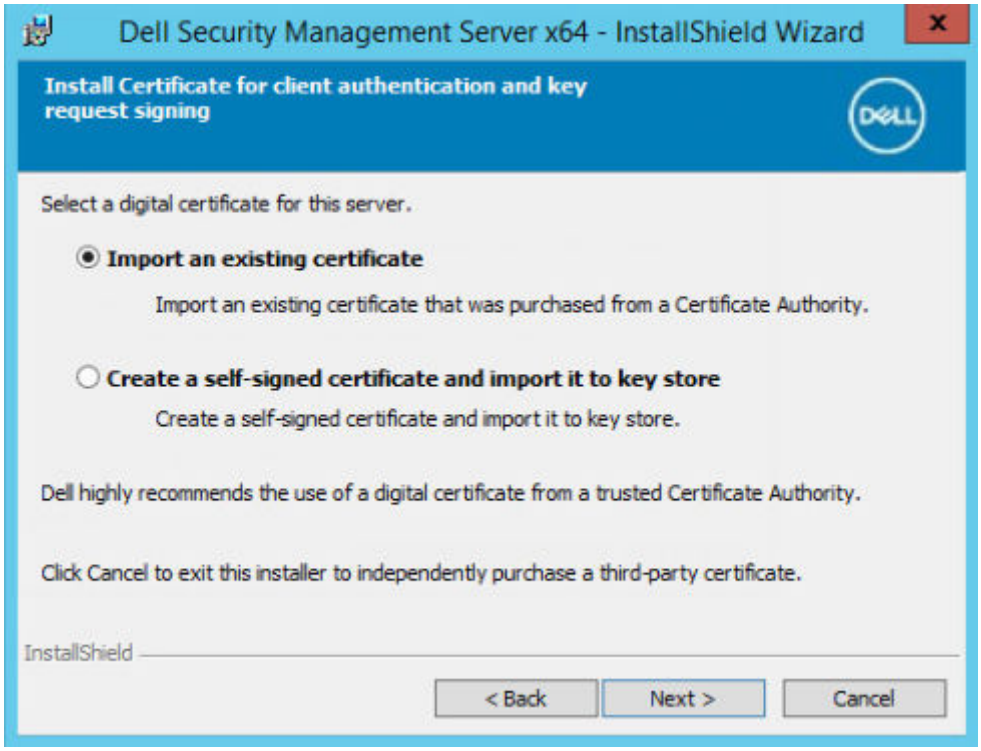
メモ: インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



11. 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**

    以下のオプション「a」または「b」を選択します。

    a. CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。



参照 をクリックして、証明書のパスを入力します。

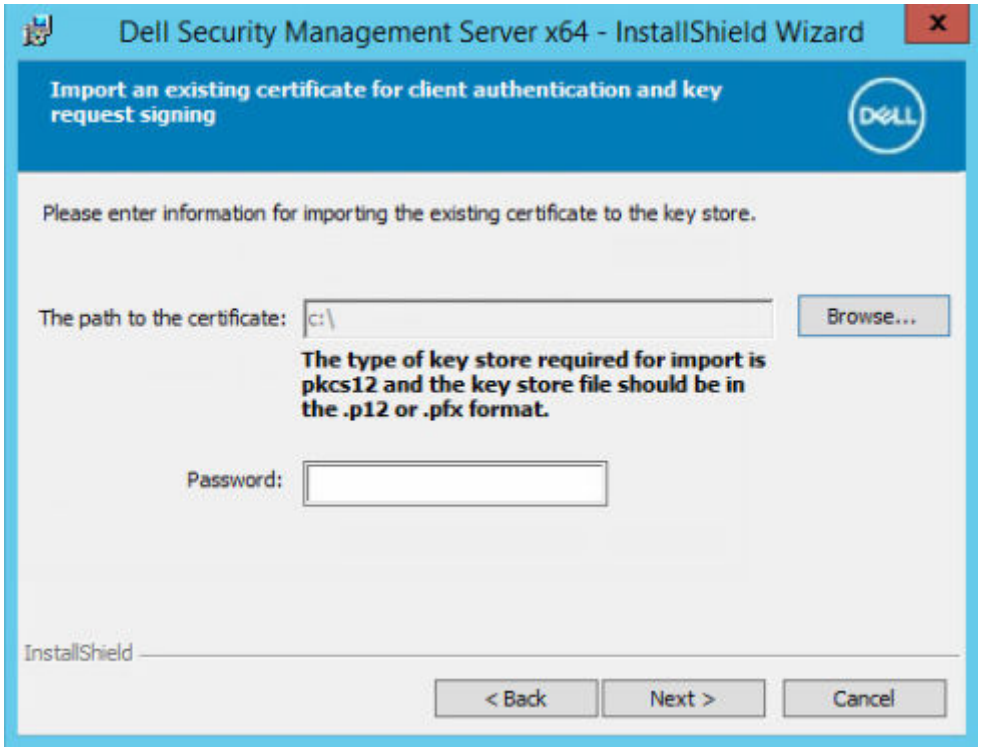
この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

メモ:

この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12 (.PFX)
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする



または

b. 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。

自己署名証明書の作成 ダイアログで、次の情報を入力します。

完全修飾コンピュータ名（例：computername.domain.com）

組織

組織単位（例：Security）

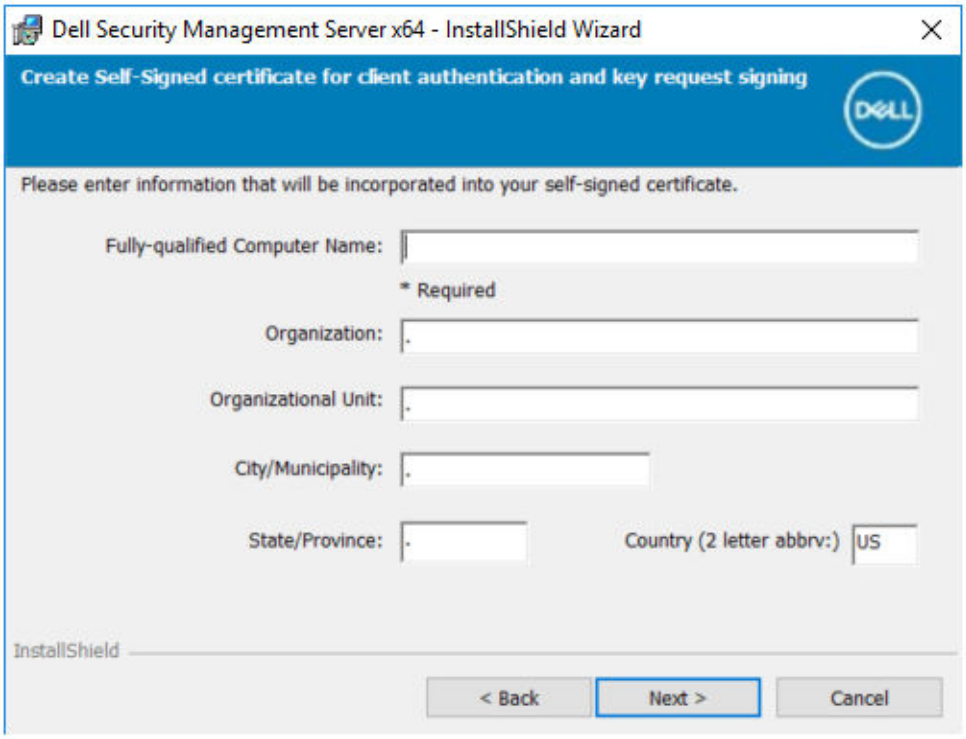
都市

州（正式名）

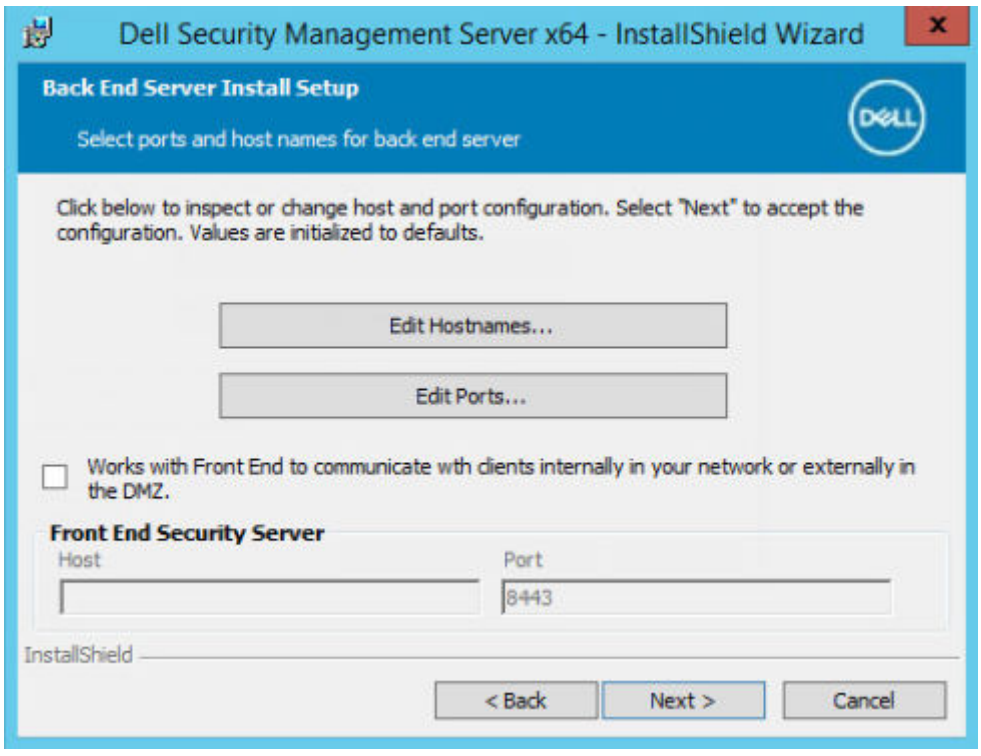
国：国を表す 2 文字の略語

次へ をクリックします。

メモ: デフォルトでは、証明書は 10 年で期限切れになります。



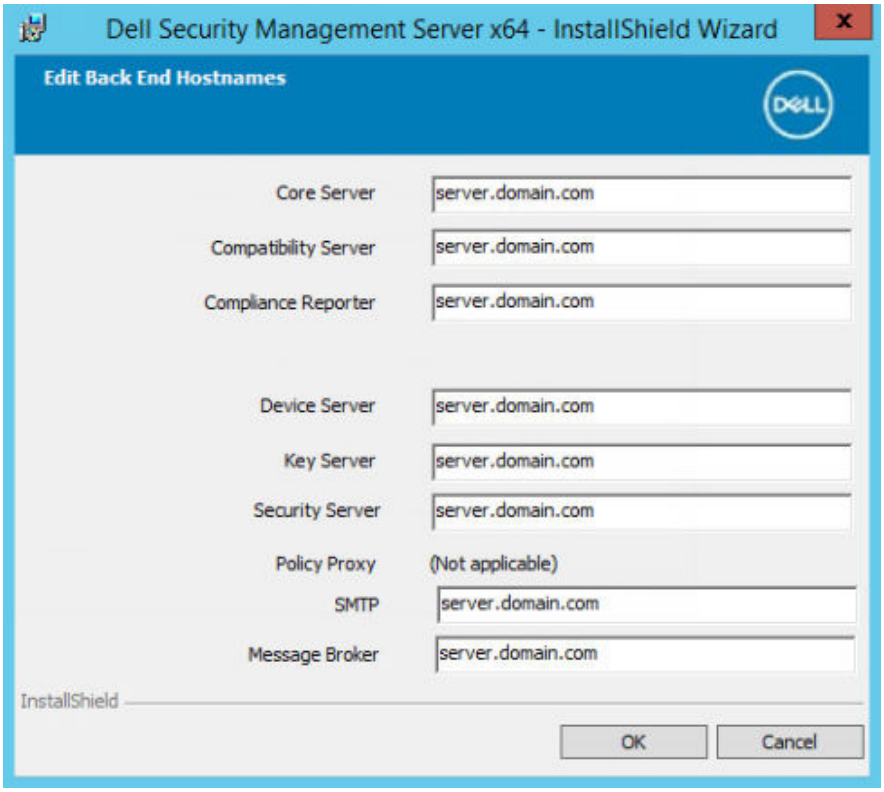
12. *バックエンドサーバインストール設定* ダイアログから、ホスト名とポートを表示または編集できます。
    - デフォルトのホスト名とポートを使用する場合は、*バックエンドサーバインストール設定* ダイアログで、**次へ** をクリックします。
    - フロントエンドサーバを使用している場合は、**ネットワークのクライアントとの内部通信、または DMZ のクライアントとの外部通信のために、フロントエンドと連携** を選択し、フロントエンドのセキュリティサーバのホスト名を入力します（server.domain.com など）。



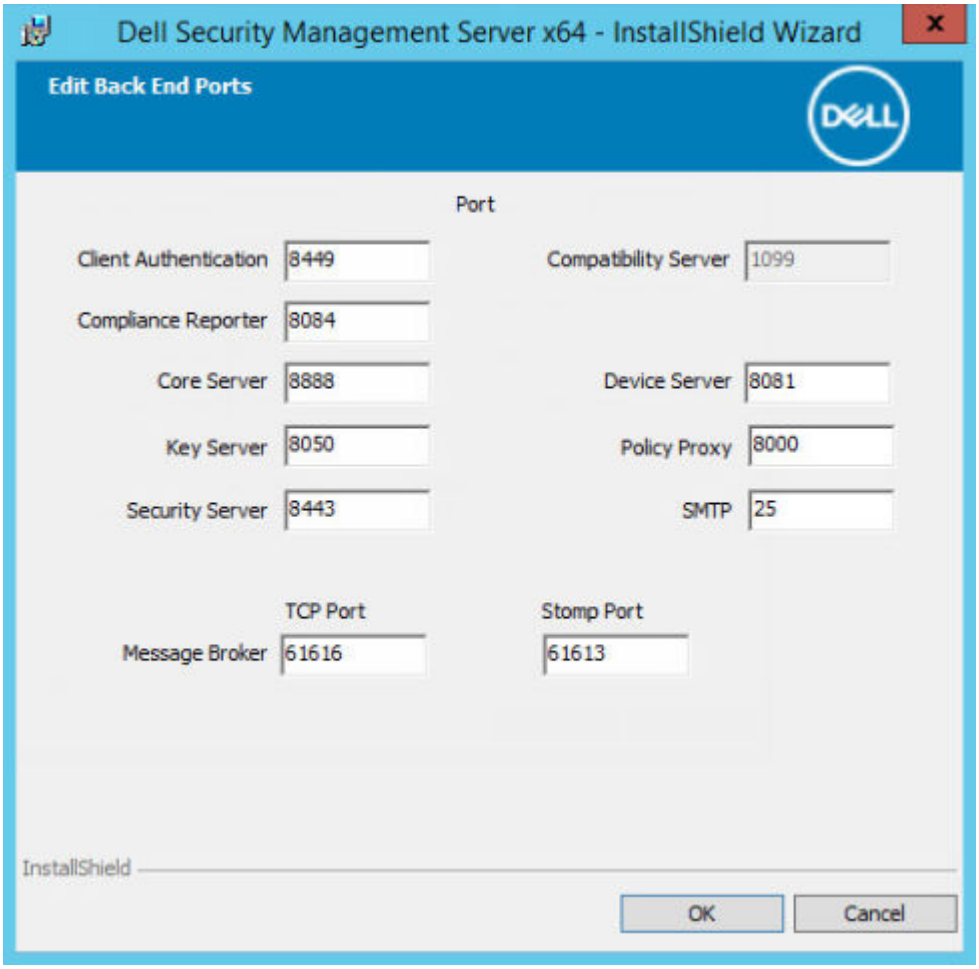
- ホスト名を表示または編集するには、**ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

  メモ: ホスト名に下線（「_」）は使用できません。

終了したら、**OK** をクリックします。

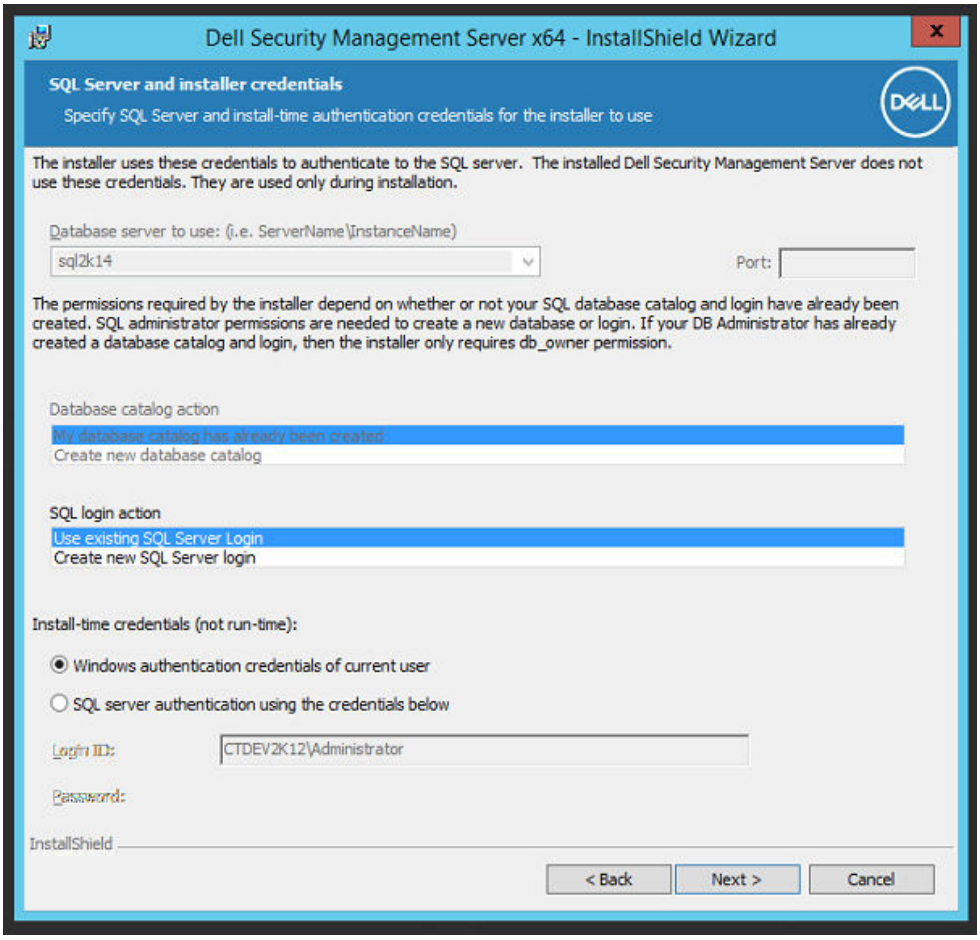


- ポートを表示または編集するには、**ポートの編集** をクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。終了したら、**OK** をクリックします。



13. インストーラが使用するための認証メソッドを指定します。
    a. **参照** をクリックしてデータベースが存在するサーバを選択します。
    b. 認証タイプを選択します。
        - **現在のユーザーの Windows 認証資格情報**

          Windows 認証を選択すると、Windows にログインするときに使用したのと同じ資格情報が認証にも使用されます（*ユーザー名* フィールドと *パスワード* フィールドは編集できない状態になります）。アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。



または

- **以下の資格情報を使った SQL server 認証**

  SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

  インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

c. **参照** をクリックして、既存のデータベースカタログの名前を選択します。
d. **次へ** をクリックします。

14. 既存のデータベースエラー ダイアログが表示された場合は、適切なオプションを選択します。

インストーラがデータベースの問題を検出すると、*既存のデータベースエラー* ダイアログが表示されます。ダイアログ内のオプションは状況により異なります。

- データベーススキーマは以前のバージョンのものとなります。(手順 a を参照してください。)
- このデータベースには、現在インストール中のバージョンに一致するデータベーススキーマがすでに含まれています。(手順 b を参照してください。)

a. データベーススキーマが以前のバージョンのものである場合は、**インストーラを終了して、このインストールを終了する** を選択します。次にデータベースをバックアップする必要があります。

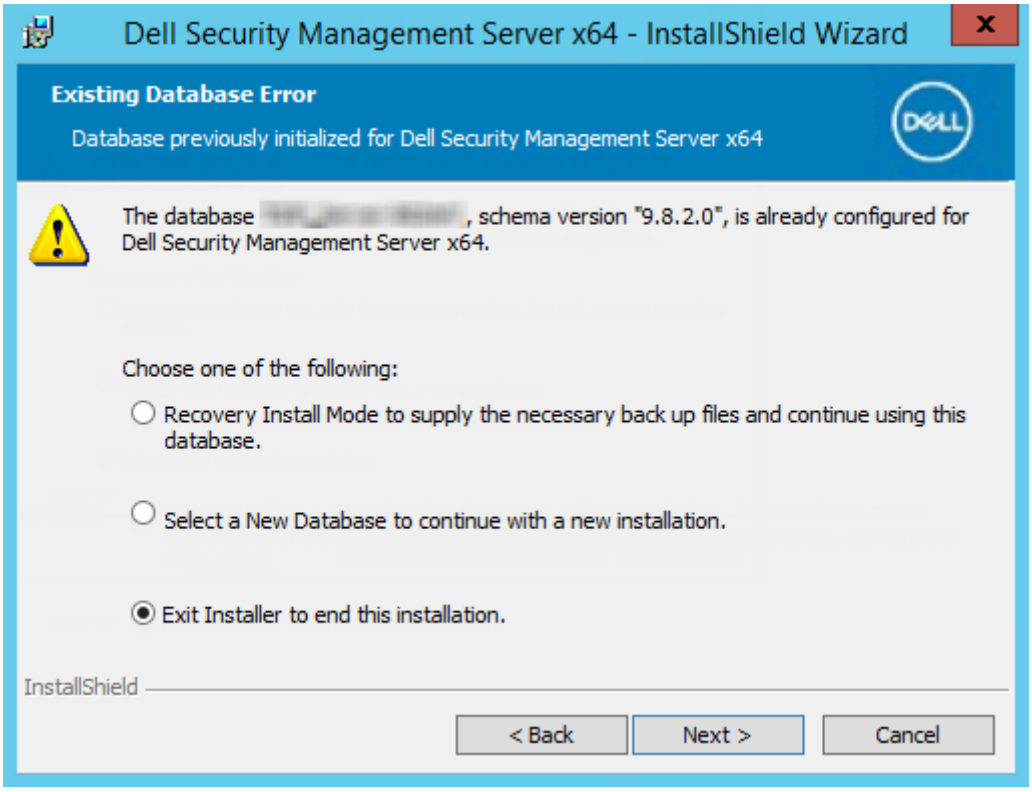
次のオプションは Dell ProSupport からの指示のもとでのみ使用します。

- **このデータベースを現在のスキーマに移行する** オプションは、故障したサーバー実装から良好なデータベースを復元するのに使用します。このオプションでは \Backup フォルダ内の復元ファイルを使用してデータベースに再接続し、その後データベースを現在のスキーマに移行します。正しいバージョンの Security Management Server を再インストールし、最新のインストーラを実行してアップグレードをするという方法を試した後に *のみ*、このオプションを使用するようにしてください。
- **データベースの移行なしで続行する** オプションでは、データベースを完全に設定せずに Security Management Server ファイルをインストールします。後にサーバー設定ツールを使用してデータベースの設定を手動で行う必要があります。また、その後も手動での変更が必要になります。

b. データベーススキーマが現行バージョンのスキーマになっているが、Security Management Server バックエンドに接続されていない場合は、*リカバリ* としてみなされます。このステップで **リカバリインストール** が選択されていないと、このダイアログが表示されます。

