

Dell Security Management Server

Installation and Migration Guide v10.2.4



メモ、注意、警告

① | **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、その問題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。

© 2012-2019 Dell Inc. 無断転載を禁じます。Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian のスイートのドキュメントに使用されている登録商標および商標 (Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™) は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel ®、Pentium ®、Intel Core Inside Duo®、Itanium®、および Xeon ® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、Advanced Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、Windows Vista®、Windows 7®、Windows 10®、Azure®、Active Directory®、Access®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Outlook®、PowerPoint®、Word®、OneDrive®、SQL Server®、および Visual C++® は、米国および/またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。Dropbox SM は、Dropbox, Inc のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標です。Apple®、App StoreSM、Apple Remote Desktop™、Boot Camp™、FileVault™、iPad®、iPhone®、iPod®、iPod touch®、iPod shuffle®、および iPod nano®、Macintosh®、および Safari® は、米国およびその他の国における Google Inc. のサービスマーク、商標、または登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。iOS® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および/またはその関連会社の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連商標は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標です。Bing® は、Microsoft Inc. の登録商標です。Ask® は、IAC Publishing, LLC の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。

2019-05

Rev. A01

1 はじめに	5
Security Management Server について.....	5
Dell ProSupport へのお問い合わせ.....	5
2 要件およびアーキテクチャ	6
Security Management Server のアーキテクチャの設計.....	6
要件.....	7
Hardware.....	8
ソフトウェア.....	10
管理コンソールの言語サポート.....	12
3 インストール前の設定	13
設定.....	13
4 インストールまたはアップグレード / 移行	16
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.....	16
新規インストール.....	16
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.....	17
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.....	21
フロントエンドサーバのインストール.....	25
アップグレード / 移行.....	27
アップグレード / 移行を開始する前に.....	27
バックエンドサーバーのアップグレード / 移行.....	28
フロントエンドサーバーのアップグレード / 移行.....	31
切断モードのインストール.....	31
切断モードでの Security Management Server のインストール.....	34
Security Management Server のアンインストール.....	34
5 インストール後の設定	35
DMZ モードの設定.....	35
サーバー設定ツール.....	35
新規またはアップデートされた証明書の追加.....	36
Dell Manager 証明書のインポート.....	38
SSL/TLS 証明書のベータ版のインポート.....	39
サーバ SSL 証明書の設定.....	39
SMTP 設定の構成.....	40
データベース名、場所、または資格情報の変更.....	40
データベースの移行.....	41
6 管理作業	43
Dell 管理者役割の割り当て.....	43
Dell 管理者役割でのログイン.....	43
クライアントアクセスライセンスのアップロード.....	43

ポリシーのコミット.....	43
Dell Compliance Reporter の設定.....	44
バックアップの実行.....	44
Security Management Server バックアップ.....	44
SQL Server のバックアップ.....	44
PostgreSQL Server のバックアップ.....	44
7 ポート.....	45
8 SQL Server ベストプラクティス.....	47
9 証明書.....	48
自己署名証明書の作成と証明書署名要求の生成.....	48
新しいキーペアと自己署名証明書の生成.....	48
証明機関からの署名付き証明書の要求.....	49
ルート証明書のインポート.....	50
証明書の要求方法の例.....	50
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.....	51
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.....	52

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。

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 のアーキテクチャの設計

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian の各ソリューションは非常に拡張性の高い製品で、組織内の暗号化を目的とした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