- 選択したデータベースのインストールを続行するには、**復元インストールモード** を選択します。
- 異なるデータベースを選ぶには、**新規データベースを選択する** を選択します。
- インストールを終了するには、**インストーラを終了して、このインストールを終了する** を選択します。

c. **次へ** をクリックします。



15. 製品が使用するための認証メソッドを選択します。これは、製品がデータベースおよび Dell サービスで作業するために使用するアカウントです。

- **Windows 認証の使用**

  以下の資格情報を使用した Windows 認証 を選択し、製品が使用するアカウントの資格情報を入力してから、**次へ** をクリックします。

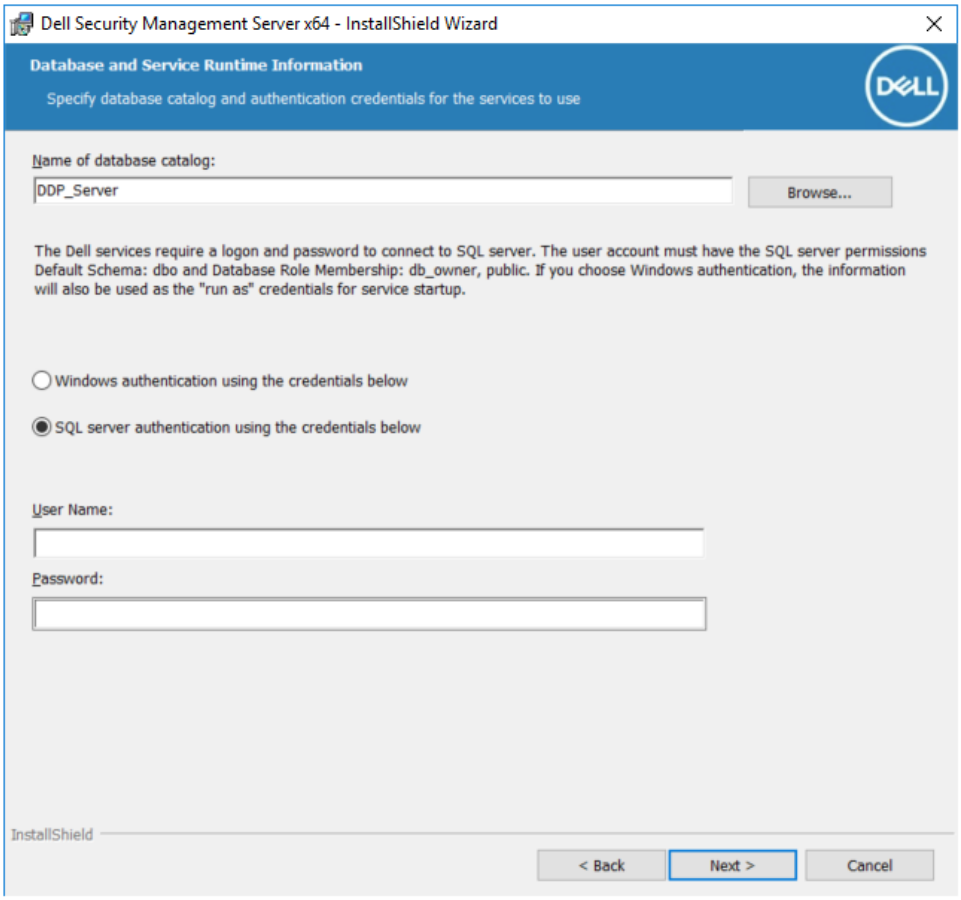
  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ：dbo およびデータベース役割メンバーシップ：db_owner を public にする必要があります。

  または

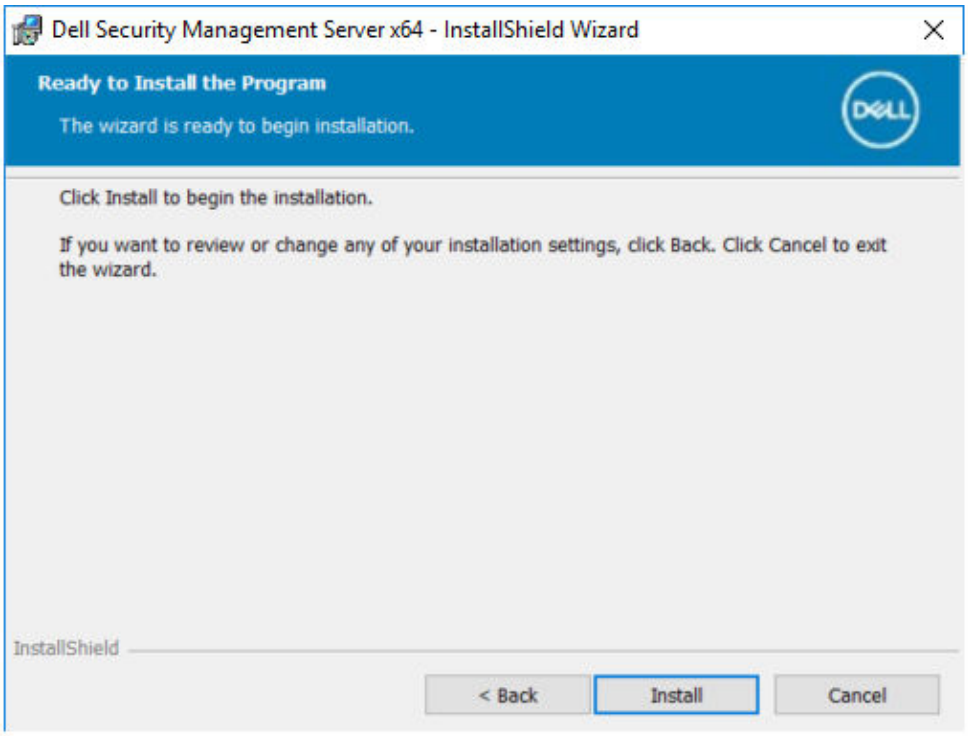
- **SQL Server 認証の使用**

  以下の資格情報を使った SQL Server 認証 を選択し、SQL Server 資格情報を入力してから **次へ** をクリックします。

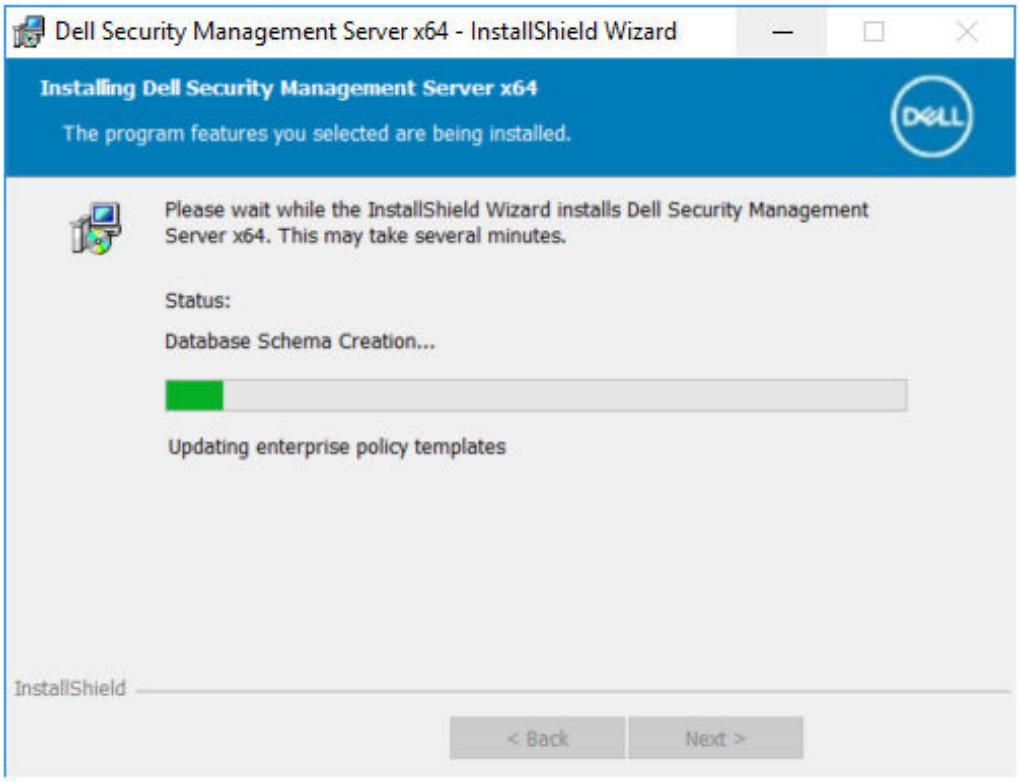
  ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ：dbo およびデータベース役割メンバーシップ：db_owner を public にする必要があります。



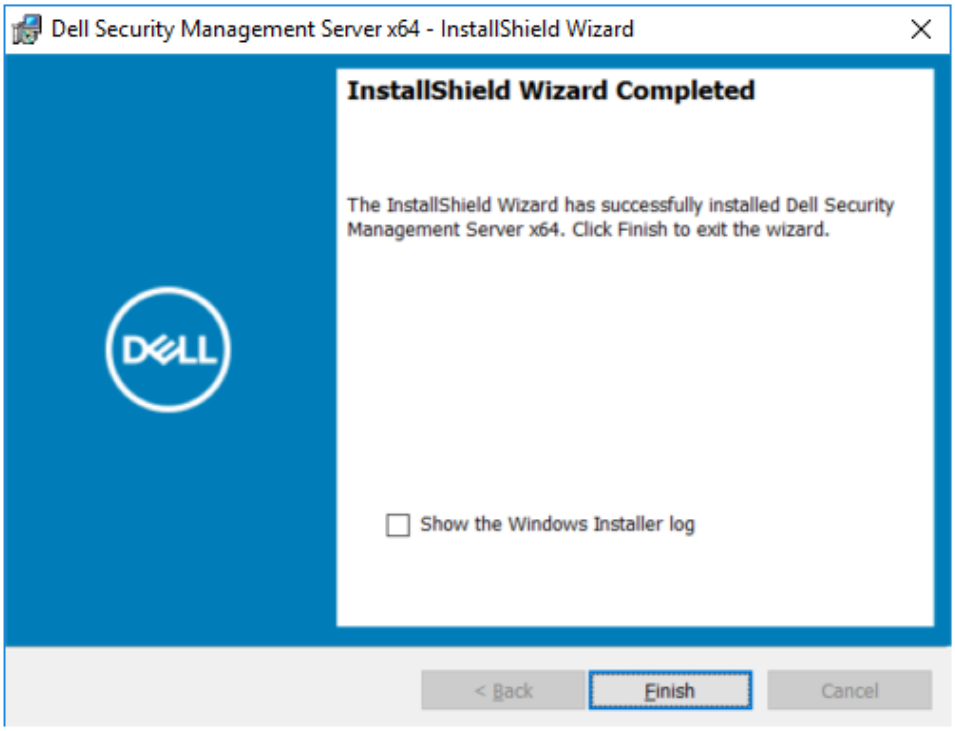
16. *プログラムインストールの準備完了*ダイアログで、**インストール** をクリックします。



ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。



インストールが完了したら、**終了** をクリックします。



これでバックエンドサーバのインストールタスクは完了です。

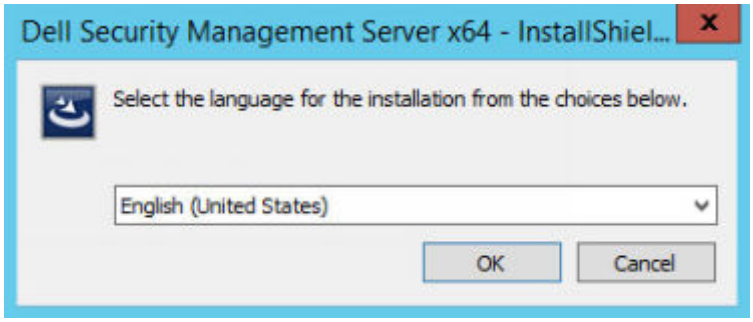
Dell サービスはインストール終了時に再起動されます。サーバを再起動する必要はありません。

フロントエンドサーバのインストール

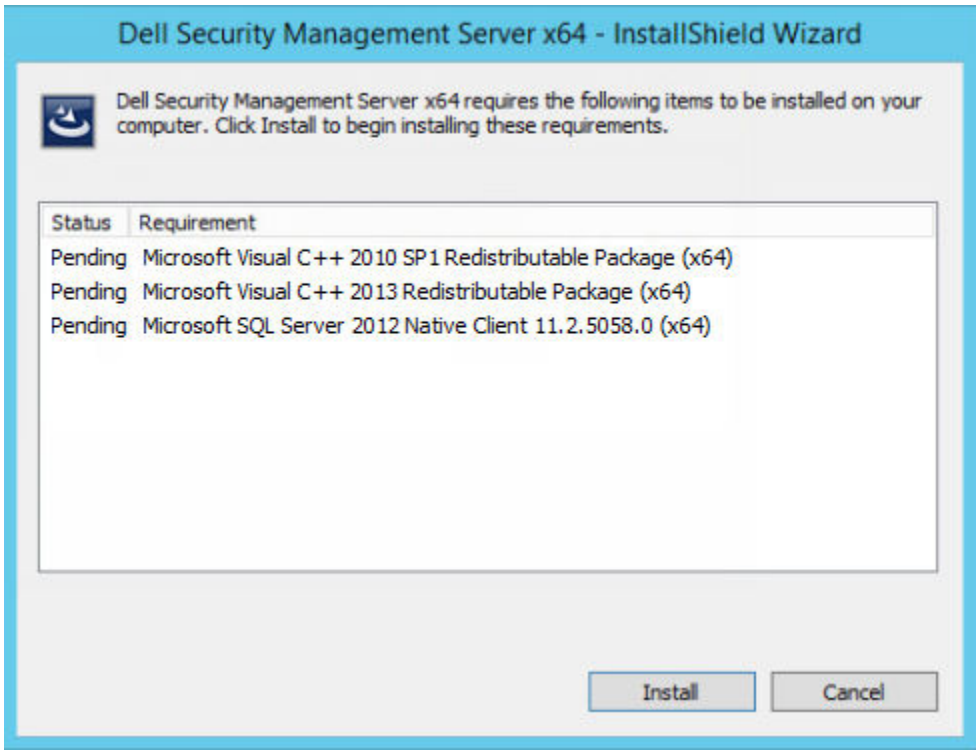
フロントエンドサーバのインストールには、Security Management Server を使用するフロントエンド (DMZ モード) オプションがあります。DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

このインストールを実行するには、DMZ サーバの完全修飾ホスト名が必要です。

1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をインストールするサーバのルートディレクトリに**解凍** (コピー / 貼り付けまたはドラッグ / ドロップではなく) します。***コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. インストール用言語を選択して **OK** をクリックします。

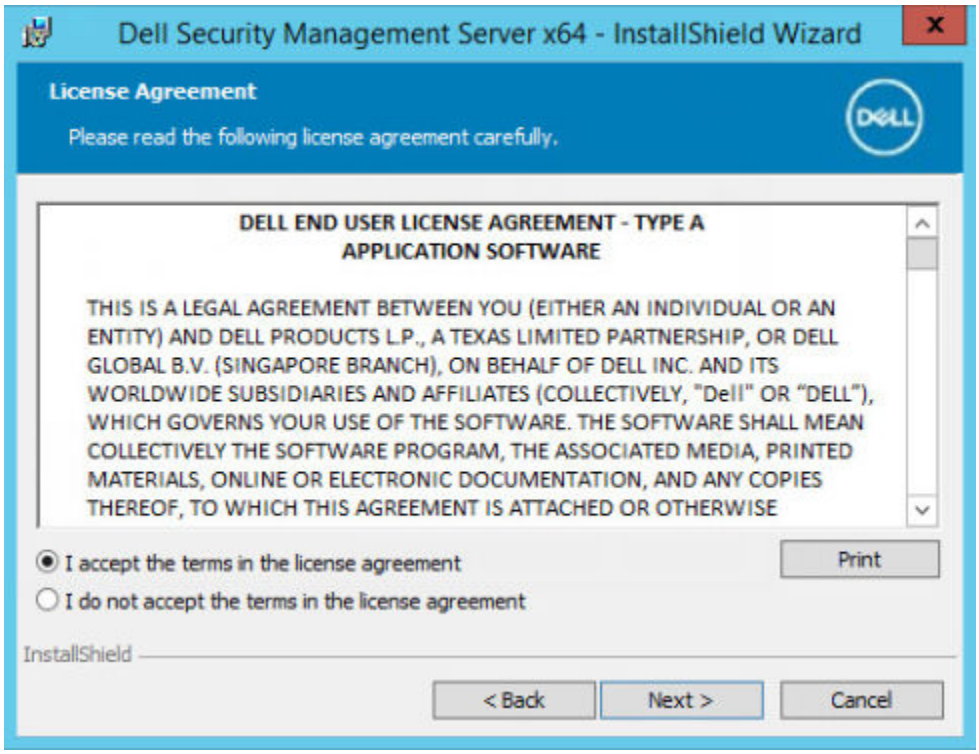


4. 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

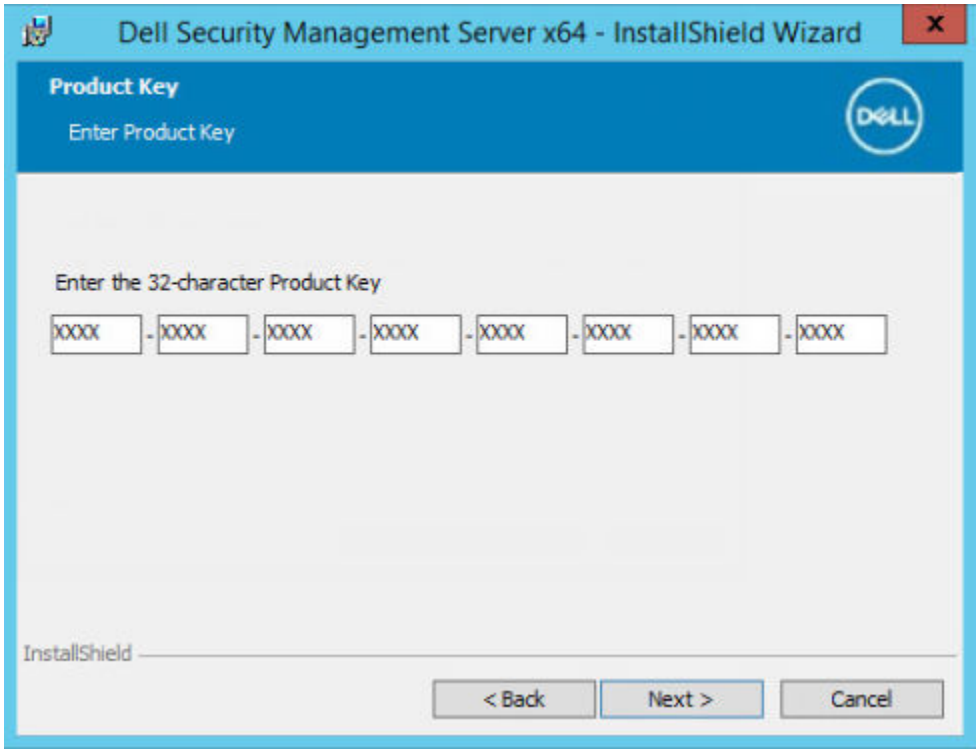


5. ようこそ ダイアログで **次へ** をクリックします。

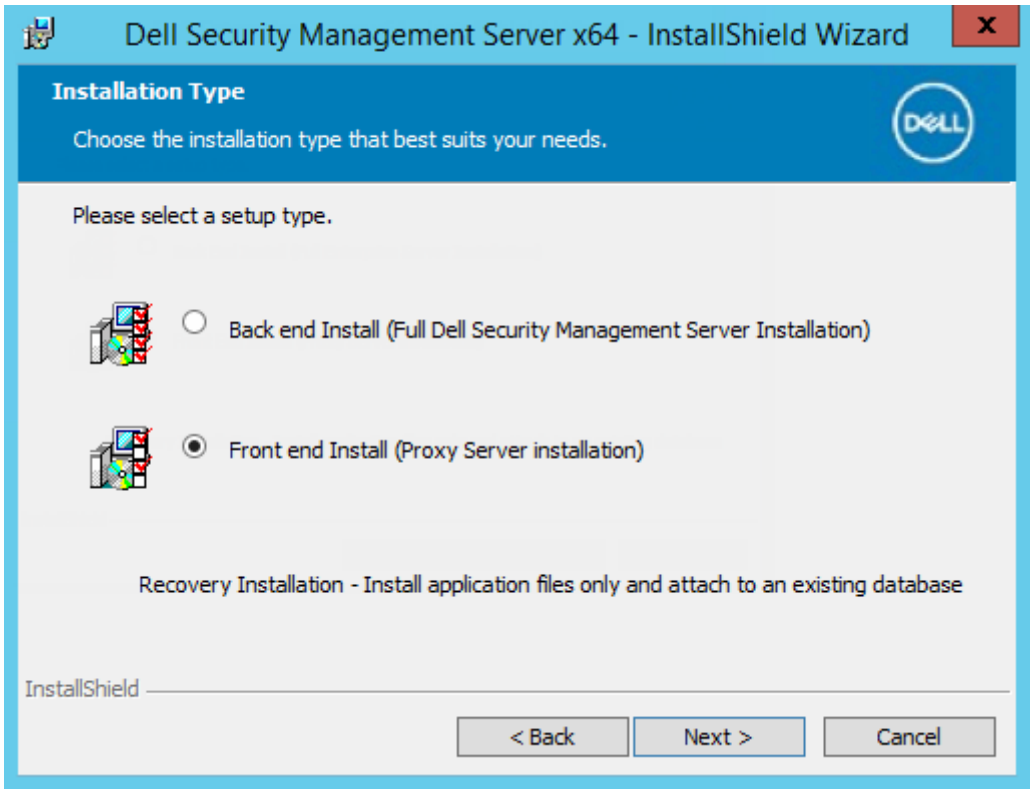
6. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。



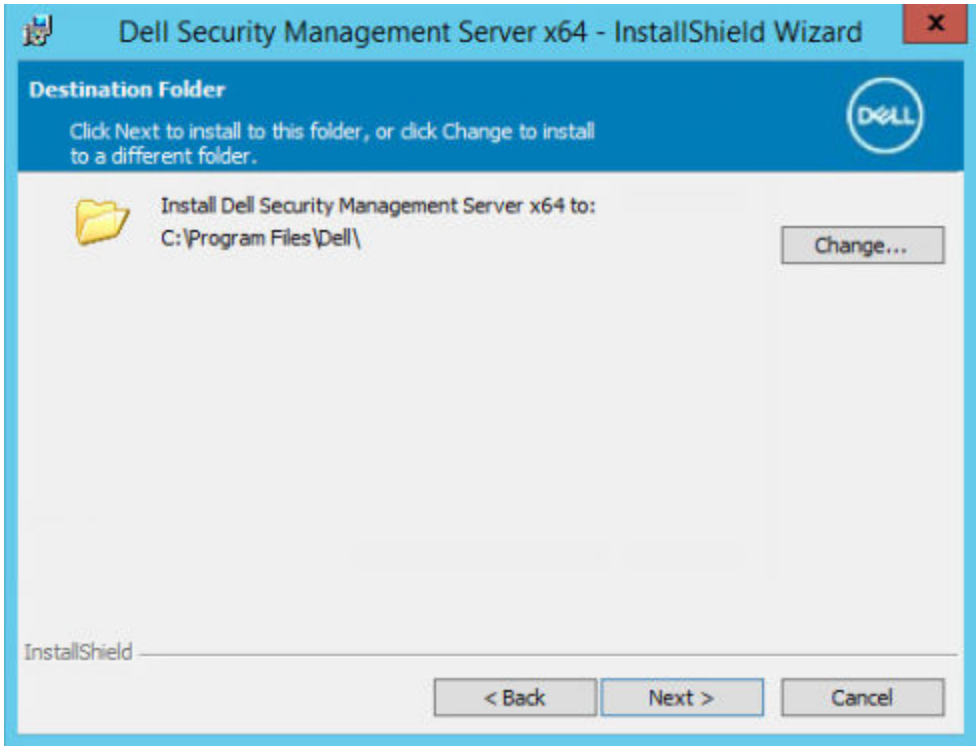
7. 「インストール前の設定」で説明したとおり、`EnterpriseServerInstallKey` `boot.ini` ファイルを `C:¥Windows` にコピーした場合は、**次へ** をクリックします。完了していない場合は、32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーは、`EnterpriseServerInstallKey.ini` ファイルに配置されます。



8. フロントエンドインストール を選択し、**次へ** をクリックします。



9. フロントエンドサーバをデフォルトの `C:\Program Files\Dell` にインストールする場合は、**次へ** をクリックします。それ以外の場所にインストールする場合は、**変更** をクリックして別の場所を選択し、**次へ** をクリックします。

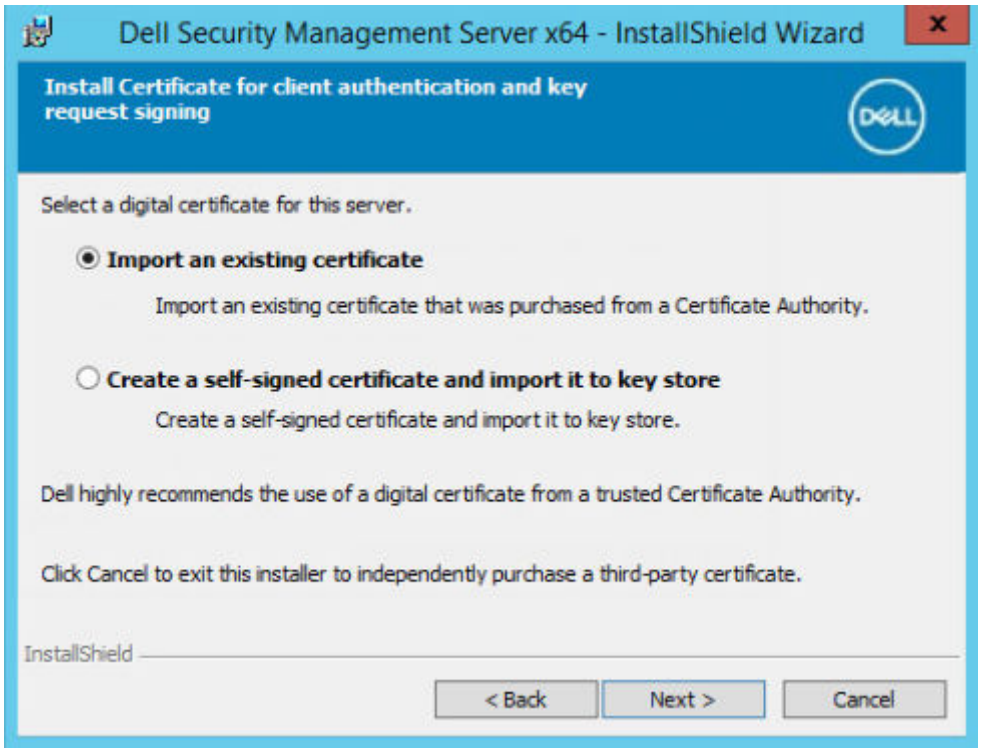


10. 使用するデジタル証明書のタイプを選択することができます。

メモ: デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。

以下のオプション「a」または「b」を選択します。

a. CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。



参照 をクリックして、証明書のパスを入力します。

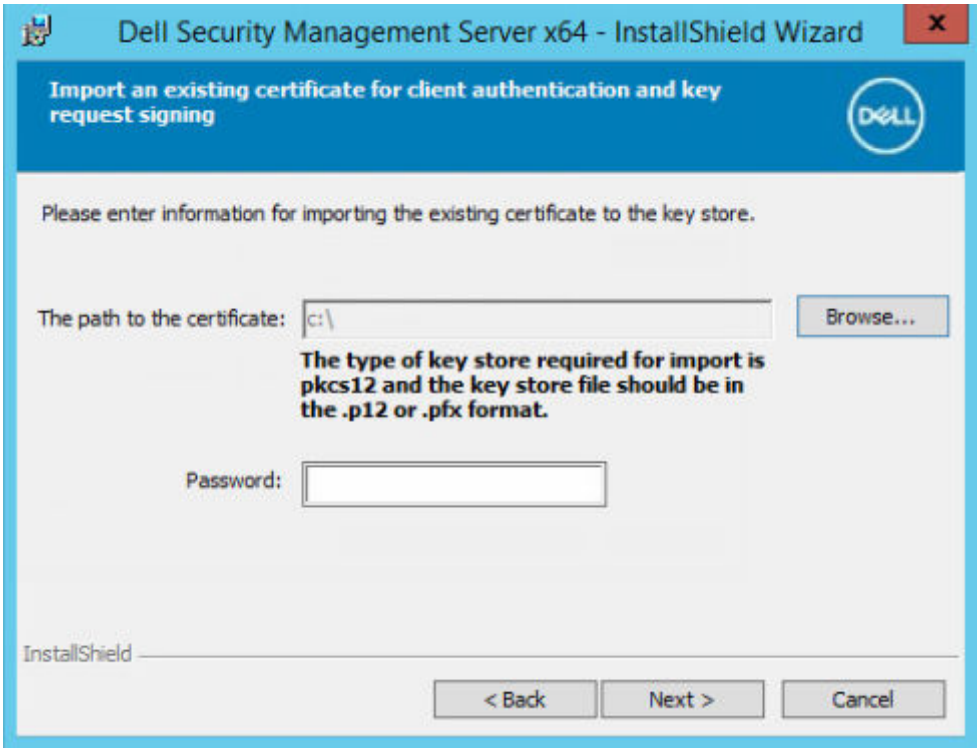
この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

メモ:

この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12 (.PFX)
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする



b. 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。

自己署名証明書の作成 ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

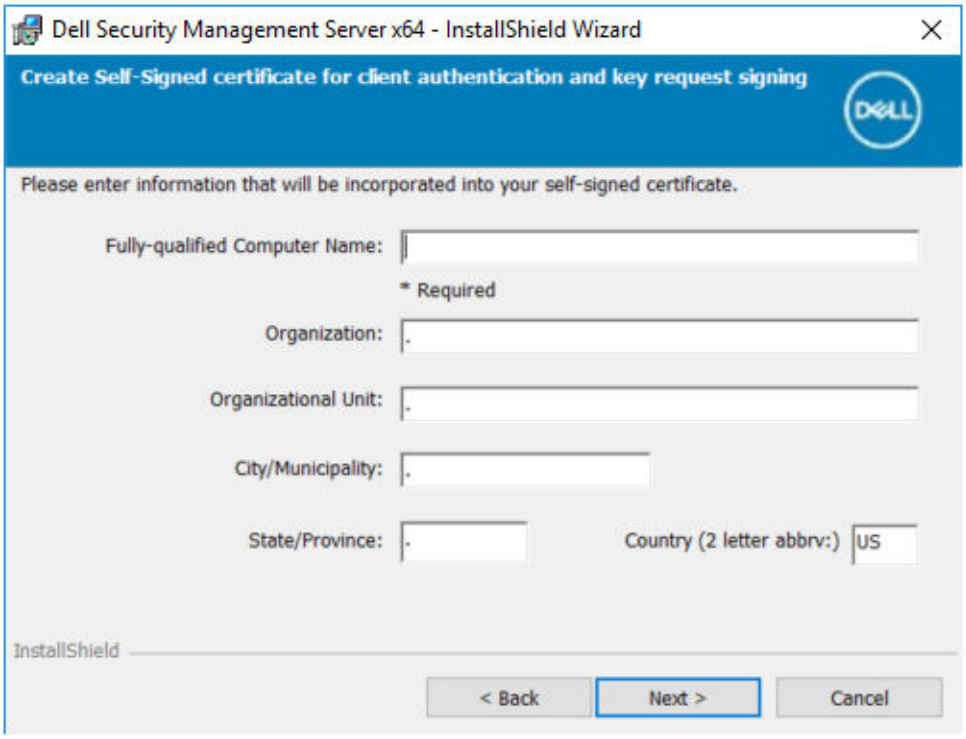
都市

州 (正式名)

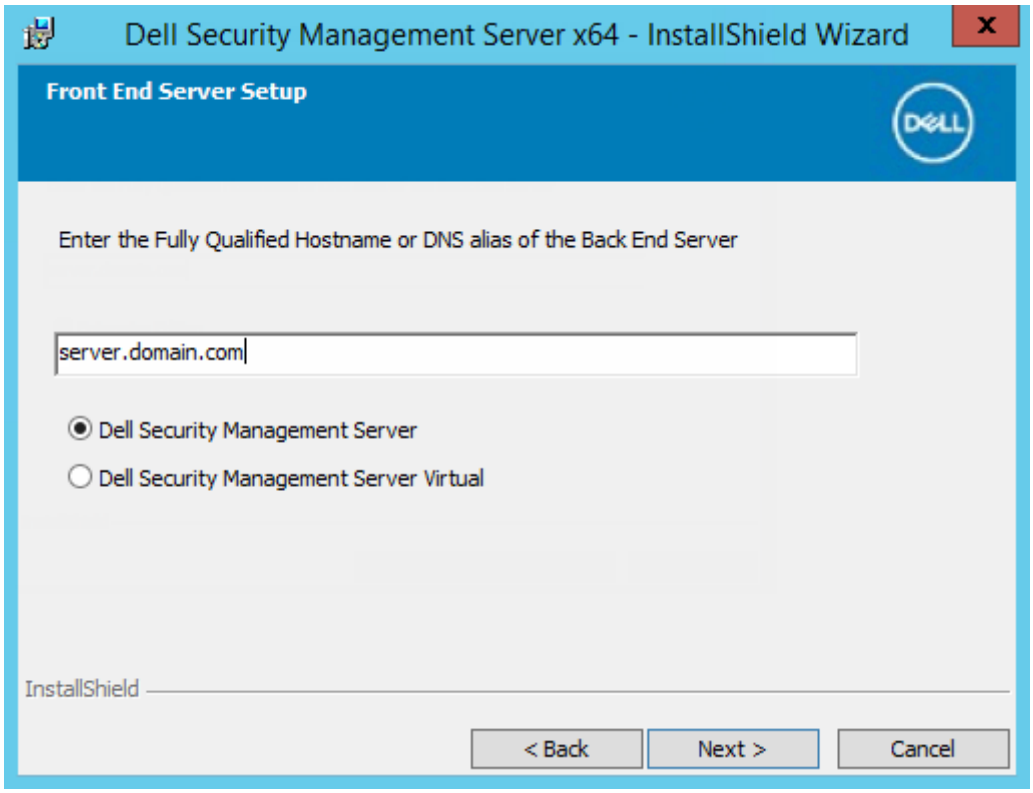
国 : 国を表す 2 文字の略語

次へ をクリックします。

メモ: デフォルトでは、証明書は 10 年で期限切れになります。

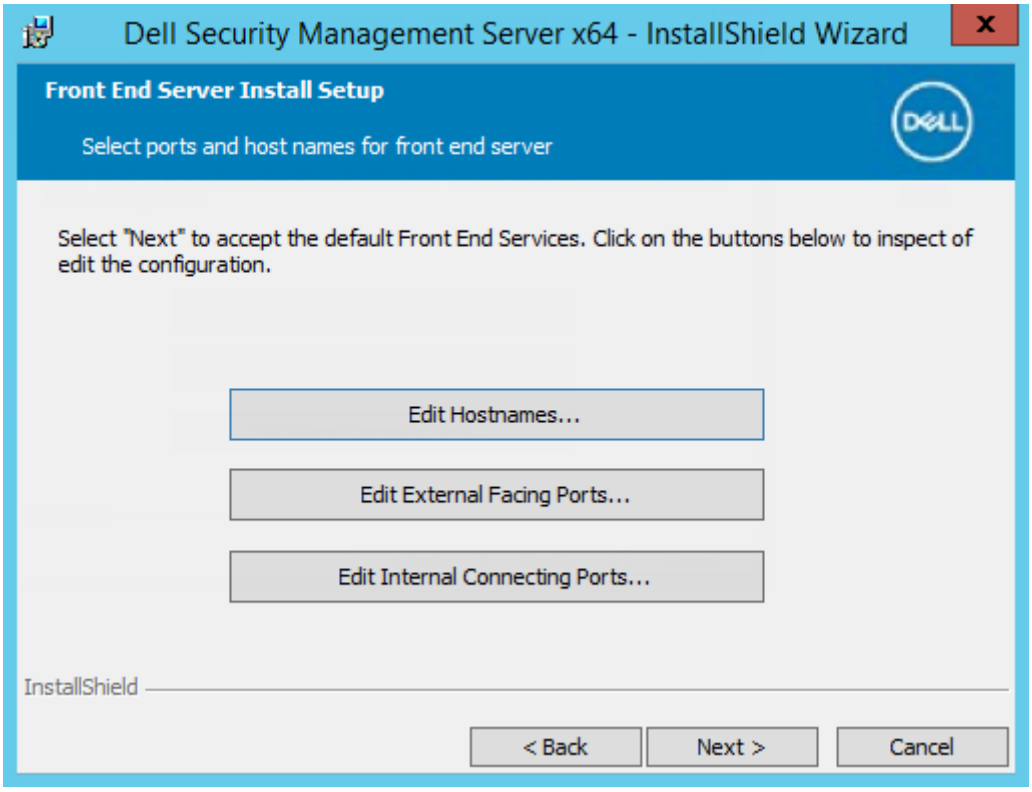


11. *フロントエンドサーバセットアップダイアログで、バックエンドサーバの完全修飾ホスト名または DNS エイリアスを入力し、* **Dell Security Management Server** を選択して、**次へ** をクリックします。



12. *フロントエンドサーバーインストールの設定ダイアログから、ホスト名とポートを表示または編集できます。*

- デフォルトのホスト名とポートを使用する場合は、*フロントエンドサーバーインストールの設定* ダイアログで、**次へ** をクリックします。



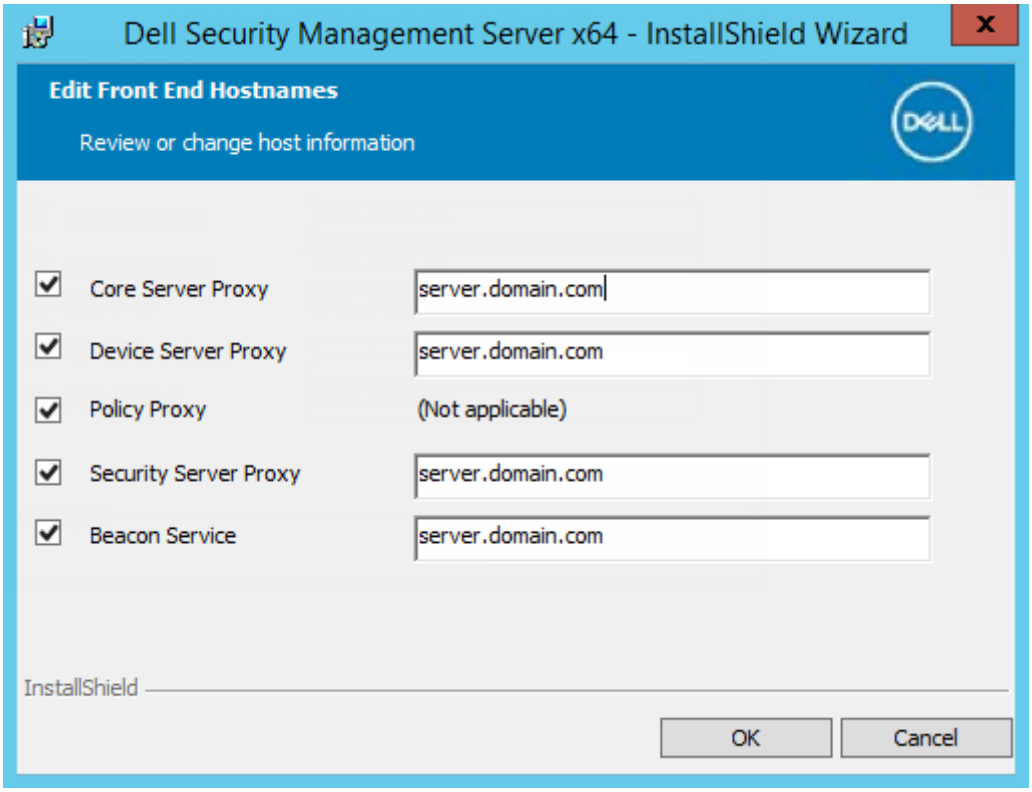
- ホスト名を表示または編集する場合は、*フロントエンドサーバーセットアップ*ダイアログで **ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

  メモ:

  ホスト名に下線(「_」)は使用できません。

  インストール時にプロキシを設定しない場合にのみ、プロキシの選択を外してください。このダイアログで選択しないと、プロキシはインストールされません。

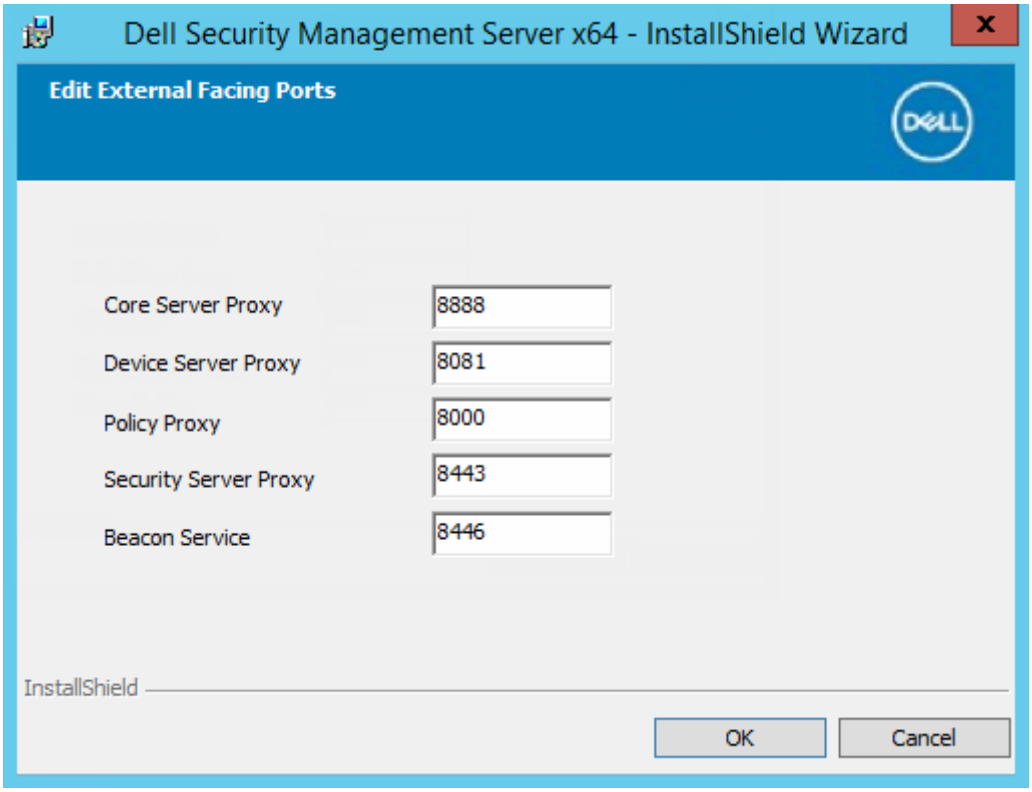
  終了したら、**OK** をクリックします。

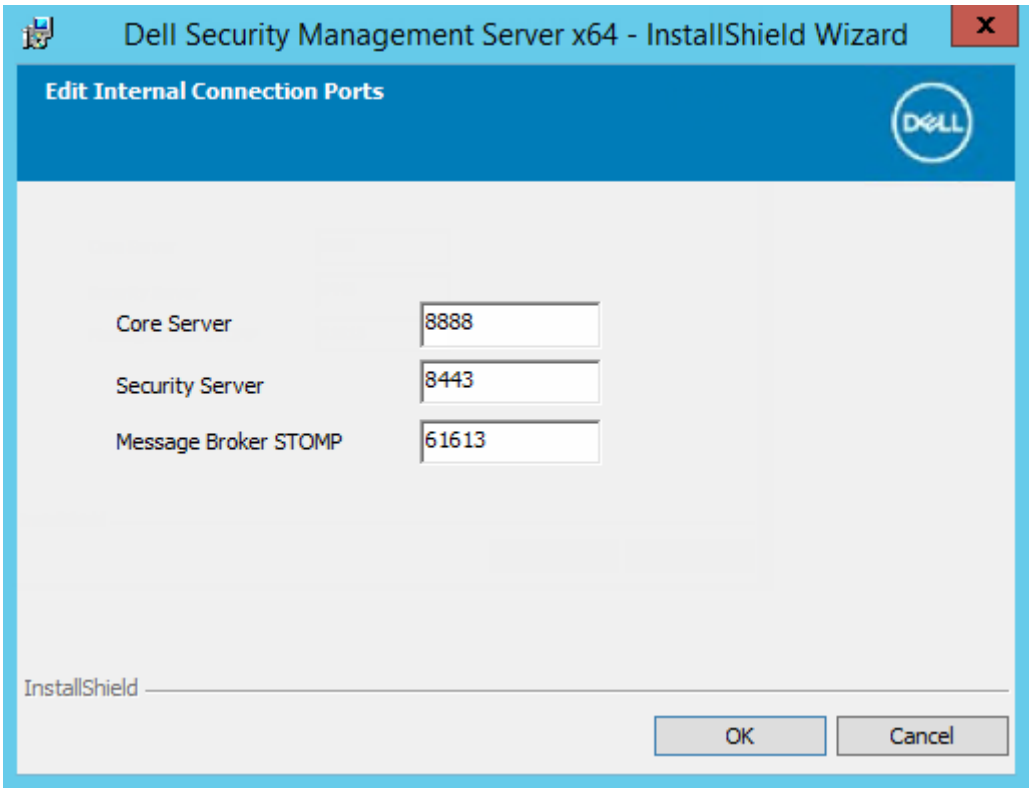


- ポートを表示または編集する場合は、*フロントエンドサーバセットアップダイアログで* **外向きポートの編集**、または **内部接続ポートの編集** のいずれかをクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。