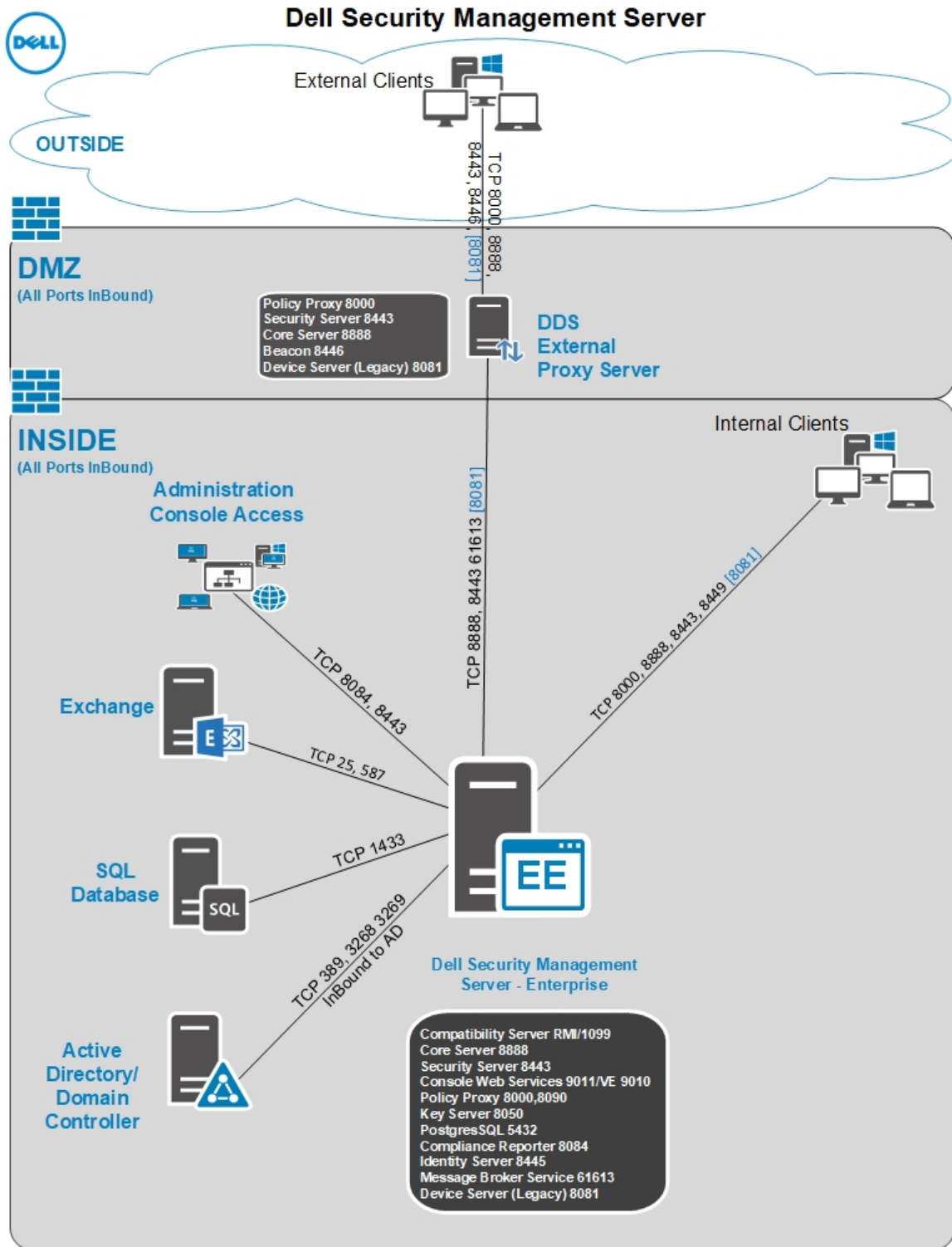
- オペレーティング システム：Windows Server 2012 R2（Standard、Datacenter 64 ビット）、Windows Server 2016（Standard、Datacenter 64 ビット）、Windows Server 2019（Standard、Datacenter）
- 仮想 / 物理マシン
- CPU：2 コア
- RAM：8.00 GB
- ドライブ C：ログ用に空きディスク容量 20 GB

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。



① | **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。

Hardware

The following table details the *minimum* hardware requirements for Security Management Server see [Security Management Server Architecture Design](#) for additional information about scaling based on the size of your deployment.

Hardware Requirements

Processor

Modern Quad-Core CPU (1.5 GHz+)

RAM

16GB

Free Disk Space

20GB of free disk space

 | **NOTE: Up to 10GB may be consumed for a local event database stored within PostgreSQL**

Network Card

10/100/1000 or better

Miscellaneous

IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

The following table details the *minimum* hardware requirements for a Security Management Server Front - End / Proxy Server.

Hardware Requirements

Processor

Modern Dual-Core CPU

RAM

8GB

Free Disk Space

20GB of free disk space for log files

Network Card

10/100/1000 or better

Miscellaneous

IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

Virtualization

The Security Management Server can be installed in a virtual environment. Only the following environments are recommended.