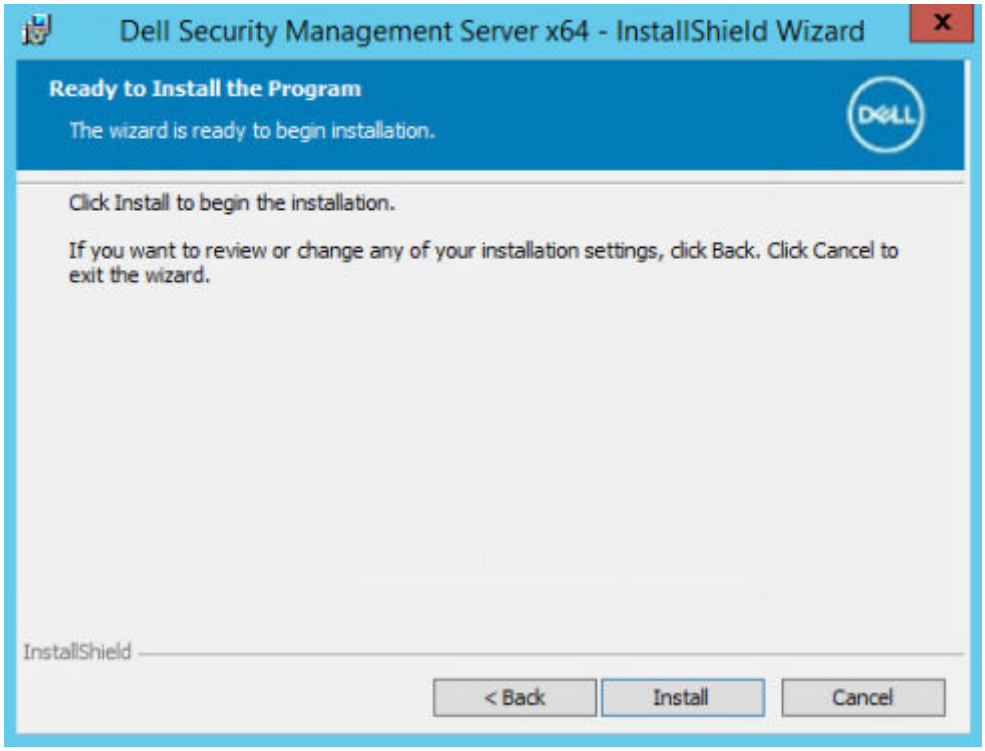
  フロントエンドのホスト名の編集 ダイアログでプロキシの選択を解除すると、そのポートは 外部ポート または 内部ポート ダイアログには表示されません。

  終了したら、**OK** をクリックします。

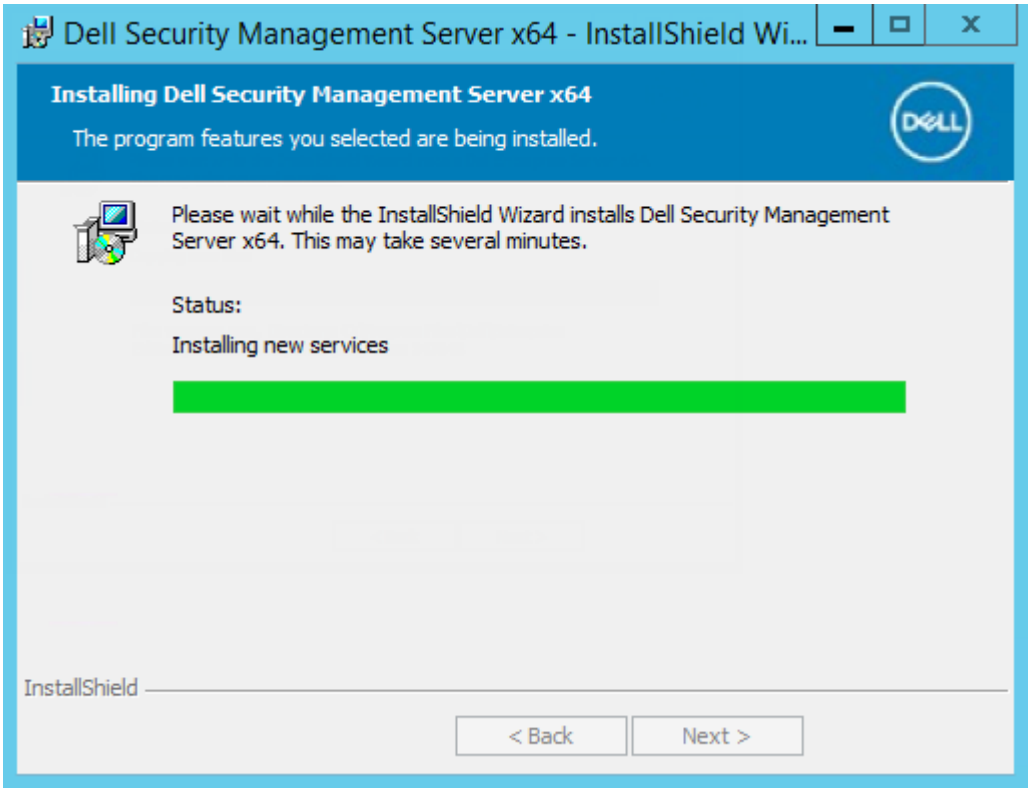




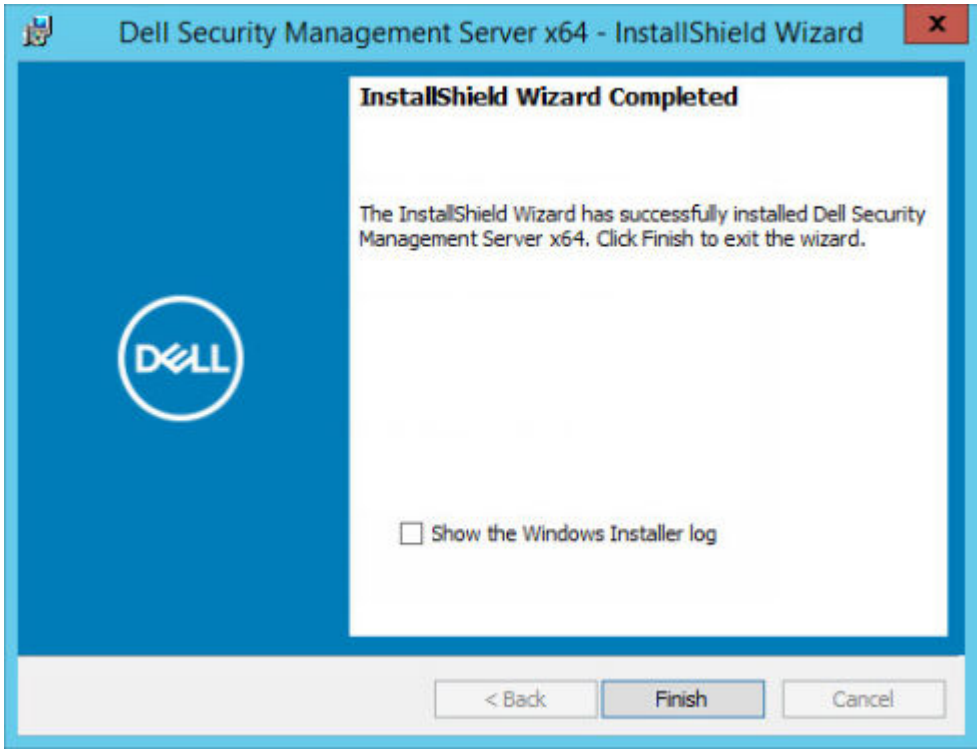
13. *プログラムインストールの準備完了* ダイアログで、**インストール** をクリックします。



ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。



14. インストールが完了したら、**終了** をクリックします。



これでフロントエンドサーバーインストールタスクは完了です。

アップグレード / 移行

Enterprise Server v9.2 以降を Security Management Server v10.x にアップグレードできます。Dell Server のバージョンが v9.2 より前の場合は、まず v9.2 にアップグレードし、その後に新しいバージョンにアップグレードしてください。

アップグレード / 移行を開始する前に

作業を開始する前に、すべての「インストール前の設定」が完了していることを確認します。

Security Management Server のインストールに関連する最新の回避策または既知の問題については、『*Security Management Server テクニカルアドバイザリー*』をお読みください。

インストールの実行元のユーザーアカウントには、SQL データベース用のデータベース所有者権限が必要です。アクセス権限の有無またはデータベースへのアクセス可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

デルでは、データベースのベストプラクティスをデルサーバのデータベースに使用し、組織の災害復旧計画にデルソフトウェアを含めることを推奨しています。

DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

本番稼働の場合、デルでは、専用サーバーに SQL Server をインストールすることを推奨します。

ポリシーの機能を十分に活用するため、Security Management Server およびクライアントの両方を最新バージョンにアップデートすることをお勧めします。

Security Management Server v10.x は、以下をサポートします。

- Encryption Enterprise：
  - Windows クライアント v8.x/v10.x
  - Mac クライアント v8.x/v10.x
  - SED 管理 v8.x/v10.x
  - BitLocker Manager v8.x/10.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprise v1.x/v2.x

- Security Management Server v9.2 以降からのアップグレード / 移行 (v9.2 より前の Security Management Server から移行する際は、Dell ProSupport に問い合わせてサポートを受けてください。)

新しいポリシーが導入されたバージョンに Security Management Server をアップグレード / 移行する場合は、更新されたポリシーをアップグレード / 移行後にコミットして、デフォルト値ではなく、独自のポリシー設定が新しいポリシーに実装されるようにしてください。

一般的に推奨されるアップグレードパスは Security Management Server およびそのコンポーネントをアップグレード / 移行し、次に Client をインストール / アップグレードすることです。

ポリシーの変更の適用

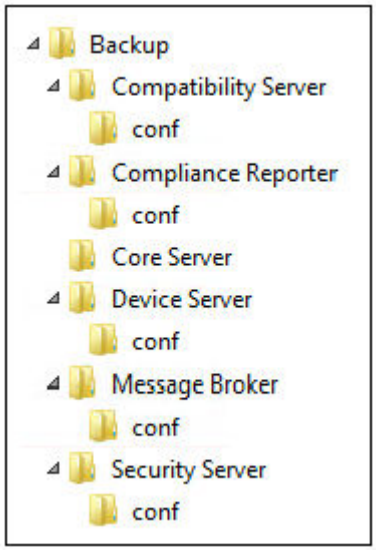
1. 管理コンソールに Dell 管理者としてログインします。
2. 左側のメニューで、**管理** > **コミット** の順にクリックします。
3. *コメント* に変更内容を入力します。
4. **ポリシーのコミット** をクリックします。
5. コミットが完了したら、管理コンソールからログオフします。

   すべての Dell サービスが実行されていることを確認します。
6. Windows の *スタート* メニューから、**スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。 *サービス* が開いたら、各 Dell サービスに移動し、必要に応じて、**サービスの開始** をクリックします。

   既存のインストールのバックアップ
7. 既存のすべてのインストールのバックアップを別の場所に作成します。バックアップには、SQL データベース、secretKeyStore および設定ファイルを含めるようにしてください。アップグレード / 移行の完了後に、既存のインストールのファイルがいくつか必要になります。

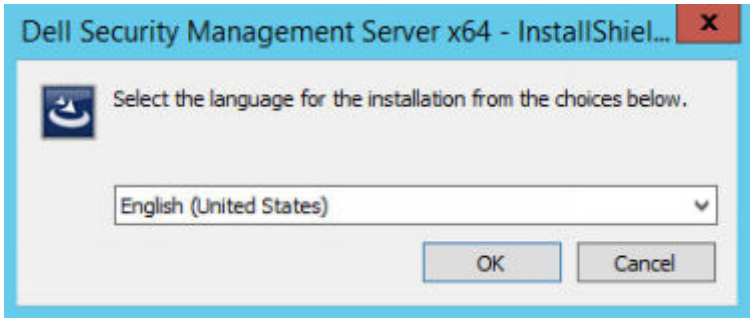
   メモ:

   インストール中、インストーラによって作成されたフォルダの構造 (例は下記参照) は変更しないでください。



バックエンドサーバーのアップグレード / 移行

1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をインストールするサーバのルートディレクトリに**解凍** (コピー / 貼り付けまたはドラッグ / ドロップではなく) します。 ***コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. インストール用言語を選択して **OK** をクリックします。

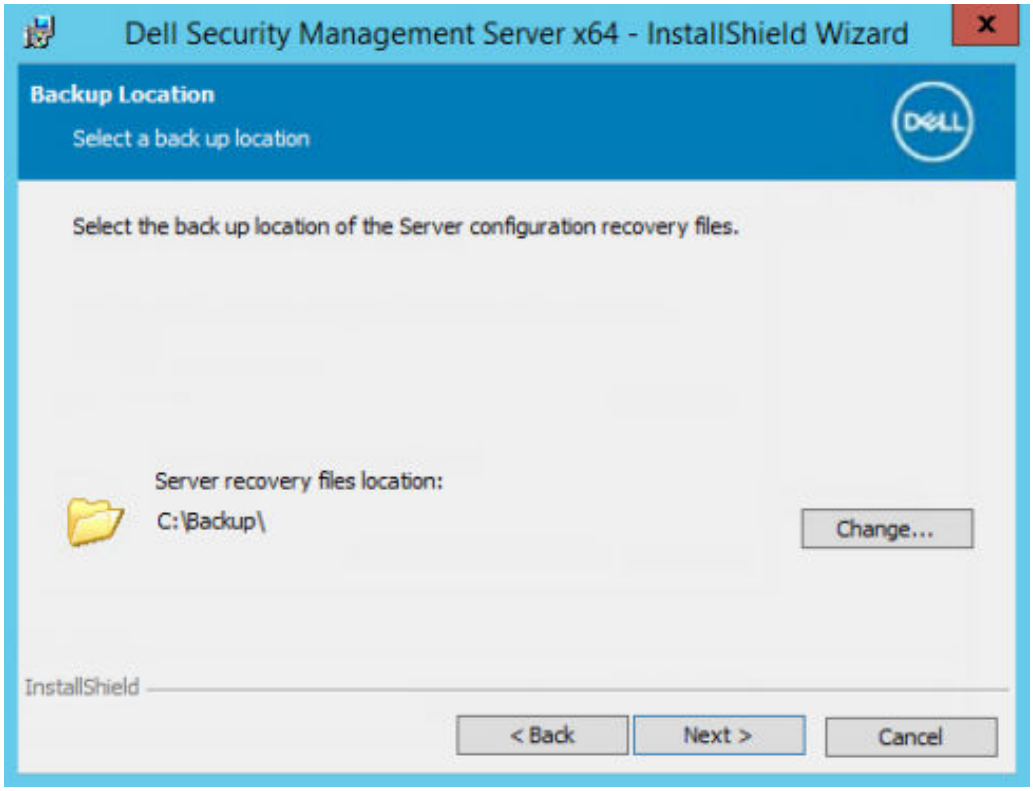


4. ようこそダイアログで **次へ** をクリックします。

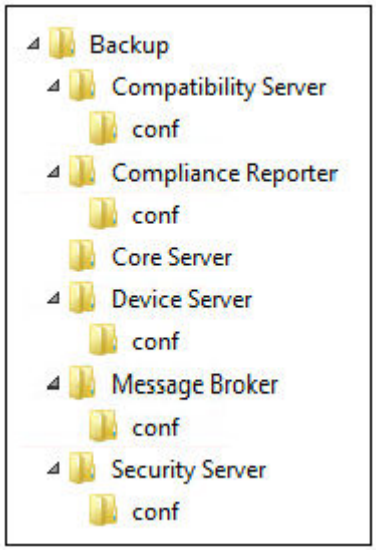
5. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

6. バックアップ設定ファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。

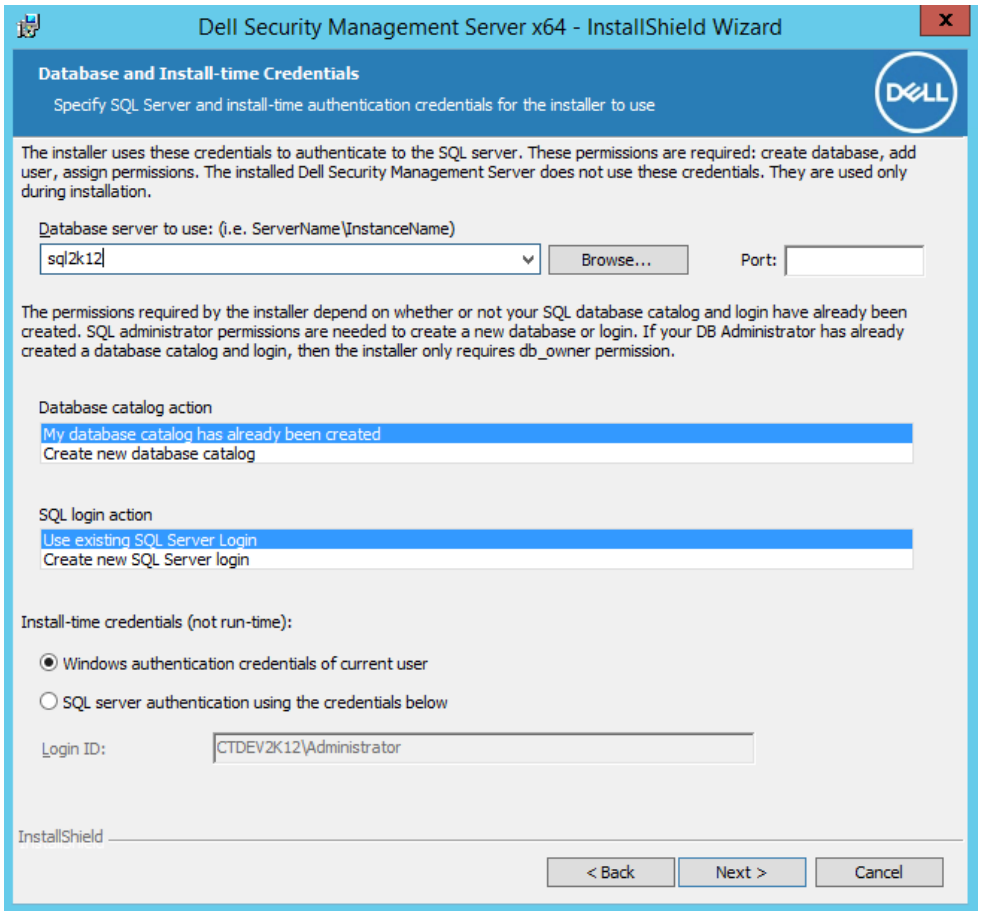
   デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。



インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



7. インストーラが的確に既存のデータベースを検出すると、ダイアログは自動入力されます。



既存のデータベースに接続するには、使用する認証メソッドを指定します。製品がインストールされた後は、ここで指定された資格情報を使用しません。

a. データベースの認証タイプを選択します。

- **現在のユーザーの Windows 認証資格情報**

  Windows 認証を選択すると、Windows へのログイン時に使用されたのと同じ資格情報が認証に使用されます（*ユーザー名* フィールドと *パスワード* フィールドは編集できなくなります）。

  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ：dbo およびデータベース役割メンバーシップ：db_owner を public にする必要があります。

または

- **以下の資格情報を使った SQL server 認証**

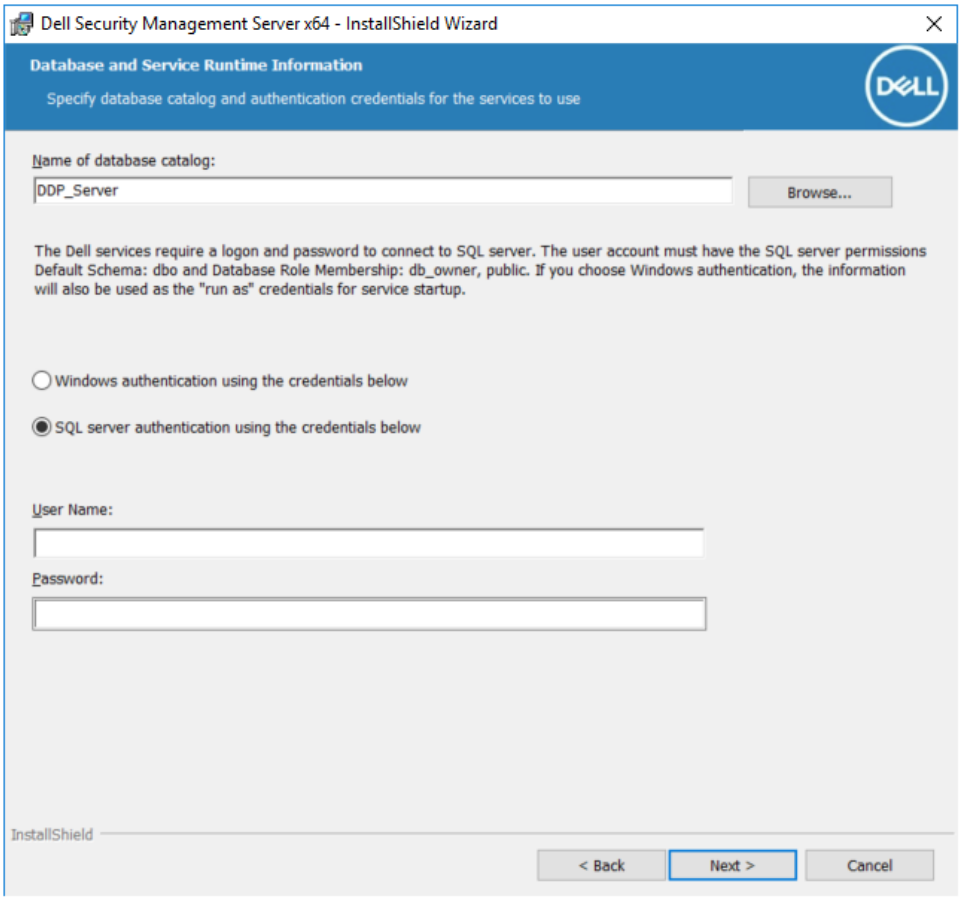
  SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

  インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

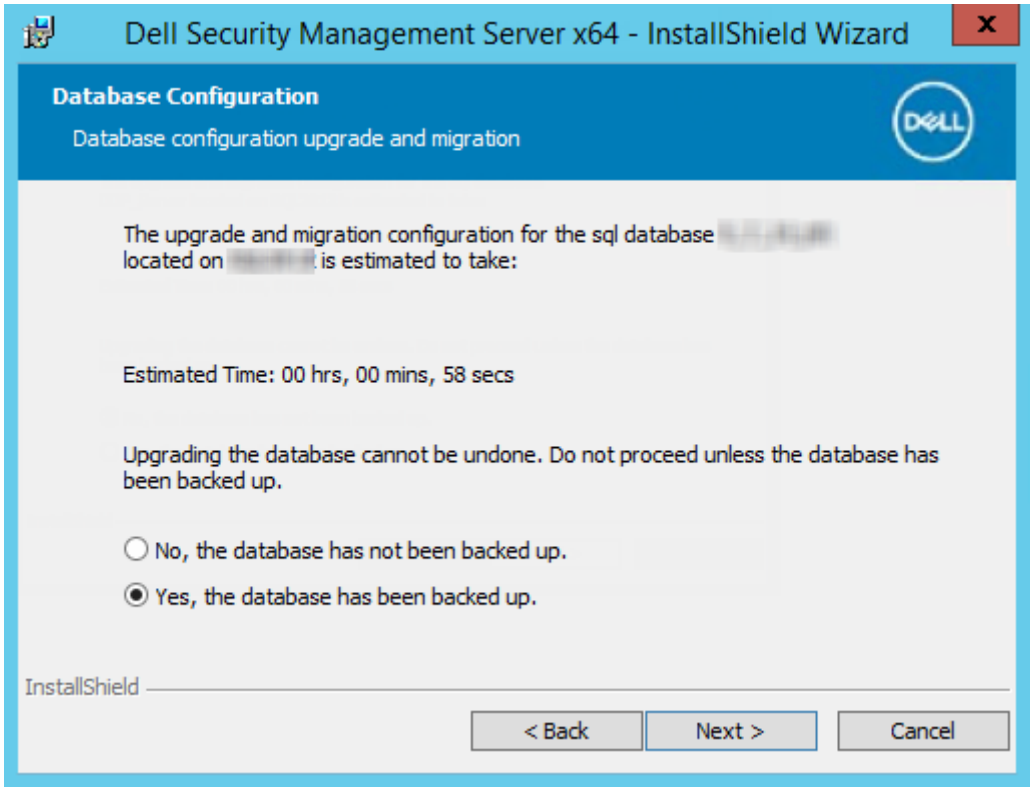
b. **次へ** をクリックします。

8. サービスランタイムアカウント情報が事前に入力されていない場合は、インストール後に製品が使用する認証メソッドを指定します。
   a. 認証タイプを選択します。
   b. SQL Server へアクセスするために Dell サービスが使用する、ドメインサービスのアカウントのユーザー名およびパスワードを入力して、**次へ** をクリックします。

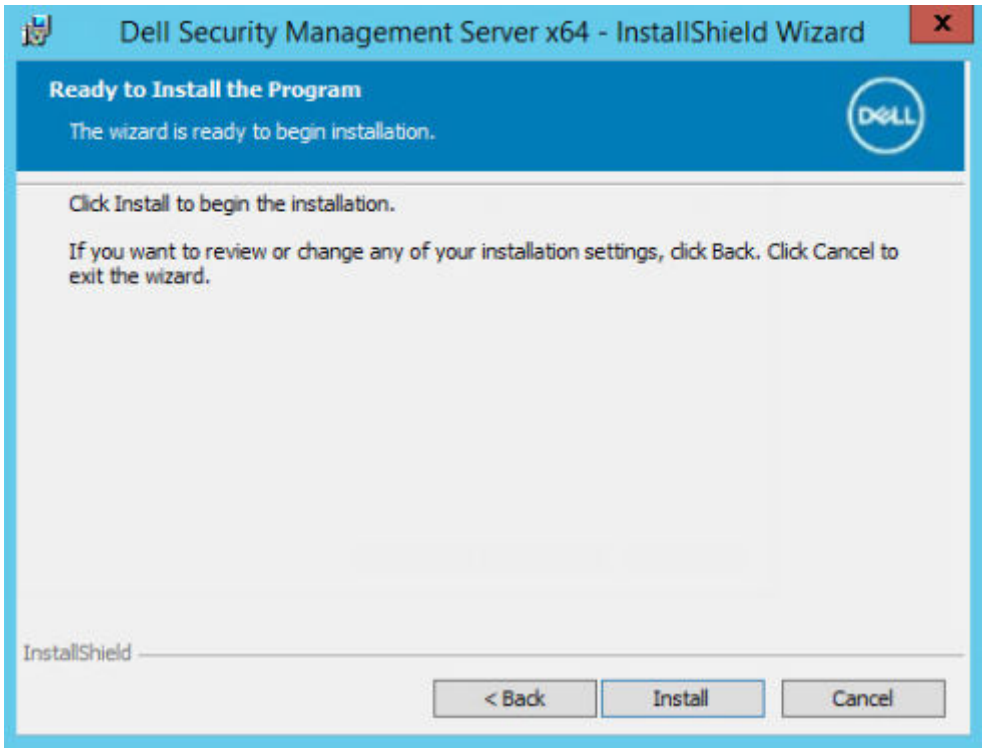
      ユーザーアカウントは DOMAIN\\Username フォーマットであり、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ： db_owner を「public」にする必要があります。



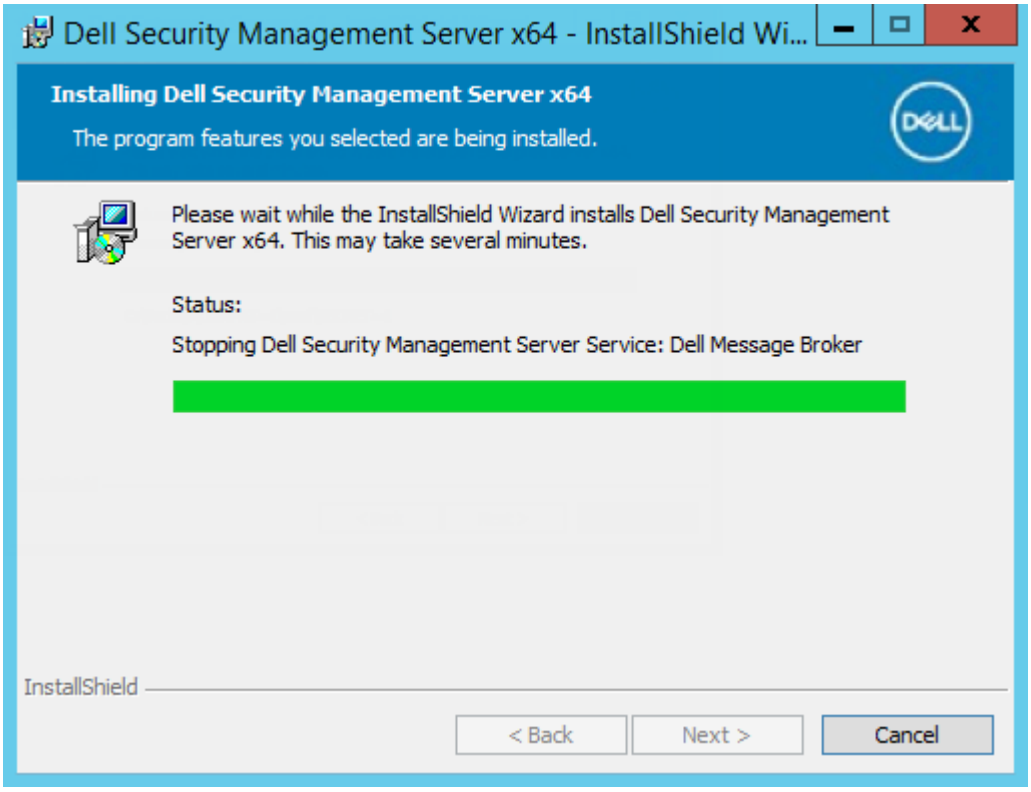
9. データベースのバックアップを作成していない場合は、インストールを続行する前にバックアップを作成する***必要があります***。***データベースのアップグレードを元に戻すことはできません。*** データベースがバックアップされた後にのみ、**はい。データベースはバックアップされています。** を選択して、**次へ** をクリックします。



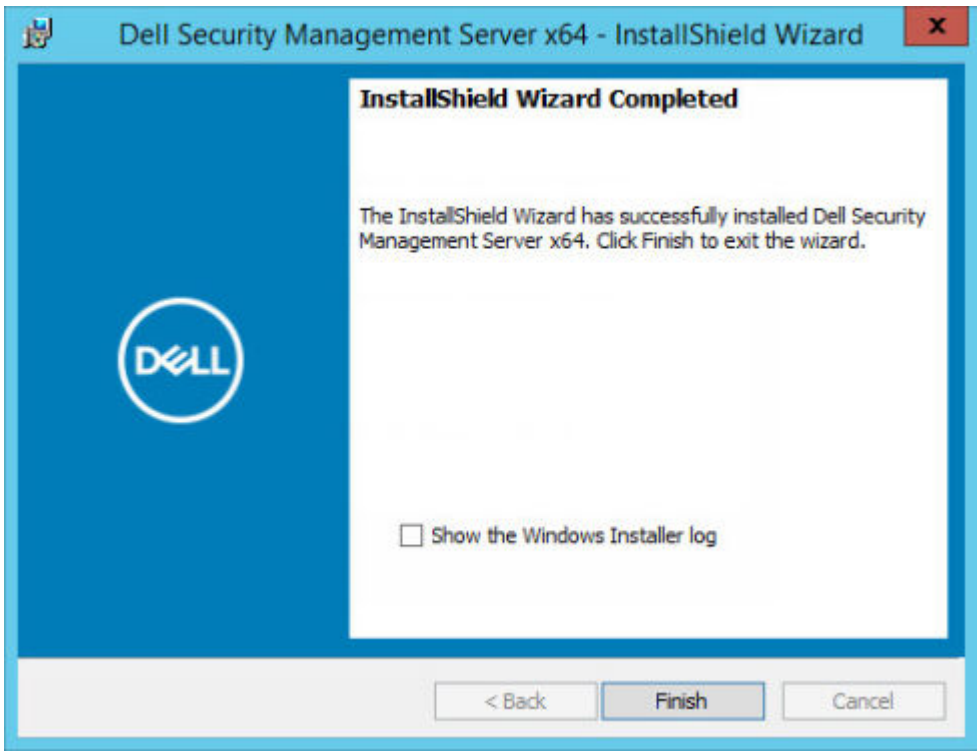
10. **インストール** をクリックしてインストールを開始します。



ステータスは、アップグレードプロセスの全体を通して進捗状況ダイアログに表示されます。



11. インストールが完了したら、**終了** をクリックします。



Dell サービスは移行終了時に再起動されます。Dell Server を再起動する必要はありません。

インストーラは手順 12 ~ 13 を自動的に実行します。これらの値に注目して変更が適切に行われたかを確認することが重要です。

12. バックアップされたインストールで、<Compatibility Server install dir>\conf\secretKeyStore を新しいインストールにコピー / 貼り付けします。

<Compatibility Server install dir>\conf\secretKeyStore に貼り付けます。

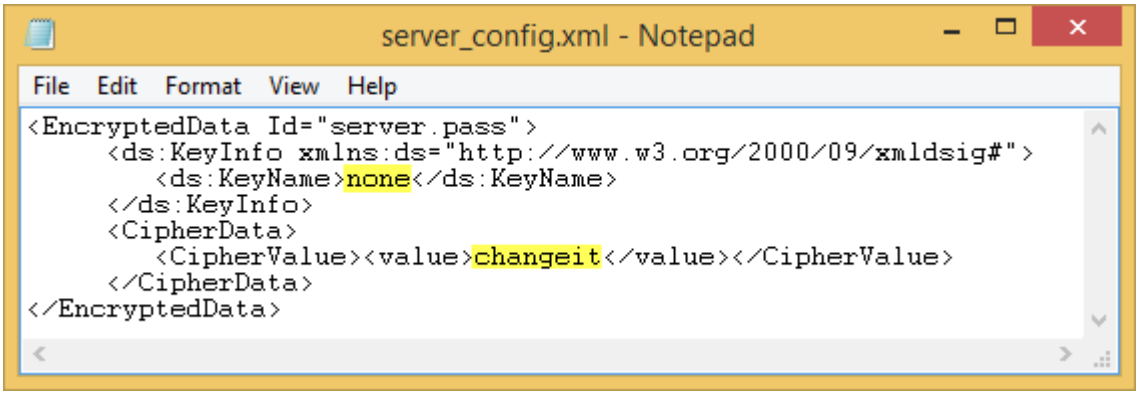
13. 新しいインストールで、<Compatibility Server install dir>\conf\server_config.xml を開き、次のように、**server.pass** 値を、バックアップした <Compatibility Server install dir>\conf\server_config.xml の値に置き換えます。

server.pass に関する手順：

パスワードがわかっている場合は、server_config.xml ファイルの例を参照し、次のように変更します。

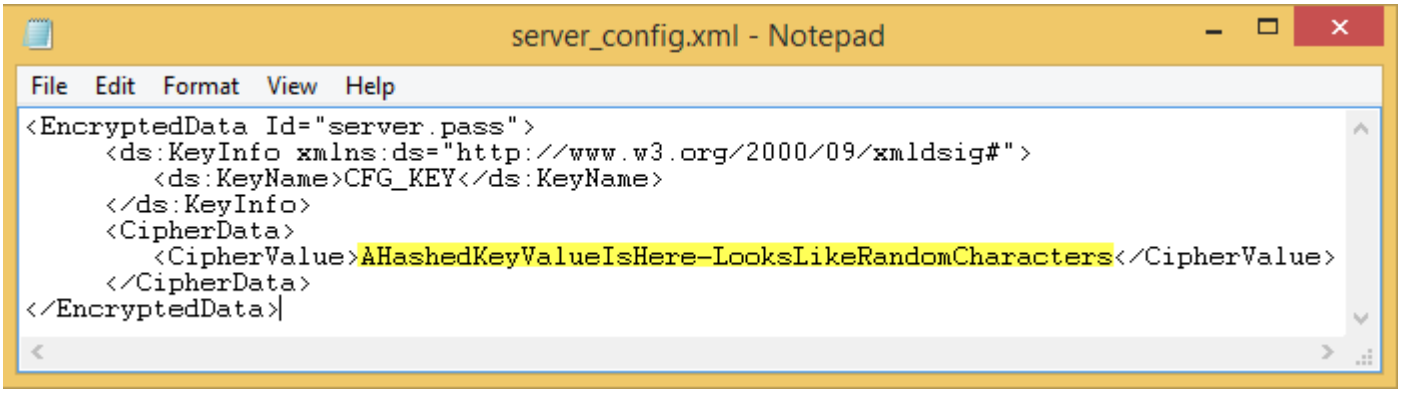
- *KeyName*（**CFG_KEY** 値）を編集して **none** にします。
- プレインテキストパスワードを入力し、*<value> </value>* で囲みます。この例では **<value>changeit</value>** となっています。
- Security Management Server が起動すると、このプレインテキストパスワードはハッシュされ、ハッシュされた値がプレインテキストに置き換えられます。

既知のパスワード



パスワードがわからない場合は、バックアップされた <Compatibility Server install dir>\conf\server_config.xml ファイルから図 4-2 にあるセクションに似たセクションを新しい *server_config.xml* ファイルの対応するセクションにカットアンドペーストします。

不明なパスワード



ファイルを保存して閉じます。

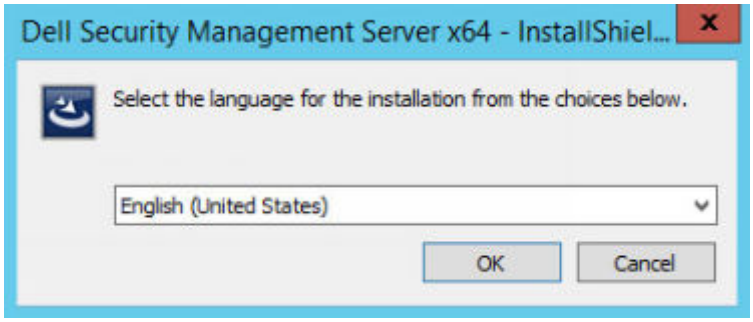
メモ:

上記以外の場合に、server_config.xml 内の server.pass 値を編集して Security Management Server のパスワードを変更しないでください。この値を変更すると、データベースにアクセスできなくなります。

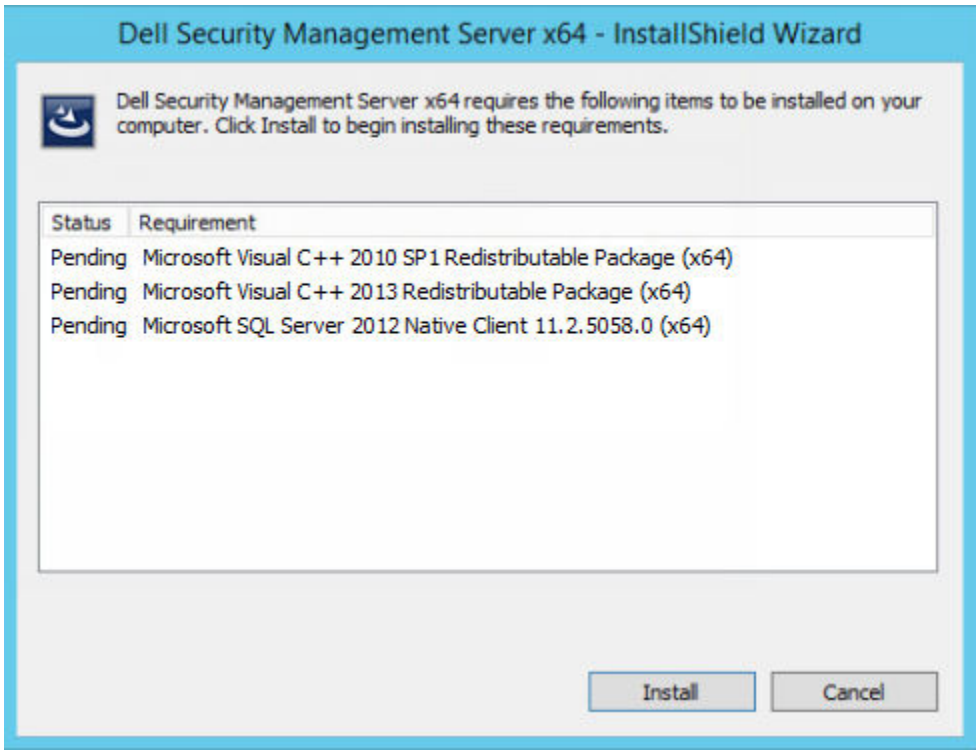
これでバックエンドサーバの移行タスクは完了です。

フロントエンドサーバーのアップグレード / 移行

1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。***コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. インストール用言語を選択して **OK** をクリックします。

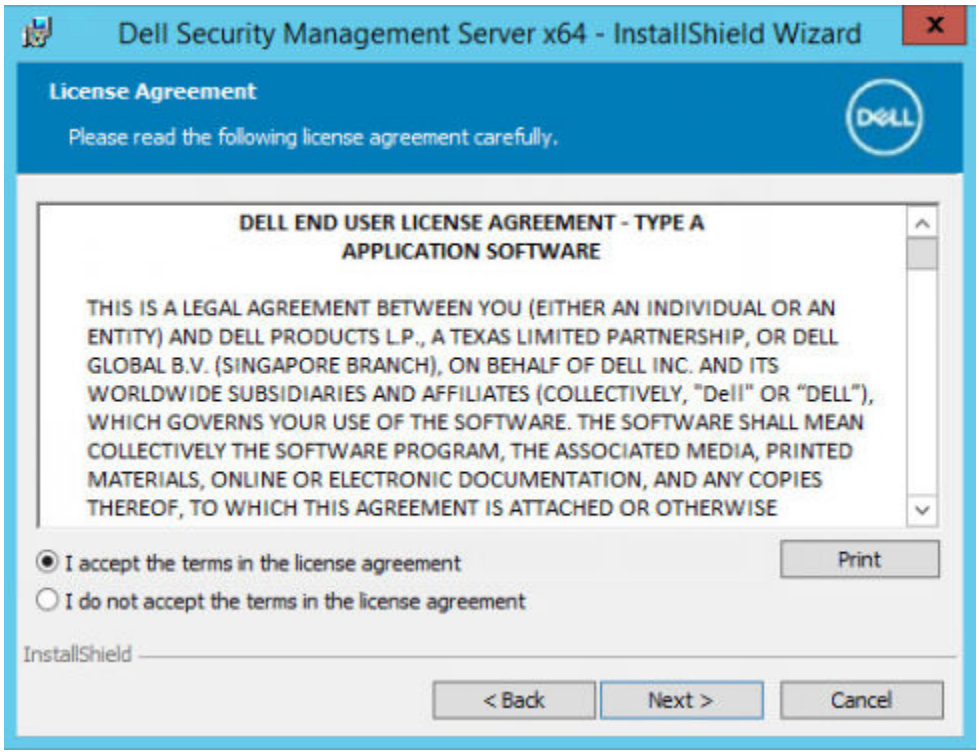


4. 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

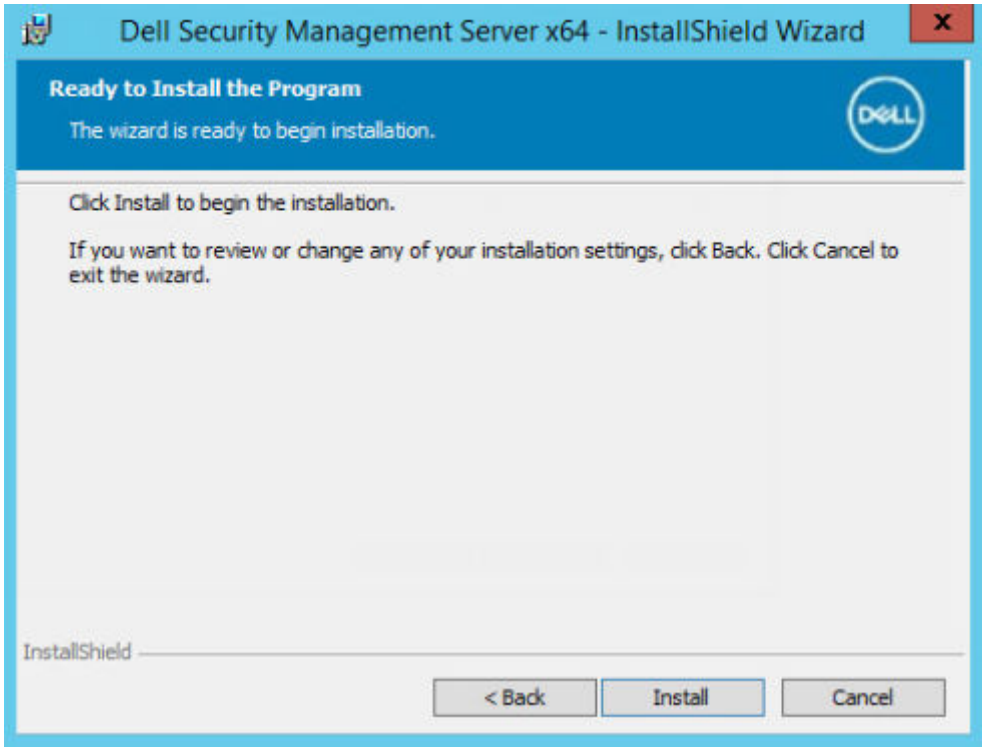


5. *ようこそ* ダイアログで **次へ** をクリックします。

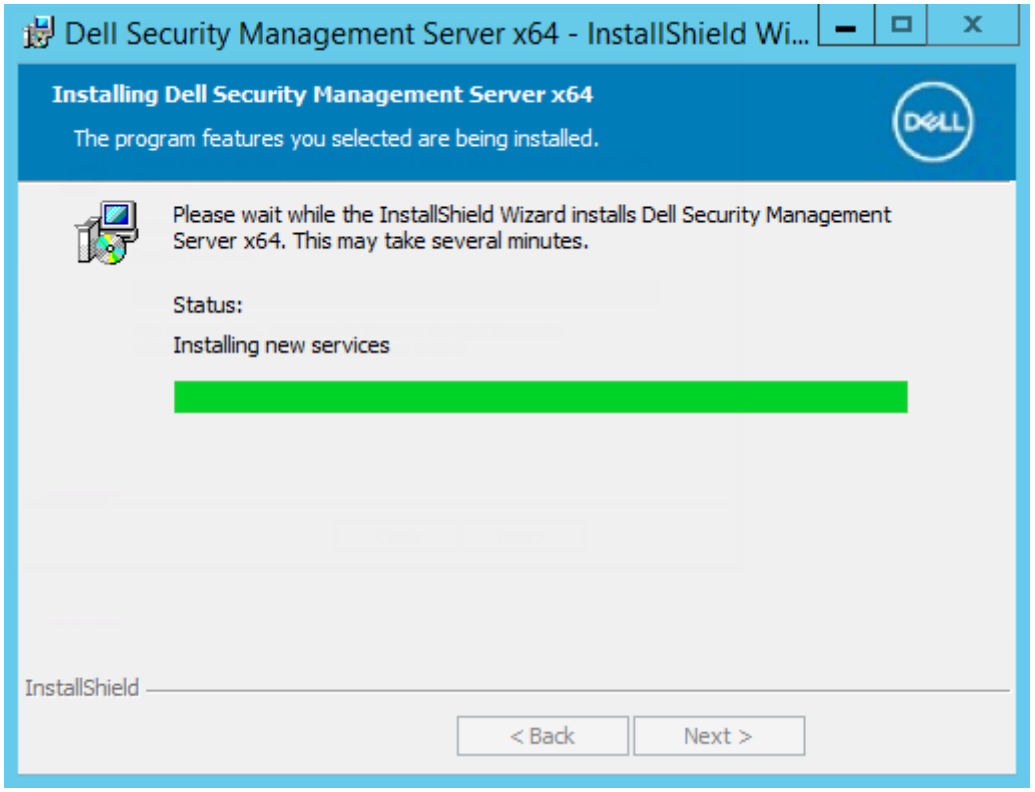
6. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。