Security Management Server v10.2.4 has been validated on the following platforms.

Hyper-V Server installed as a Full or Core installation or as a role in Windows Server 2012, Windows Server 2016, or Windows Server 2019.

- Hyper-V Server
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended
 - Hardware must conform to minimum Hyper-V requirements
 - 4 GB minimum RAM for dedicated image resource
 - Must be run as a Generation 1 Virtual Machine
 - See <https://technet.microsoft.com/en-us/library/hh923062.aspx> for more information

Security Management Server v10.2.4 has been validated with VMware ESXi 5.5, VMware ESXi 6.0, and VMware ESXi 6.5.

NOTE: When running VMware ESXi and Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019, VMXNET3 Ethernet Adapters are recommended.

- VMware ESXi 5.5
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended
 - See <http://www.vmware.com/resources/compatibility/search.php> for a complete list of supported Host Operating Systems
 - Hardware must conform to minimum VMware requirements
 - 4 GB minimum RAM for dedicated image resource
 - See <http://pubs.vmware.com/vsphere-55/index.jsp> for more information
- VMware ESXi 6.0
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended
 - See <http://www.vmware.com/resources/compatibility/search.php> for a complete list of supported Host Operating Systems
 - Hardware must conform to minimum VMware requirements
 - 4 GB minimum RAM for dedicated image resource
 - See <http://pubs.vmware.com/vsphere-60/index.jsp> for more information
- VMware ESXi 6.5
 - 64-bit x86 CPU required
 - Host computer with at least two cores
 - 8 GB RAM minimum recommended
 - See <http://www.vmware.com/resources/compatibility/search.php> for a complete list of supported Host Operating Systems
 - Hardware must conform to minimum VMware requirements
 - 4 GB minimum RAM for dedicated image resource
 - See <http://pubs.vmware.com/vsphere-65/index.jsp> for more information

NOTE: The SQL Server database hosting the Security Management Server must be run on a separate computer for performance reasons.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run on a redundant system, such as a SQL Cluster, to ensure availability and data continuity. It is also recommended to perform daily full backups with transactional logging enabled to ensure that any newly generated keys through user/device activation are recoverable.

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。

- ① **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 を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、ロールと権限が制限されたアプリケーションサーバ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。たとえば、Security Management Server を特権インフラストラクチャサーバ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。
- ① **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を再起動する必要があります。
- ① **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
- ① **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、インストーラが自動でインストールします。
- **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、インストーラが自動でインストールします。
- **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、インストーラが自動でインストールします。
- **.NET Framework バージョン 3.5 SP1**
- **.NET Framework バージョン 4.5**
Microsoft は、.NET Framework バージョン 4.5 のセキュリティアップデートを公開しました。
- **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、インストーラが自動でインストールします。

Security Management Server - バックエンドサーバおよびデルフロントエンドサーバ

- **Windows Server 2012 R2**
 - Standard Edition
 - Datacenter Edition
- **Windows Server 2016**
 - Standard Edition
 - Datacenter Edition
- **Windows Server 2019**
 - Standard Edition
 - Datacenter Edition

LDAP リポジトリ

- Active Directory 2008 R2
- Active Directory 2012 R2
- Active Directory 2016

管理コンソールおよび Compliance Reporter

- Internet Explorer 11.x 以降
- Mozilla Firefox 41.x 以降
- Google Chrome 46.x 以降

① | 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。

① | 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 2008 R2** - Standard Edition / Enterprise Edition
- **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

① | 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。

① | 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には、ローカル管理者権限が必要です。Dell Security Management Server の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
バックエンド	新規インストール	新しいログインの作成	securityadmin
バックエンド	アンインストール	該当なし	該当なし

タイプ	アクション	シナリオ	必要な SQL 特権
プロキシのフロントエンド	任意	該当なし	該当なし

① **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および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。

こうした権限は、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を確認してください。

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ーフェイス (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	

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

- 1 有効な場合は、Internet Explorer セキュリティ強化の構成 (ESC) を無効にします。ブラウザのセキュリティオプションで、デルサーバの URL を信頼済みサイトに追加します。サーバを再起動します。
- 2 各コンポーネントの次のポートを開きます。