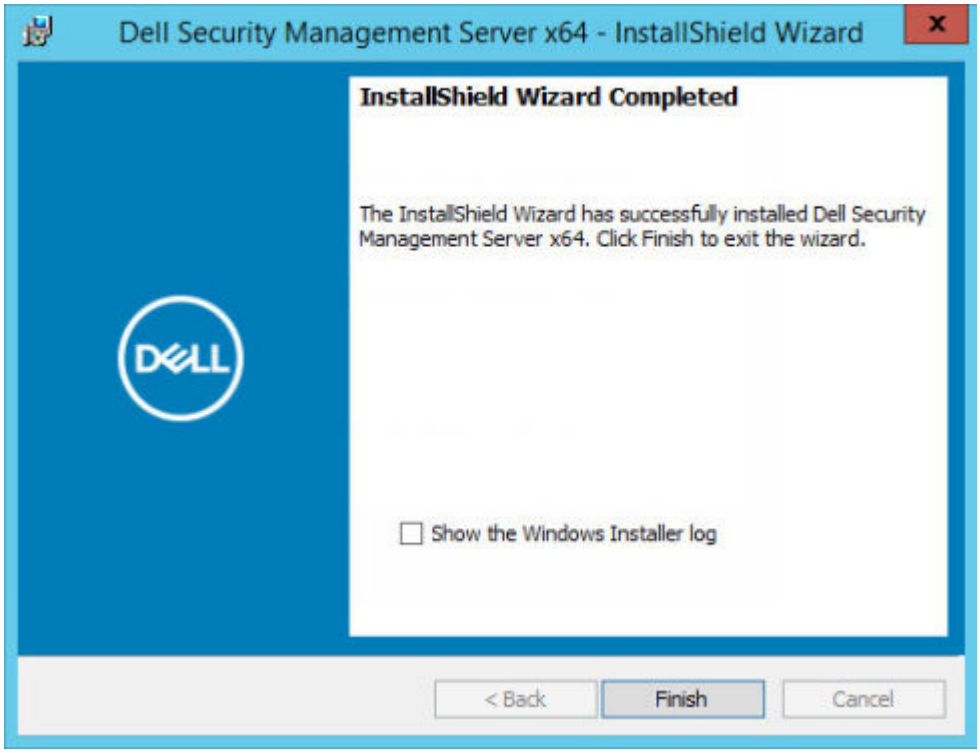
7. *プログラムインストールの準備完了*ダイアログで、**インストール** をクリックします。



ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。



8. インストールが完了したら、**終了** をクリックします。



9. バックエンドサーバーがフロントエンドサーバーと通信するように設定します。
   a. バックエンドサーバーで、<Security Server install dir>\conf\ に移動して、application.properties ファイルを開きます。
   b. publicdns.server.host を探し、外部で解決可能なホスト名を設定します。
   c. publicdns.server.port を探し、ポートを設定します (デフォルト値は 8443)。

   Dell サービスはインストール終了時に再起動されます。インストール後の設定が完了するまで Dell Server を再起動する必要はありません。

切断モードのインストール

切断モードは、インターネットおよびセキュアではない LAN または他のネットワークから Security Management Server を分離します。Security Management Server を切断モードでインストールすると、そのまま切断モードが維持され、接続モードには戻せません。

Security Management Server を切断モードでインストールするには、コマンドラインを使用します。

次の表には、使用可能なスイッチが一覧表示されています。

スイッチ	意味
/v	*.exe 内の .msi に変数を渡す
/s	サイレントモード

次の表には、使用可能な表示オプションが一覧表示されています。

オプション	意味
/q	進行状況ダイアログなし、処理完了後に自動で再起動
/qb	**キャンセル** ボタンを含む進行状況ダイアログ
/qn	ユーザーインタフェースなし

次の表は、インストールで使用できるパラメータの詳細です。これらのパラメータは、コマンドラインで指定することもできますし、プロパティを使用してファイルから呼び出すこともできます。

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

パラメータ
AGREE_TO_LICENSE=Yes - この値は「Yes」である必要があります。
PRODUCT_SN=xxxxx - 標準的な場所にライセンス情報を持っている場合は任意です。そうでない場合はこちらに入力します。
INSTALLDIR=<path> - オプション。
BACKUPDIR=<path> - ここにリカバリファイルが保存されます。 **メモ:** このインストール中にインストーラによって作成されたフォルダの構造 (例は下記参照) は変更しないでください。
AIRGAP=1 - 切断モードで Security Management Server をインストールするには、この値を「1」にする必要があります。
SSL_TYPE=n - n が 1 の場合は CA 機関から購入した既存の証明書をインポートし、2 の場合は自己署名証明書を作成します。SSL_TYPE 値は、必要な SSL プロパティを決定します。 以下は SSL_TYPE=1 で必要です： SSL_CERT_PASSWORD=xxxxx SSL_CERT_PATH=xxxxx 以下は SSL_TYPE=2 で必要です： SSL_CITYNAME SSL_DOMAINNAME SSL_ORGNAME SSL_UNITNAME SSL_COUNTRY - オプション、デフォルト = "US" SSL_STATENAME
SSOS_TYPE=n - n が 1 の場合は CA 機関から購入した既存の証明書をインポートし、2 の場合は自己署名証明書を作成します。SSOS_TYPE 値は、必要な SSOS プロパティを決定します。 以下は SSOS_TYPE=1 で必要です： SSOS_CERT_PASSWORD=xxxxx SSOS_CERT_PATH=xxxxx 以下は SSOS_TYPE=2 で必要です： SSOS_CITYNAME SSOS_DOMAINNAME SSOS_ORGNAME SSOS_UNITNAME SSOS_COUNTRY - オプション、デフォルト = "US" SSOS_STATENAME
DISPLAY_SQLSERVER - この値は SQL Server インスタンスとポート情報を取得するために解析されます。 例： DISPLAY_SQLSERVER=SQL_server\Server_instance, port
IS_AUTO_CREATE_SQLSERVER=FALSE - オプション。デフォルト値はデータベースが作成されていないことを意味する FALSE です。データベースはサーバ上にすでに存在している必要があります。

パラメータ
新しいデータベースを作成するには、この値を TRUE に設定します。
IS_SQLSERVER_AUTHENTICATION=0 - オプション。デフォルト値は 0 で、現在ログインしているユーザーの Windows 認証用資格情報を SQL サーバの認証に使用するように指定します。SQL 認証を使用するには、この値を 1 に設定します。 メモ: インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL Server に認証する必要があります。この資格情報は、インストール時の資格情報であり、実行時の資格情報ではありません。 SQL 認証を使用する場合は、以下が必要です。 IS_SQLSERVER_USERNAME IS_SQLSERVER_PASSWORD
EE_SQLSERVER_AUTHENTICATION - 必須。製品が使用するための認証メソッドを指定します。このステップによりアカウントと製品が関連付けられます。これらの資格情報も、Dell サービスが Security Management Server で作業する際に使用されます。Windows 認証を使用するには、この値を 0 に設定します。SQL 認証を使用するには、値を 1 に設定します。 メモ: アカウントではシステム管理者権限があること、SQL サーバを管理することができることを確認してください。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ：dbo およびデータベース役割メンバーシップ：db_owner を public にする必要があります。 SQL_EE_USERNAME - 必須。Windows 認証では、「ドメイン\ユーザー名」の形式を使用します。SQL 認証で、ユーザー名を指定します。 SQL_EE_PASSWORD - 必須。Windows ユーザー名または SQL ユーザー名に関連付けられているパスワードを指定します。 SQL 認証を使用する場合は (EE_SQLSERVER_AUTHENTICATION=1)、次が有効です。 RUNAS_KEYSERVER_USER - キーサーバを、「ドメイン/ユーザー」という形式の Windows ユーザー名「として実行」に設定します。これは、Windows のユーザーアカウントである必要があります。 RUNAS_KEYSERVER_PSWD - キーサーバを Windows のユーザーアカウントに関連付けられている Windows パスワード「として実行」に設定します。
SQL_ADD_LOGIN=T - オプション。デフォルトは null です (このログインは追加されません)。値が T に設定されており、SQL_EE_USERNAME がログインまたはデータベースのユーザーではない場合、インストーラはユーザーの SQL 認証用資格情報を追加し、権限を設定して製品で資格情報を使用できるようにしようとします。
以下は、ホスト名のパラメータです。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。形式は **server.domain.com** である必要があります。 メモ: ホスト名に下線 (「_」) は使用できません。
CORESERVERHOST - オプション。Core Server ホスト名。
RMIHOST - オプション。Compatibility Server ホスト名。
REPORTERHOST - オプション。Compliance Reporter ホスト名。
DEVICEHOST - オプション。Device Server ホスト名。
KEYSERVERHOST - オプション。Key Server ホスト名。
TIGAHOST - オプション。Security Server ホスト名。
SMTP_HOST - オプション。SMTP ホスト名。
ACTIVEMQHOST - オプション。Message Broker ホスト名。
以下はポートのパラメータです。必要に応じて、ポートを編集します。デルはデフォルトの使用を推奨します
SERVERPORT_CLIENTAUTH - オプション。

パラメータ
REPORTERPORT - オプション。
DEVICEPORT - オプション。
KEYSERVERPORT - オプション。
GKPORT - オプション。
TIGAPORT - オプション。
SMTP_PORT - オプション。
ACTIVEMQ_TCP - オプション。
ACTIVEMQ_STOMP - オプション。

切断モードでの Security Management Server のインストール

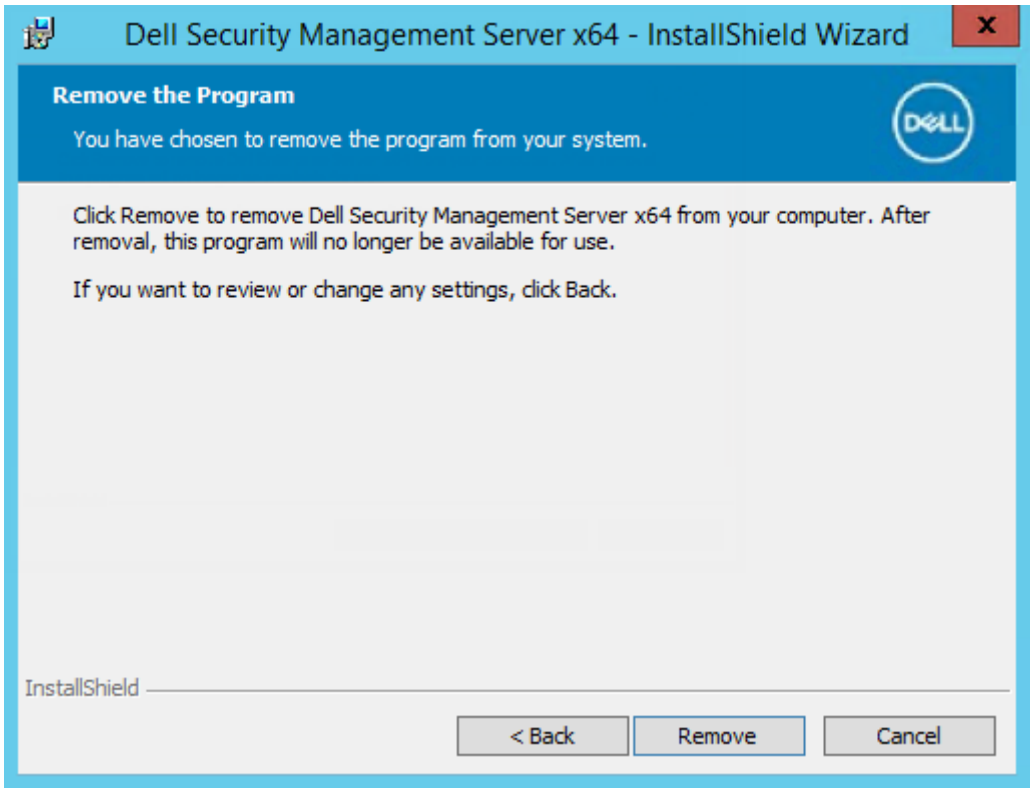
次の例では、C:\mysetups\eeoptions.txt\" " のファイルにリストされたインストールパラメータを使用して、進捗状況ダイアログを表示しながらサイレントモードで Security Management Server をインストールします。

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

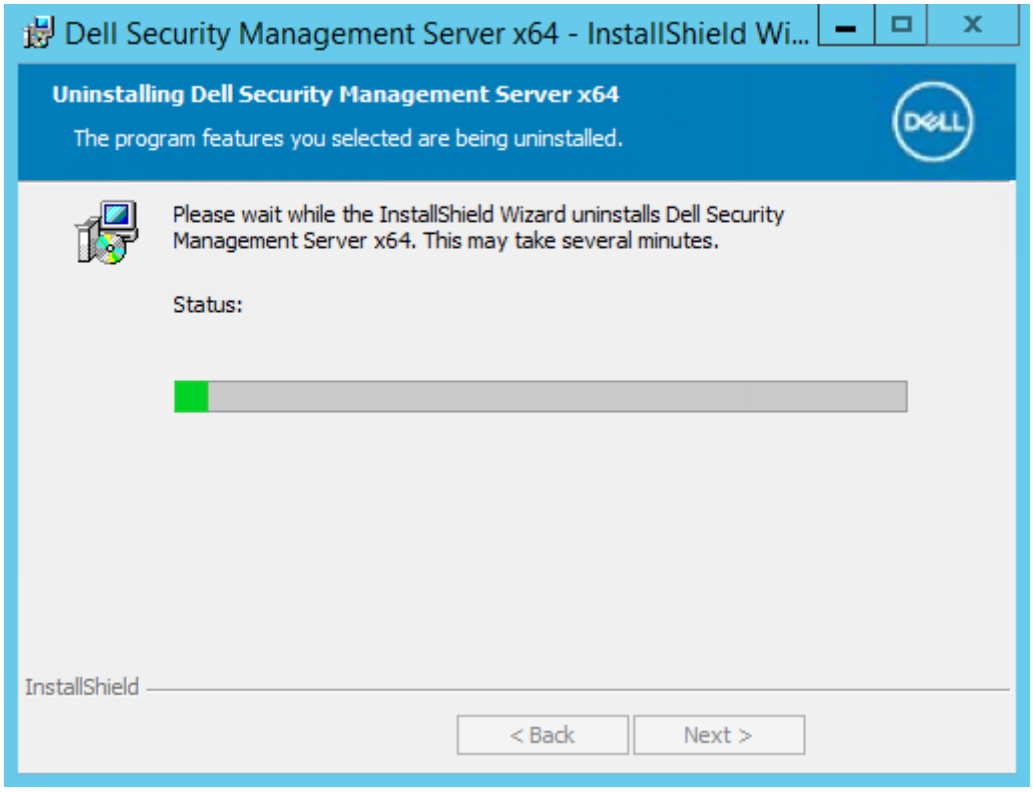
Security Management Server のアンインストール

1. Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server をアンインストールするサーバのルートディレクトリに**解凍**(コピー/貼り付けまたはドラッグ/ドロップではなく)します。***コピー/貼り付けまたはドラッグ/ドロップを行うと、エラーが発生し、インストールは失敗します。***
2. **setup.exe** をダブルクリックします。
3. *ようこそ*ダイアログで **次へ** をクリックします。

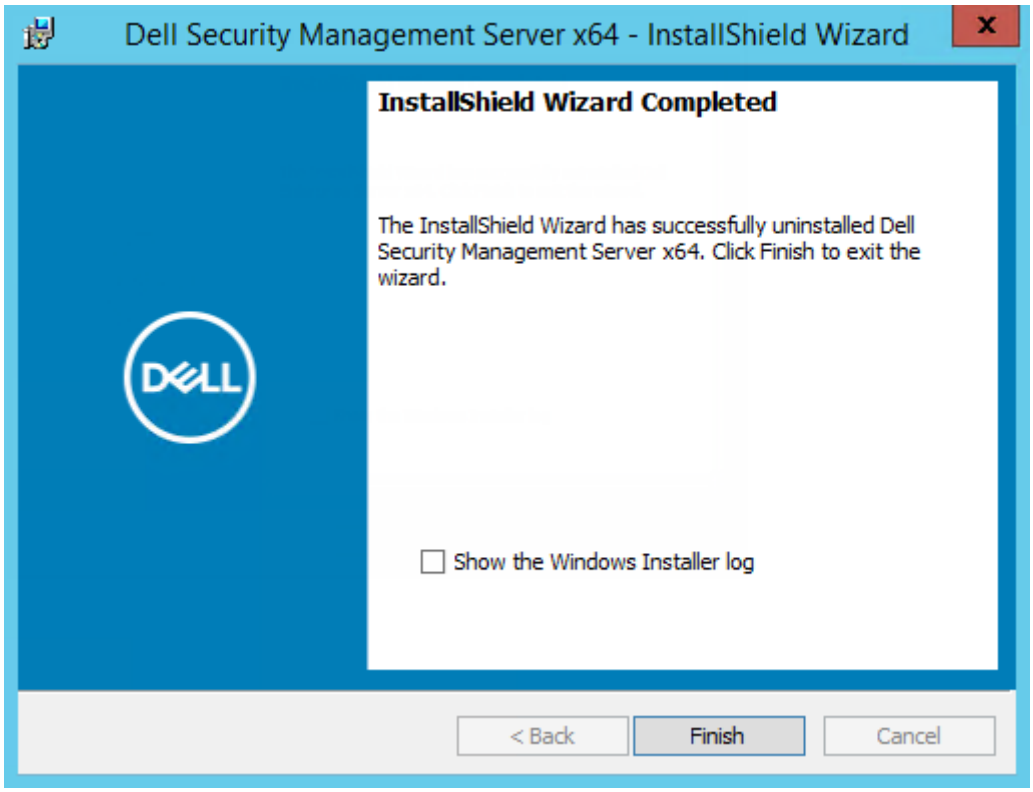
4. *プログラムの削除* ダイアログで、**削除** をクリックします。



ステータスは、アンインストールプロセスの全体を通して進捗状況ダイアログに表示されます。



5. アンインストールが完了したら、**終了** をクリックします。



5

インストール後の設定

Security Management Server の設定に関連する最新の回避策や既知の問題については、『*Security Management Server Technical Advisories*』(Security Management Server テクニカル アドバイザリー) をお読みください。

Security Management Server を初めてインストールするのか、既存のインストールをアップグレードするのかによって、環境のいくつかのコンポーネントを設定する必要があります。

Security Management Server のインストール後に、次のデフォルトを変更する必要があります。

- 次の場所にあるバック エンド サーバーのパスワードを変更します。

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- 次の場所にある環境内のすべてのフロント エンド サーバーのパスワードを変更します。

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

パスワードは次のように表示されます：`proxy-server.password=ENC(<texthere>)`

パスワードを変更するには、次の手順を実行します。

1. 次を選択します：`ENC(<texthere>)`
2. 選択したテキストを次に変更します：`CLR(<newpasswordhere>)`

   サービスが再開されると、変更した行が `CLR` から `ENC` に変わり、パスワードが暗号化されます。

メモ：proxy-server.username も変更できますが、メッセージ ブローカーの application.properties ファイルおよびアクティブなすべてのフロント エンド サーバー内で一致している必要があります。

DMZ モードの設定

Security Server が DMZ とプライベートネットワークに導入され、DMZ サーバのみが信頼できる証明機関 (CA) からのドメイン証明書を持っている場合は、その信頼できる証明書をプライベートネットワークの Security Server の Java キーストアに追加するために、手動でいくつかの手順を実行する必要があります。

信頼できる証明書が使用されている場合は、この項を省略してください。

メモ: デルでは、DMZ サーバおよびプライベートネットワークサーバの両方に対して信頼できる証明機関からのドメイン証明書を使用することを強く推奨します。

Microsoft のキーストア内の既存の証明書を使用して Dell Encryption の証明書をアップデートする情報については、http://www.dell.com/support/article/us/en/19/sln297240/ を参照してください。

サーバー設定ツール

インストールの完了後に環境設定が必要になった場合は、サーバ設定ツールを使用して変更します。

サーバー設定ツールでは、次の操作を行うことができます。

- 新規またはアップデートされた証明書の追加
- Dell Manager 証明書のインポート
- ID 証明書のインポート
- サーバ SSL 証明書の設定
- 電子メール サービスの SMTP の設定
- データベース名、場所、または資格情報の変更
- データベースの移行

Dell Core Server および Compatibility Server をサーバ設定ツールと同時に実行することはできません。Core Server サービスおよび Compatibility Server サービスを *サービス* 画面で停止します（**スタート > 実行** をクリックし、***Services.msc*** と入力）。その後に、サーバ設定ツールを起動します。

サーバ設定ツールを起動するには、**スタート** > **Dell** > **サーバ設定ツールの実行** の順に選択します。

サーバ設定ツールのログは、`C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs` に保存されます。

新規またはアップデートされた証明書の追加

証明書は、自己署名証明書または署名付き証明書のどちらを使用するか選択できます。

- **自己署名証明書**は、作成者自身によって署名されます。自己署名証明書は、パイロット、POC などに適しています。実稼働環境の場合は、パブリック CA 署名付き証明書またはドメイン署名付き証明書の使用をお勧めします。
- **署名付き**（パブリック CA 署名付きまたはドメイン署名付き）証明書は、パブリック CA またはドメインにより署名されます。パブリック認証局（CA）により署名された証明書の場合、通常は署名元 CA の証明書が Microsoft 証明書ストアにすでに存在するため、信頼チェーンは自動的に確立されます。ドメイン CA 署名付き証明書の場合は、ワークステーションがドメインに所属していれば、ドメインから提供される署名元 CA の証明書はワークステーションの Microsoft 証明書ストアに追加されているので、信頼チェーンが作成されます。

証明書の設定の影響を受けるコンポーネントは以下のとおりです。

- Java サービス（Device Server など）
- .NET アプリケーション（Core Server）
- 起動前認証用に使用されるスマートカードの検証（Security Server）
- Dell Manager に送信されるポリシーバンドルの署名に使用される秘密暗号化キーのインポート Dell Manager は、自己暗号化ドライブまたは BitLocker Manager が搭載された管理対象 Encryption クライアントの SSL 検証を実行します。
- クライアントワークステーション：
  - BitLocker Manager を実行しているワークステーション
  - Encryption Enterprise を実行しているワークステーション（Windows）
  - Endpoint Security Suite Enterprise を実行しているワークステーション

使用する証明書の種類に関する情報：

スマートカードを使用した起動前認証には Security Server での SSL 検証が必要です。Dell Manager は、Dell Core Server への接続時に SSL 検証を実行します。こうした種類の接続では、署名元 CA がキーストアに含まれている必要があります（対象の Dell Server コンポーネントに応じて、Java キーストアまたは Microsoft キーストアのいずれかになります）。自己署名証明書が選択された場合は、次のオプションを使用できます。

- 起動前認証用に使用されるスマートカードの検証：
  - Security Server の Java キーストアに「Root Agency」署名証明書と完全な信頼チェーンをインポートします。完全な信頼チェーンがインポートされる必要があります。

Dell Manager：

- Microsoft キーストアにあるワークステーションの「信頼されたルート証明機関」(「ローカルコンピュータ」用)に「Root Agency」署名証明書（生成された自己署名証明書からのもの）を挿入します。

  Security Management Server は、Active Directory 使用時に LDAP チャネル バインディングおよび LDAP 署名を行うための Microsoft 要件と互換性があります。

  Security Management Server でこれを有効にするには、Microsoft の証明書キーストア内の「信頼されたルート」ストアにインポートされたドメイン コントローラー証明書のルート発行証明書が必要です。

- Server サイド SSL 検証の動作を変更します。サーバサイドの SSL 信頼検証を無効にするには、設定 タブで **信頼チェーンチェックの無効化** を選択します。

証明書の作成方法には、*高速*と*詳細*の 2 つがあります。

いずれか **ひとつ** の方法を選択します。

- 高速 – すべてのコンポーネントに対して自己署名付き証明書を生成する場合はこの方法を選択します。これは最も簡単な方法ですが、自己署名証明書はパイロットや POC などにのみ適しています。実稼働環境では、パブリック CA 署名付き証明書またはドメイン署名付き証明書の使用をお勧めします。
- 詳細 – 各コンポーネントを個別に設定する場合はこの方法を選択します。

高速

1. 最上部のメニューから、[**アクション**] > [**証明書の設定**] を選択します。
2. 設定ウィザードが起動されたら、**高速** を選択し、**次へ** をクリックします。利用できる場合は、Security Management Server のインストール時に作成された自己署名証明書の情報が使用されます。
3. 最上部のメニューから、[**設定**] > [**保存**] を選択します。プロンプトが表示されたら、保存を確定します。

これで証明書セットアップは完了です。本項の残りの部分では、証明書の詳細な作成方法について詳しく説明します。

詳細

証明書を作成するには、[*自己署名付き証明書の生成*] と [*現在の設定の使用*] の 2 つの方法があります。いずれか**ひとつ**のパスを選択します。

- 方法 1 – 自己署名付き証明書の生成
- 方法 2 - 現在の設定の使用

方法 1 – 自己署名付き証明書の生成

1. 最上部のメニューから、[**アクション**] > [**証明書の設定**] を選択します。
2. 設定ウィザードが起動されたら、**詳細** を選択し、**次へ** をクリックします。
3. [**自己署名証明書の生成**] を選択し、[**次へ**] をクリックします。利用できる場合は、Security Management Server のインストール時に作成された自己署名証明書の情報が使用されます。
4. 最上部のメニューから、[**設定**] > [**保存**] を選択します。プロンプトが表示されたら、保存を確定します。

これで証明書セットアップは完了です。本項の残りの部分では、証明書その他の作成方法について詳しく説明します。

方法 2 - 現在の設定の使用

1. 最上部のメニューから、[**アクション**] > [**証明書の設定**] を選択します。
2. 設定ウィザードが起動されたら、**詳細** を選択し、**次へ** をクリックします。
3. [**現在の設定の使用**] を選択し、[**次へ**] をクリックします。
4. *Compatibility Server SSL 証明書*ウィンドウで、**自己署名証明書の生成** を選択し、**次へ** をクリックします。利用できる場合は、Security Management Server のインストール時に作成された自己署名証明書の情報が使用されます。

   次へ をクリックします。
5. *Core Server SSL 証明書* ウィンドウで、以下のいずれかを選択します。
   - *証明書の選*択 - 既存の証明書を使用する場合はこのオプションを選択します。**次へ** をクリックします。

     既存の証明書の場所を参照し、既存の証明書に関連付けられているパスワードを入力して、[**次へ**] をクリックします。

     完了したら、**終了** をクリックします。
   - *自己署名証明書の生成* - 利用できる場合は、Security Management Server のインストール時に作成された自己署名証明書の情報が使用されます。このオプションを選択すると、メッセージ セキュリティ証明書ウィンドウが表示されなくなり ([*現在の設定の使用*] オプションを選択すると表示されます)、Dell Compatibility Server 用に作成された証明書が使用されます。

     完全修飾コンピュータ名が正しいことを確認します。**次へ** をクリックします。

     同じ名前の証明書がすでにあることを示す警告メッセージが表示されます。使用するかどうかを尋ねるメッセージが表示されたら、**はい** をクリックします。

     完了したら、**終了** をクリックします。
   - *現在の設定の使用* - 証明書の設定を Security Management Server の初期構成後に随時変更する場合にこのオプションを選択します。このオプションでは、すでに設定済みの証明書はそのまま残ります。このオプションを選択すると、メッセージセキュリティ証明書 ウィンドウに進みます。

     メッセージセキュリティ証明書 ウィンドウで、次のいずれか**ひとつ**を選択します。
     - *証明書の選*択 - 既存の証明書を使用する場合はこのオプションを選択します。**次へ** をクリックします。

       既存の証明書の場所を参照し、既存の証明書に関連付けられているパスワードを入力して、[**次へ**] をクリックします。

       完了したら、**終了** をクリックします。

- *自己署名証明書の生成* - 利用できる場合は、Security Management Server のインストール時に作成された自己署名証明書の情報が使用されます。

  次へ をクリックします。

  完了したら、**終了** をクリックします。

これで証明書セットアップは完了です。

変更が完了したら、次の手順に従います。

1. 最上部のメニューから、[**設定**] > [**保存**] を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。 *サービス*が開いたら、それぞれの Dell サービスに移動し、[**サービスの開始**] をクリックします。

Dell Manager 証明書のインポート

暗号化管理エージェントが搭載された Security Management Server のリモート管理クライアントが導入に含まれている場合は、新しく作成した (または既存の) 証明書をインポートする必要があります。Dell Manager 証明書は、Security Management Server のリモートで管理されているクライアントおよび暗号化管理エージェントへ送られた、ポリシーバンドルにサインするための、プライベートキーを保護する手段として使用されます。この証明書は他の証明書のいずれにも無関係にすることができます。さらに、このキーが漏洩した場合は、これを新しいキーと交換することが可能で、Dell Manager はポリシーバンドルを復号化できない場合に新しい公開鍵を要求します。

1. Microsoft 管理コンソールを開きます。
2. **ファイル** > **スナップインの追加と削除** をクリックします。
3. **追加** をクリックします。
4. *スタンドアロンスナップインの追加* ウィンドウで **証明書** を選択し、**追加** をクリックします。
5. **コンピュータアカウント** を選択し、**次へ** をクリックします。
6. *コンピュータの選*択ウィンドウで **ローカルコンピュータ (このコンソールが実行されているコンピュータ)** を選択し、**終了** をクリックします。
7. **閉じる** をクリックします。
8. **OK** をクリックします。
9. *コンソールルートフォルダ*で、*証明書 (ローカルコンピュータ)* を展開します。
10. *パーソナル*フォルダを展開し、必要な証明書を見つけます。
11. 目的の証明書をハイライトし、**全てのタスク** > **エクスポート** を右クリックします。
12. 証明書のエクスポートウィザードが開いたら、**次へ** をクリックします。
13. **はい、秘密キーをエクスポートします** を選択し、**次へ** をクリックします。
14. **Personal Information Exchange - PKCS #12 (.PFX)** を選択してから、サブオプションの **可能な場合は証明書パスにすべての証明書を含める** と **すべての拡張プロパティをエクスポートする** を選択します。**次へ** をクリックします。
15. パスワードを入力し、確認します。ここにはどのようなパスワードを選んでも問題ありません。自分に覚えやすく、他人にはわかりにくいパスワードを選んでください。**次へ** をクリックします。
16. **参照** をクリックしてファイルを保存する場所を指定します。
17. *ファイル名* に、保存するファイルの名前を入力します。**保存** をクリックします。
18. **次へ** をクリックします。
19. **終了** をクリックします。
20. 正しくエクスポートされたことを知らせるメッセージが表示されます。MMC を閉じます。
21. Dell Server 設定ツールに戻ります。
22. 最上部のメニューから、**アクション** > **DM　証明書のインポート** を選択します。

23. エクスポートしたファイルが保存されている場所に移動します。ファイルを選択し、**開く** をクリックします。

24. そのファイルに関連付けられているパスワードを入力し、**OK** をクリックします。

これで Dell Manager 証明書のインポートが完了しました。

変更が完了したら、次の手順に従います。

1. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。*サービス* が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

SSL/TLS 証明書のベータ版のインポート

導入にサーバーの暗号化が含まれている場合は、新しく作成した（または既存の）証明書をインポートする必要があります。SSL/TLS 証明書のベータ版は、クライアントサーバに送信されるポリシーバンドルの署名に使用する秘密キーを保護します。

1. 最上部のメニューから、**アクション** > **SSL/TLS 証明書のベータ版のインポート** を選択します。
2. 証明書を参照して選択し、**次へ** をクリックします。
3. *証明書パスワード* プロンプトに、既存の証明書に関連付けられているパスワードを入力します。
4. Windows アカウントダイアログで、いずれかのオプションを選択します。
   a. ID 証明書に関連付けられている資格情報を変更するには、**ID 証明書で異なる Windows アカウント資格情報を使用する** を選択します。
   b. 現在ログオンしているアカウントの資格情報を継続して使用するには、**次へ** をクリックします。
5. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

サーバ SSL 証明書の設定

サーバー設定ツールで、**設定**タブをクリックします。

Dell Manager：

サーバサイドの Dell Manager SSL 信頼検証を無効にするには、**信頼チェーンチェックの無効化** を選択します。

SCEP：

Mobile Edition を使用している場合は、SCEP をホスティングするサーバの URL を入力します。

メモ: v9.8 では、Mobile Edition はサポートされなくなりました。

変更が完了したら、次の手順に従います。

1. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。*サービス* が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

SMTP 設定の構成

サーバー設定ツールで、**SMTP** タブをクリックします。

このタブでは、製品情報、通知、および Advanced Threat Prevention の Threat Relay メッセージの SMTP 設定を行います。

設定の変更が完了したら、セキュリティサーバサービスを再起動します。設定を更新するには、セキュリティサーバサービスを再起動する必要があります。

以下の情報を入力します。

1. *ホスト名* に、SMTP サーバの FQDN (smtpservername.domain.com など) を入力します。
2. *ユーザー名* に、メールサーバにログインするユーザー名を入力します。書式は、DOMAIN\jdoe、jdoe、あるいは組織の要件に従ったものになります。
3. *パスワード* に、このユーザー名に関連付けられているパスワードを入力します。
4. *送信元アドレス* に、電子メールの送信元アドレスを入力します。これはユーザー名のアカウントと同じ (jdoe@domain.com) にしても、特定のユーザー名が電子メールを送信するために使用する別のアカウント (CloudRegistration@domain.com) にしてもかまいません。
5. *ポート* に、ポート番号 (通常は 25) を入力します。
6. [*認証*] メニューで、[*True*] または [*False*] のいずれかを選択します。

メモ: 認証を 偽 に設定した場合、ユーザー名とパスワードは空白にする必要があります。

変更が完了したら、次の手順に従います。

1. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。 *サービス* が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

データベース名、場所、または資格情報の変更

サーバ設定ツールで、**データベース** タブをクリックします。

1. *サーバ名* に、データベースをホスティングしているサーバの完全修飾ドメイン名 (インスタンス名がある場合はインスタンス名も含む) を入力します。例：SQLTest.domain.com\DellDB。

   IP アドレスも使用できますが、完全修飾ドメイン名を使用することをお勧めします。
2. *サーバポート* に、ポート番号を入力します。

   デフォルト以外の SQL Server インスタンスを使用する場合は、*ポート：* にインスタンスの動的ポートを指定してください。その代替として、SQL Server Browser サービスを有効化して、UDP ポート 1434 が開放されていることを確認します。詳細については https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx を参照してください。
3. *データベース* に、データベースの名前を入力します。
4. *認証：* で、**Windows 認証** または **SQL Server 認証** を選択します。Windows 認証を選択すると、Windows にログインするときに使用したのと同じ資格情報が認証に使用されます (*ユーザー名* と *パスワード* は編集できない状態になります)。
5. *ユーザー名：* に、このデータベースに関連付けられている適切なユーザー名を入力します。
6. *パスワード：* に、*ユーザー名* にリストされたユーザー名のパスワードを入力します。
7. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
8. データベース設定をテストするには、最上部メニューから、**アクション** > **データベース設定のテスト** を選択します。設定ウィザードが起動します。
9. *設定のテスト* ウィンドウでテストに関する情報を読み、**次へ** をクリックします。
10. *データベース* タブで Windows 認証 を選択した場合は、任意で代替の資格情報を入力して、Security Management Server の実行時に使用したものと同じ資格情報を使用できるようにすることができます。**次へ** をクリックします。
11. *設定のテスト* ウィンドウに、接続設定テスト、互換性テスト、およびデータベース移行テストの結果が表示されます。
12. **終了** をクリックします。

メモ:

SQL データベース、または SQL インスタンスのどちらかが非デフォルトの照合順序で設定されている場合は、非デフォルトの照合順序が大文字と小文字を区別するものである必要があります。照合順序のリストと、大文字と小文字の区別については、https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx を参照してください。

変更が完了したら、次の手順に従います。

1. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。*サービス* が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

データベースの移行

最新アップグレードのサーバを使用して、v9.2 以降のデータベースを最新のスキーマに移行することができます。

サーバ設定ツールで、**データベース** タブをクリックします。

1. 既存のデルサーバデータベースのバックアップをまだ実行していない場合は、**今すぐ実行してください**。
2. 最上部のメニューから、**アクション** > **データベースの移行** を選択します。設定ウィザードが起動します。
3. *エンタープライズデータベースの移行*ウィンドウに警告が表示されます。データベース全体をバックアップ済みか、既存のデータベースのバックアップを取る必要がないことを確認してください。**次へ** をクリックします。

   *データベースの移行*ウィンドウに、移行の状態を示す情報メッセージが表示されます。

   完了したら、エラーがないか確認します。

   メモ: エラーメッセージに  **が付いている場合は、データベースタスクが失敗しており、是正処置を取らなければデータベースの移行を適切に実行できません。完了 をクリックして、データベースエラーを修正し、本項の手順を再度開始します。**
4. **終了** をクリックします。

移行が完了したら、以下の操作を実行します。

1. 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2. Dell Server 設定ツールを閉じます。
3. **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。*サービス* が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

6

管理作業

Dell 管理者役割の割り当て

1. Security Management Server Virtual 管理者として、管理コンソール（https://server.domain.com:8443/webui/）にログインします。デフォルトの資格情報は **superadmin/changeit** です。
2. 左ペインで **ポピュレーション** > **ドメイン** をクリックします。
3. ユーザーを追加するドメインをクリックします。
4. ドメイン詳細 ページで、**メンバー** タブをクリックします。
5. **ユーザーの追加** をクリックします。
6. 共通名、UPN（Universal Principal Name）、または sAMAccountName によるユーザー名の検索に使用するフィルターを入力します。ワイルドカード文字は * です。

   共通名、UPN（Universal Principal Name）、および sAMAccountName は、各ユーザーのエンタープライズディレクトリサーバーで定義されている必要があります。ユーザーがドメインまたはグループのメンバーであるにもかかわらず、管理のドメインまたはグループのメンバーリストに表示されない場合は、エンタープライズディレクトリサーバでそのユーザーの 3 つの名前がすべて正しく定義されていることを確認してください。

   クエリでは、一致が見つかるまで、共通名、UPN、sAMAccountName の順に自動的に検索します。

7. *ディレクトリユーザーリスト*から、ドメインに追加するユーザーを選択します。複数のユーザーを選択するには、<Shift><click> または <Ctrl><click> を使用します。
8. **追加** をクリックします。
9. メニューバーから、指定したユーザーの **詳細とアクション** タブをクリックします。
10. メニューバーをスクロールして、**管理者** タブを選択します。
11. 管理者の役割を選択して、このユーザーに追加します。
12. **保存** をクリックします。

Dell 管理者役割でのログイン

1. 管理コンソールからログアウトします。
2. 管理コンソールにログインし、ドメインユーザーの資格情報でログインします。

クライアントアクセスライセンスのアップロード

クライアントアクセスライセンスは、初回購入時またはクライアントアクセスライセンスを追加した場合には初回購入後に、インストールファイルとは別に付与されています。

1. 左側のペインで、**管理** をクリックします。
2. **ライセンス管理** をクリックします。
3. **ファイルを選択する** をクリックし、クライアントライセンス ファイルを探して選択します。

ポリシーのコミット

インストールが完了したらポリシーをコミットします。

ポリシーの変更を保存し、ポリシーのインストール後、またはそれ以後にポリシーをコミットするには、次の手順に従います。

1. 左側のペインで、**管理** > **コミット** をクリックします。

2. *コメント* に、変更内容の説明を入力します。
3. **ポリシーのコミット** をクリックします。

Dell Compliance Reporter の設定

1. 左側のペインで、**Compliance Reporter** をクリックします。
2. Dell Compliance Reporter が起動されたら、デフォルトの資格情報 *superadmin/changeit* を使用してログインします。

バックアップの実行

災害復旧のため、夜間に作成される差分で、次の場所のバックアップが毎週作成されるようにしてください。災害復旧の計画に関する詳細については、http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en を参照してください。Compliance Reporter データのバックアップに関する詳細については、http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en を参照してください。

Security Management Server バックアップ

インストール中 (27 ページ の 手順 10)、またはアップグレード / 移行中 (68 ページ の 手順 6) に設定ファイルのバックアップ用に選択した場所に、保存したファイルを定期的にバックアップしてください。このデータはほとんど変更されることがなく、必要に応じて手動で再設定できるため、週次バックアップでも十分です。最も重要なファイルには、データベースに接続するための情報が保存されています。

<インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

SQL Server のバックアップ

トランザクションログを有効にして、夜間の完全バックアップを実行し、3~4 時間ごとに差分データベースバックアップを実行します。バックアップデータベースが使用可能な場合、トランザクションログおよび/またはログ配布タスクは 15 分 (可能な場合はそれ以下) 間隔で実行することが推奨されます。通常通り、データベースのベストプラクティスをデルサーバデータベースに使用し、組織の災害復旧計画にデルソフトウェアを含めることをお勧めします。

SQL Server のベストプラクティスの詳細については、次のリストを参照してください。このリストを実装していない場合は、Dell Security のインストール時に実装してください。

PostgreSQL Server のバックアップ

監査イベントは C:\ProgramData\Dell\PostgreSQL\10.7\data にある PostgreSQL Server に保存され、日常的にバックアップする必要があります。バックアップ手順については、「/C:/ProgramData/Dell/PostgreSQL/10.7/data」を参照してください。

デルでは、データベースのベストプラクティスを PostgreSQL データベースに使用し、組織の災害復旧計画にデルソフトウェアを含めることを推奨します。

7

ポート

以下の表は、各コンポーネントとその機能について説明しています。

名前	デフォルトポート	説明
ACL サービス	TCP/8006	さまざまな Dell Security 製品の各種の権限とグループ アクセスを管理します。 メモ: ポート 8006 は現在保護されていません。このポートがファイアウォールで適切にフィルタリングされていることを確認してください。このポートは内部専用です。
Compliance Reporter	HTTP(S)/8084	監査とコンプライアンスのレポートのために、環境の詳細ビューを提供します。 メモ: ポート 8084 は、ファイアウォールを介したフィルタリングが必要です。このポートは内部でのみ使用することをお勧めします。
管理コンソール	HTTP(S)/8443	企業全体での導入に対応する管理コンソールとコントロールセンター。
Core Server	HTTPS/8888	ポリシーフロー、ライセンス、起動前認証の登録、SED Management、BitLocker Manager、Threat Protection、Advanced Threat Prevention を管理します。Compliance Reporter および管理コンソールが使用するインベントリデータを処理します。認証データを収集し、保管します。役割に基づいたアクセスを制御します。
Device Server	HTTPS/8081	アクティベーションとパスワードの復元をサポートします。 Security Management Server のコンポーネント Encryption Enterprise (Windows および Mac) に必要です。
Security Server	HTTPS/8443	Policy Proxy との通信を行います。また、フォレンジック キーの取得、クライアントのアクティベーション、SED-PBA およびフル ディスク暗号化-PBA の通信、ならびに管理コンソールへの認証のための ID 検証を含む認証または仲裁のための Active Directory を管理します。SQL データベースアクセスが必要です。
Compatibility Server	TCP/1099	エンタープライズアーキテクチャを管理するためのサービスです。アクティベー

名前	デフォルトポート	説明
		ション中の初期インベントリデータおよび移行時のポリシーデータを収集、保管します。ユーザーグループに基づいてデータを処理します。 **メモ:** ポート 1099 は、ファイアウォールを介したフィルタリングが必要です。このポートは内部でのみ使用することをお勧めします。
Message Broker サービス	TCP/ 61616 および STOMP/ 61613	デルサーバのサービス間の通信を処理します。ポリシープロキシのキュー操作のために Compatibility Server によって作成されるポリシー情報をステージします。 SQL データベースアクセスが必要です。 **メモ:** ポート 61616 は、ファイアウォールを介したフィルタリングが必要です。このポートは内部でのみ使用することをお勧めします。 **メモ:** ポート 61613 は、フロントエンド モードで構成した Security Management Server に対してのみ開かれるようにする必要があります。
Key Server	TCP/ 8050	Kerberos API を使用して、クライアント接続のネゴシエーション、認証、暗号化を行います。 重要なデータの取得には SQL データベースのアクセスが必要です。
Policy Proxy	TCP/ 8000	セキュリティポリシーのアップデートとインベントリのアップデートを配信するためのネットワークベースの通信パスを提供します。
PostGres	TCP/ 5432	イベンティング データ用に使用されるローカル データベース。 **メモ:** ポート 5432 は、ファイアウォールを介したフィルタリングが必要です。このポートは内部でのみ使用することをお勧めします。
LDAP	TCP/ 389/636 (ローカルドメインコントローラ)、 3268/3269 (グローバルカタログ) TCP/	ポート 389 - このポートはローカルドメインコントローラからの情報の要求に使用されます。ポート 389 に送信される LDAP 要求は、グローバルカタログのホームドメイン内にあるオブジェクトの検索にのみ使用できます。ただし、要求側のアプリケーションは、これらのオブジェクトに対するすべての属性を取得できます。たとえば、ポート 389 への要求は、ユーザーの部門を取得するために使用することができます。

名前	デフォルトポート	説明
	135/ 49125+ (RPC)	ポート 3268 - このポートは、特にグローバルカタログをターゲットとするクエリ用に使用されます。ポート 3268 に送信される LDAP 要求は、フォレスト全体でのオブジェクトの検索に使用することができます。ただし、返されるのはグローバルカタログへのリプリケーション用にマークされた属性のみです。たとえば、ポート 3268 を使用してユーザーの部門は返すことはできません。これは、この属性がグローバルカタログに複製されないためです。
Microsoft SQL データベース	TCP/ 1433	デフォルトの SQL Server ポートは 1433 であり、クライアントポートには 1024 から 5000 の間の値がランダムに割り当てられます。
クライアント認証	HTTPS/ 8449	クライアントサーバがデルサーバを認証できるようにします。Server Encryption に必要です。

8

SQL Server ベストプラクティス

以下に、SQL Server のベストプラクティスを説明するリストを示します。ベストプラクティスをまだ実装していない場合は、Dell Security のインストール時に実装するようにしてください。

1. データファイルおよびログファイルが格納される NTFS ブロックサイズが 64 KB になっていることを確認します。SQL Server エクステント（SQL ストレージの基本単位）は 64 KB です。

   詳細については、Microsoft の TechNet 記事「ページとエクステントについて」を検索してください。

2. 一般的なガイドラインとして、SQL Server の最大メモリ数は、インストールされているメモリの 80 パーセントに設定します。

   詳細については、Microsoft の TechNet 記事「*サーバー メモリーの構成オプション*」を検索してください。

   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3. インスタンスのスタートアッププロパティで -t1222 を設定して、デッドロックが発生した場合にその情報を取得できるようにします。

   詳細については、Microsoft の TechNet 記事「トレース フラグ（Transact-SQL）」を検索してください。

   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4. すべてのインデックスが、インデックスを再構築するための週次メンテナンスジョブの対象になっていることを確認します。

5. アクセス許可と機能が、Security Management Server によって使用されるデータベースに対して適切であることを確認します。詳細については、KB 記事 SLN307771 を参照してください。

9

証明書

この章では、Security Management Server を使用して証明書を取得する方法について説明します。

スマートカード認証を設定する方法の詳細については、「http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en」を参照してください。

Dell Data Security Server で使用する SSL/TLS 証明書を要求するための最小要件については、「http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en」を参照してください。

Microsoft のキーストア内の既存の証明書を使用して Dell Encryption の証明書をアップデートする情報については、http://www.dell.com/support/article/us/en/19/sln297240/ を参照してください。