内部：

Active Directory 通信：TCP/389

電子メール通信 (オプション)：25

対フロントエンド (必要な場合)：

外部ポリシープロキシからメッセージブローカへの通信：STOMP/61613

バックエンドセキュリティサーバへの通信：HTTPS/8443

バックエンドコアサーバへの通信：HTTPS/8888

RMI ポートへの通信 - 1099

バックエンドデバイスサーバへの通信：HTTP(S)/8443 - Security Management Server が v7.7 以降の場合。お使いの Dell Server が v7.7 より前の場合は、HTTP (HTTPS) /8081 です。

ビーコンサーバ：HTTP/8446 (Data Guardian を使用している場合)

外部 (必要な場合)：

SQL データベース：TCP/1433

管理コンソール：HTTPS/8443

LDAP：TCP/389/636 (ローカルドメインコントローラ)、TCP/3268/3269 (グローバルカタログ)、TCP/135/49125+ (RPC)

互換サーバ：TCP/1099

Compliance Reporter：HTTP(S)/8084 (インストール時に自動的に設定)

ID サーバ：HTTPS/8445

コアサーバ：HTTPS/8888 (8888 はインストール時に自動的に設定)

デバイスサーバ : HTTP(S)/8443 (Security Management Server v7.7 以降) または HTTP(S)/8081 (v7.7 より前の Dell Server)

キーサーバ : TCP/8050

ポリシープロキシ : TCP/8000

セキュリティサーバ : HTTPS/8443

クライアントの認証 : HTTPS/8449 (サーバ暗号化を使用している場合)

Advanced Threat Prevention を使用している場合、クライアント通信 : HTTPS/TCP/443

デルサーバのデータベースの作成

- 3 次の手順はオプションです。データベースがまだない場合、インストーラがデータベースを 1 つ作成します。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、以下の指示に従って SQL Management Studio で SQL データベースおよび SQL ユーザーを作成してください。

Security Management Server をインストールする際は、「**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**」の手順に従ってください。

Security Management Server は、SQL 認証および Windows 認証の両方に対応しています。デフォルトの認証方法は SQL 認証です。

データベースを作成してから、db_owner 権限を持つ Dell データベースユーザーを作成します。db_owner では、許可の割り当て、データベースのバックアップと復元、オブジェクトの作成と削除、ユーザーアカウントと役割の制限なしでの管理が可能です。また、このユーザーがゲストアドプロシージャを実行する許可 / 権限を持っていることを確認します。

デフォルト以外の SQL Server インスタンスを使用するときは、Security Management Server をインストールした後、サーバ設定ツールのデータベース タブで、そのインスタンスの動的ポートを指定する必要があります。詳細については、「**サーバー設定ツール**」を参照してください。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](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx) を参照してください。

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。

SQL データベースおよび SQL ユーザーを SQL Management Studio で作成するには、以下を 1 つ選びます。

Visual C++ 2010/2013/2015 再頒布可能パッケージのインストール

- 4 Visual C++ 2010、2013、および 2015 再頒布可能パッケージをインストールしていない場合はインストールします。必要な場合は、Security Management Server インストーラにこれらのコンポーネントのインストールを許可できます。

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

- 5 .NET Framework 4.5 をインストールしていない場合はインストールします。

Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 - <https://www.microsoft.com/en-us/download/details.aspx?id=30653>

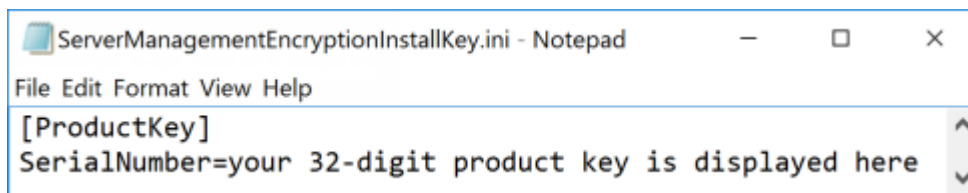
SQL Native Client 2012 のインストール

- 6 SQL Server 2012 または SQL Server 2016 を使用している場合は、SQL Native Client 2012 をインストールします。必要な場合は、Security Management Server インストーラにこのコンポーネントのインストールを許可できます。