自己署名証明書の作成と証明書署名要求の生成

このセクションでは、Java ベースのコンポーネントの自己署名証明書を作成する手順について詳しく説明します。このプロセスは、.NET ベースのコンポーネントの自己署名証明書の作成には使用 **できません**。

実稼動環境でない環境では自己署名証明書 *のみ*を推奨します。

組織で SSL サーバー証明書が必要な場合、または他の理由で証明書を作成する必要がある場合は、このセクションで、Keytool を使用した Java キーストアの作成プロセスが説明されています。

組織が認証にスマートカードを使用することを計画している場合は、Keytool を使用して、スマートカードユーザーの証明書で使用される完全な証明書信頼チェーンをインポートする必要があります。

Keytool は、証明書署名要求 (CSR) の形式で、VeriSign® や Entrust® などの証明機関 (CA) に渡される秘密鍵を作成します。その後、CA はこの CSR に基づいて署名したサーバー証明書を作成します。サーバー証明書は、署名機関証明書とともにファイルにダウンロードされます。その後、証明書は cacerts ファイルにインポートされます。

新しいキーペアと自己署名証明書の生成

1. **conf** ディレクトリ (Compliance Reporter、Security Server、または Device Server) に移動します。
2. デフォルトの証明書データベースをバックアップします。

   スタート > **ファイル名を指定して実行** をクリックして、**move cacerts cacerts.old** と入力します。
3. Keytool をシステムパスに追加します。コマンドプロンプトで次のコマンドを入力します。

   set path=%path%;<Dell Java Install Dir>\bin
4. 証明書を生成するため、次のようにして Keytool を実行します。

   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell **-keystore .\cacerts**
5. Keytool プロンプトが表示されたら次の情報を入力します。

   メモ:

   設定ファイルは、編集する前にバックアップしてください。指定されたパラメータのみを変更してください。これらのファイル内のその他のデータ (タグを含む) を変更すると、システムの破損や障害が発生するおそれがあります。デルは、これらのファイルの許可されてない変更に起因する問題が、Security Management Server の再インストールなしで解決できることを保証できません。

- *キーストアのパスワード*: パスワードを入力し (サポートされていない文字は <>;&" ')、コンポーネント **conf** ファイル内の変数を次のように同じ値に設定します。

  <Compliance Reporter install dir>\conf\eserver.properties.Set the value eserver.keystore.password =

  <Device Server install dir>\conf\application.properties.Set the value keystore.password =

<Security Server install dir>\conf\application.properties.Set the value keystore.password =

- *完全修飾サーバー名*：現在作業中のコンポーネントがインストールされているサーバーの完全修飾名を入力します。この完全修飾名には、ホスト名とドメイン名を含めます（例：server.domain.com）。
- *組織単位*：適切な値を入力します（例：セキュリティ）。
- *組織*：該当する値を入力します（例：Dell）。
- *市区町村*：適切な値を入力します（例：Dallas）。
- *都道府県*：省略形でない都道府県の名前を入力します（たとえば、Texas）。
- 2 文字の国コード。
- ユーティリティによって、情報が正しいことを確認するように求められます。情報が正しい場合は、**はい**と入力します。

  情報が正しくない場合は、**no** と入力します。Keytool は以前に入力された各値を表示します。**Enter** をクリックして値を受け入れるか、値を変更して **Enter** をクリックします。
- *別名のキーパスワード*：ここに別のパスワードを入力しなかった場合は、このパスワードがデフォルトでキーストアのパスワードになります。

証明機関からの署名付き証明書の要求

次の手順に従って、「新しいキーペアと自己署名証明書の生成」で作成された自己署名付き証明書の証明書署名要求（CSR）を生成します。

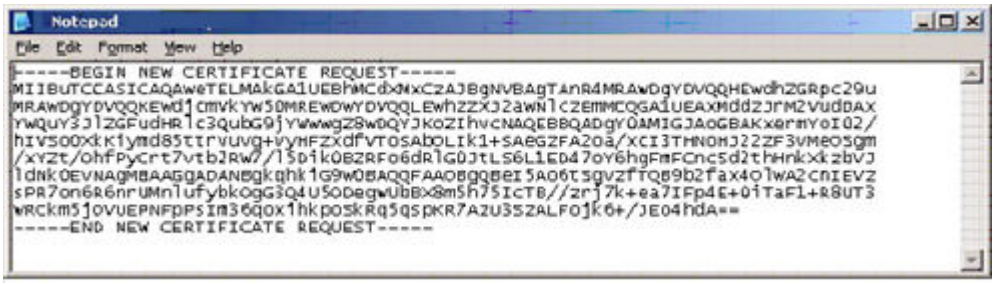
1. <**certificatealias**> で以前に使用した値と同じ値を代入します。

   ```
   keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
   <csr-filename>
   ```

   例：**keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file** Dell**.csr**

   .csr ファイルには、CA 上での証明書の作成時に使用する BEGIN/END ペアがあります。

   例 .CSR ファイル

2. 証明機関からの SSL サーバー証明書の取得には、所属組織のプロセスに従います。署名用に <csr-filename> の内容を送信します。

   メモ:

   有効な証明書を要求する方法は数通りあります。方法の例を、「**証明書の要求方法の例**」に示します。
3. 署名付き証明書を受信したら、ファイルに保存します。
4. ベストプラクティスとして、インポートプロセスでエラーが発生した場合に備え、この証明書をバックアップします。このバックアップを用意しておけば、処理をやり直す必要がなくなります。

ルート証明書のインポート

ルート証明書の証明機関が Verisign（Verisign Test ではない）の場合は、この手順をスキップして次の手順に進み、署名付き証明書をインポートしてください。

証明機関のルート証明書により、署名付き証明書を認証します。

1. 次の**いずれか**を実行します。
   - 証明機関のルート証明書をダウンロードして、ファイルに保存します。
   - エンタープライズディレクトリサーバーのルート証明書を取得します。
2. 次の**いずれか**を実行します。
   - Compliance Reporter、Security Server、Device Server に対して SSL を有効にする場合は、コンポーネントの **conf** ディレクトリに変更します。
   - Security Management Server とエンタープライズディレクトリサーバ間の SSL を有効にする場合は、<**Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** に変更します (JRE cacerts のデフォルトのパスワードは **changeit** です)。
3. 次のようにして Keytool を実行し、ルート証明書をインストールします。

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

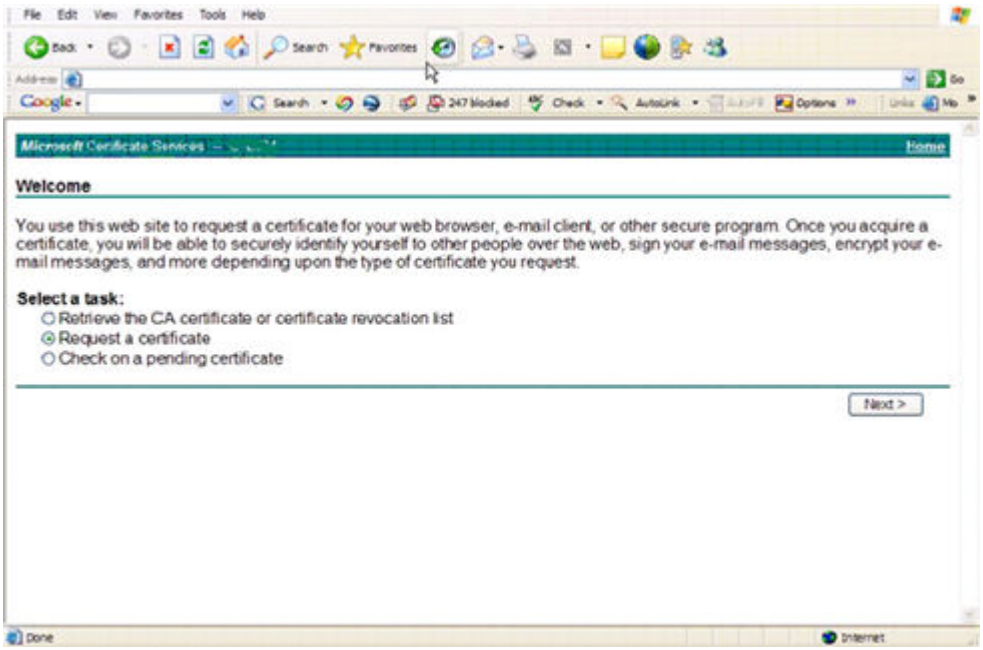
例： **keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer**

証明書の要求方法の例

証明書の要求方法の一例として、組織内に設定されている Microsoft CA Server に Web ブラウザを使用してアクセスする方法があります。

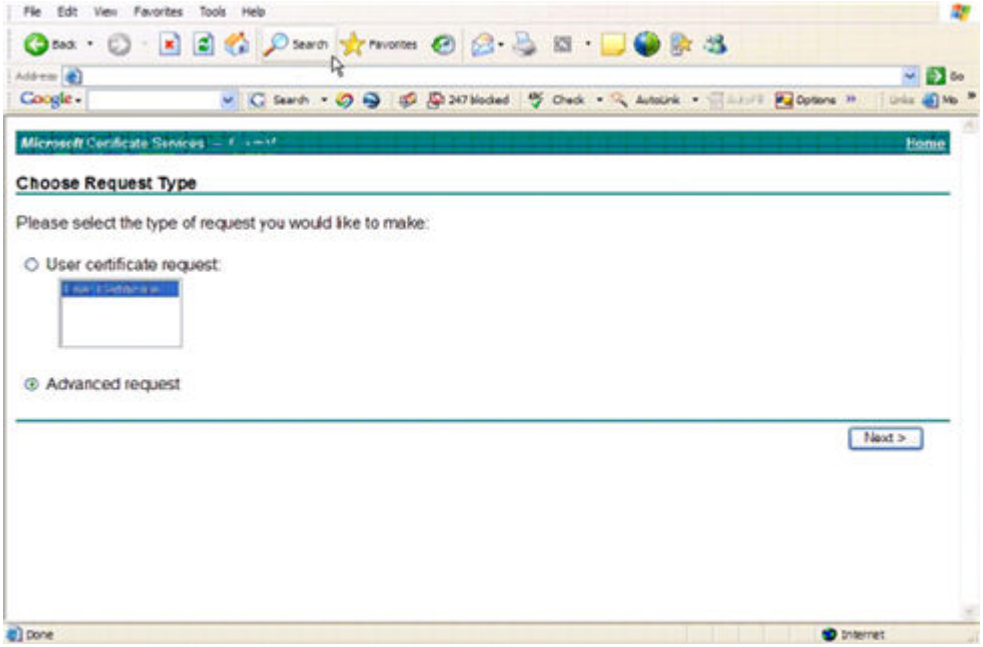
1. Microsoft CA Server に移動します。IP アドレスは組織から提供されます。
2. **証明書の要求** を選択し、**次へ** をクリックします。

Microsoft 証明書サービス



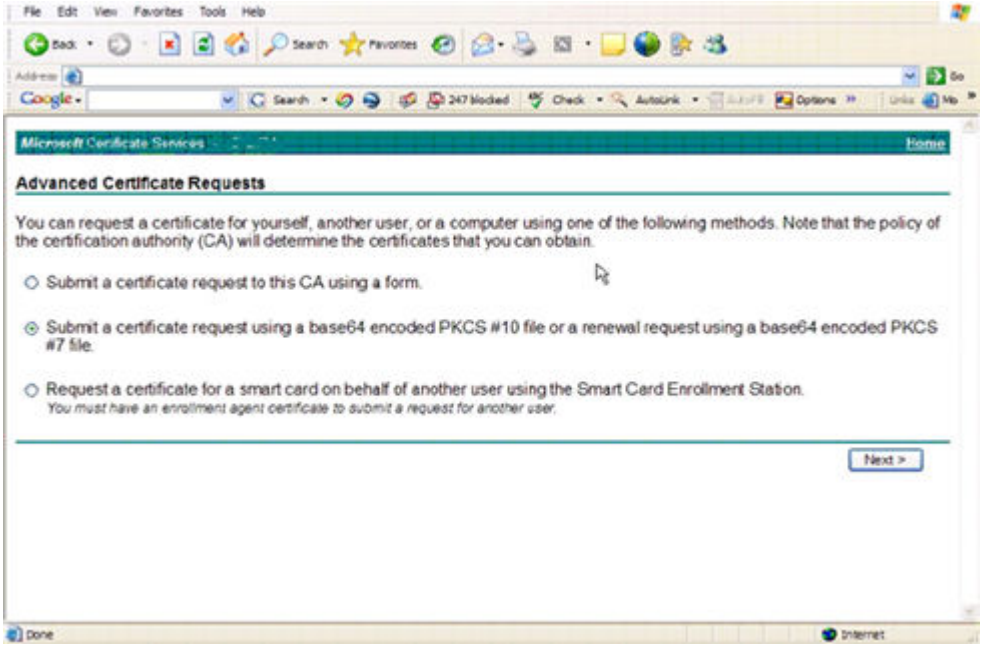
3. **高度な要求** を選択し、**次へ** をクリックします。

要求タイプの選択



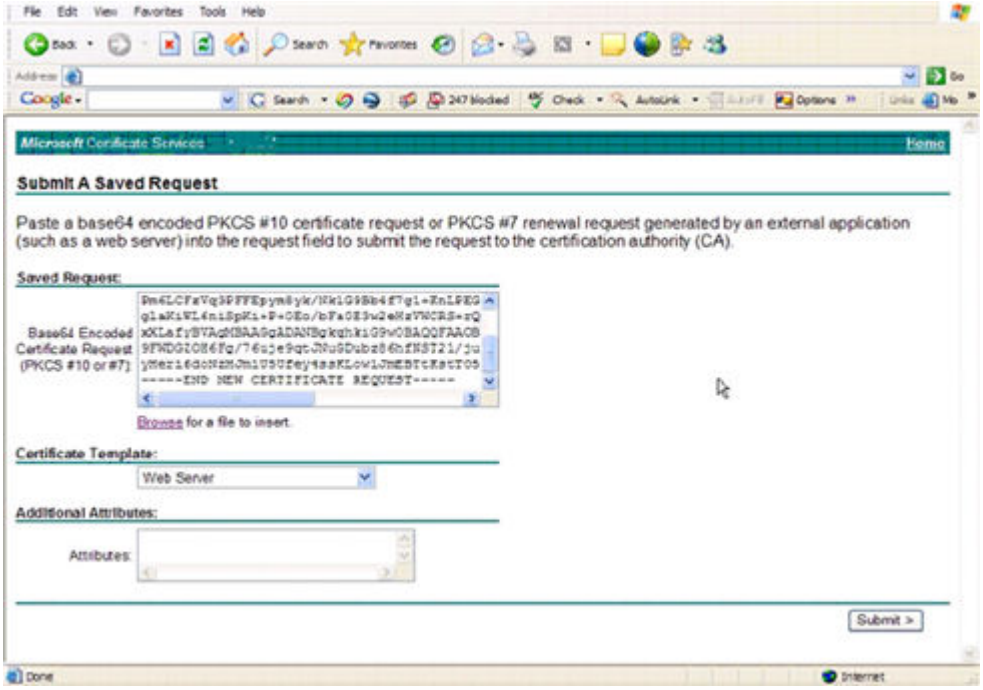
4. **base64 エンコード PKCS #10 ファイルを使用して証明書要求を送信する** オプションを選択し、**次へ** をクリックします。

高度な証明書の要求



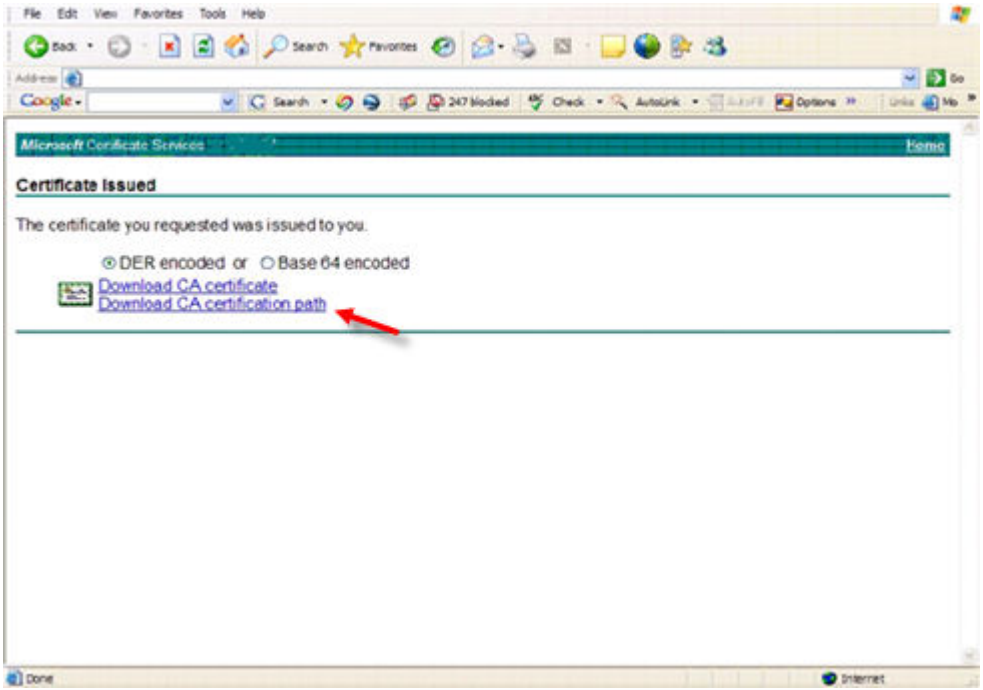
5. CSR 要求の内容をテキストボックスに貼り付けます。**Web Server** の証明書テンプレートを選択し、**送信** をクリックします。

保存した要求の送信



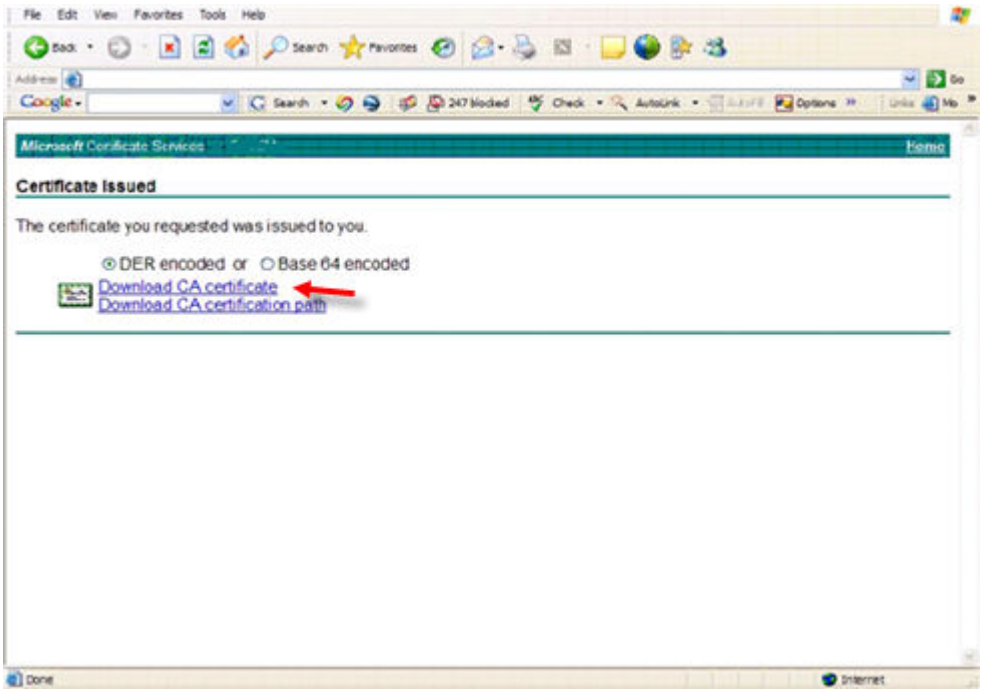
6. 証明書を保存します。**DER エンコード** を選択し、**CA 証明書のダウンロード** をクリックします。

CA 証明書のダウンロード



7. 証明書を保存します。**DER エンコード** を選択し、**CA 証明パスのダウンロード** をクリックします。

CA 証明パスのダウンロード



8. 変換された署名機関証明書をインポートします。コマンドプロンプトに戻ります。タイプ：

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9. 署名機関証明書がインポートされたので、次にサーバー証明書をインポートできます (信頼チェーンを確立できます)。タイプ：

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

自己署名証明書の別名を使用して、CSR 要求とサーバー証明書をペアにします。

10. cacerts ファイルのリストは、サーバ証明書の**証明書チェーンの長さ**が **2** であることを示しています。これは、証明書が自己署名されていないことを示します。タイプ：

```
keytool -list -v -keystore cacerts
```

チェーン内の 2 番目の証明書の証明書指紋は、インポートされた署名機関証明書です (リストのサーバー証明書の下にもリストされます)

証明書管理コンソールを使用した証明書の .PFX へのエクスポート

MMC に .crt ファイル形式の証明書がある場合は、Keytool で使用するためにその証明書を .pfx ファイルに変換する必要があります (Security Server が DMZ モードで使用されるとき、*ならびに* Dell Manager 証明書をサーバ設定ツールにインポートするとき)。

1. Microsoft 管理コンソールを開きます。
2. **ファイル** > **スナップインの追加と削除** をクリックします。
3. **追加** をクリックします。
4. *スタンドアロンスナップインの追加* ウィンドウで **証明書** を選択し、**追加** をクリックします。
5. **コンピュータアカウント** を選択し、**次へ** をクリックします。
6. *コンピュータの選*択ウィンドウで **ローカルコンピュータ (このコンソールが実行されているコンピュータ)** を選択し、**終了** をクリックします。
7. **閉じる** をクリックします。
8. **OK** をクリックします。
9. *コンソールルートフォルダ*で、*証明書 (ローカルコンピュータ)* を展開します。
10. *パーソナルフォルダ*を展開し、必要な証明書を見つけます。

11. 目的の証明書をハイライトし、**全てのタスク** > **エクスポート** を右クリックします。
12. 証明書のエクスポートウィザードが開いたら、**次へ** をクリックします。
13. **はい、秘密キーをエクスポートします** を選択し、**次へ** をクリックします。
14. **Personal Information Exchange - PKCS #12 (.PFX)** を選択してから、サブオプションの **可能な場合は証明書パスにすべての証明書を含める** と **すべての拡張プロパティをエクスポートする** を選択します。**次へ** をクリックします。
15. パスワードを入力し、確認します。ここにはどのようなパスワードを選んでも問題ありません。自分に覚えやすく、他人にはわかりにくいパスワードを選んでください。**次へ** をクリックします。
16. **参照** をクリックしてファイルを保存する場所を指定します。
17. *ファイル名* に、保存するファイルの名前を入力します。**保存** をクリックします。
18. **次へ** をクリックします。
19. **終了** をクリックします。

    正しくエクスポートされたことを知らせるメッセージが表示されます。MMC を閉じます。

SSL に非信頼証明書が使用された場合の信頼署名証明書の Security Server への追加

1. Security Server サービスが実行されている場合は停止します。
2. <Security Server install dir>\conf\ の cacerts ファイルをバックアップします。

   Keytool を使用して次の手順を実行します。

3. 信頼 PFX をテキストファイルに次の場所にエクスポートし、エイリアスを文書化します。

   ```
   keytool -list -v -keystore "
   ```

4. PFX を <Security Server install dir>\conf\ の cacerts ファイルにインポートします。

   ```
   keytool -importkeystore -v -srckeystore "
   ```

5. <Security Server install dir>\conf\application.properties で keystore.alias.signing の値を変更します。

   ```
   keystore.alias.signing=AliasNamePreviouslyDocumented
   ```

   Security Server サービスを開始します。