<http://www.microsoft.com/en-us/download/details.aspx?id=35580>

オプション

- 7 **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。



サーバーのインストール前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。

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。

Server 2016 でのインストール時間を短縮するには、次の除外を Windows Defender に追加します。

- C:\Program Files\Dell\Enterprise Edition
- C:\Windows\Installer
- インストーラの実行元であるファイルのパスです。

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\\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 に問い合わせサポートを受けてください。

① 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。

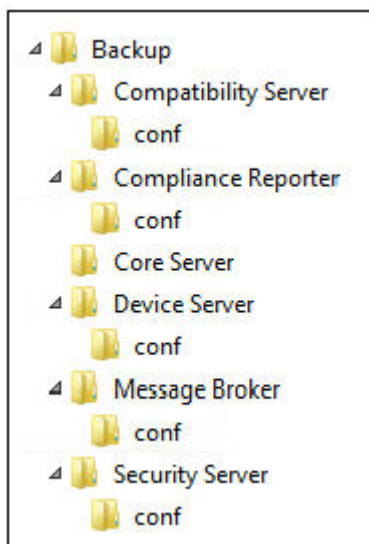
- [フロントエンドサーバのインストール](#) - バックエンドサーバと通信するようにフロントエンドサーバをインストールします。

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。

① **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。

① | 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。

① | 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。

① **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。

① **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。

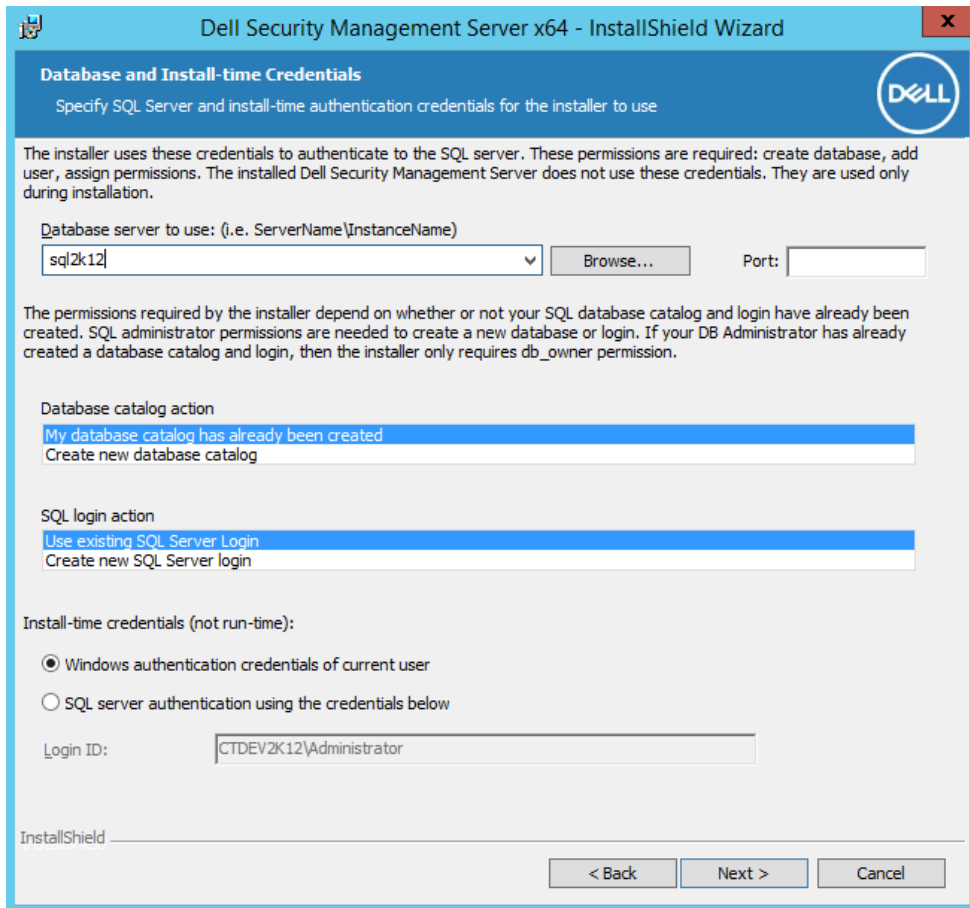
- 13 バックエンドサーバーインストール設定ダイアログから、ホスト名とポートを表示または編集できます。
- デフォルトのホスト名とポートを使用する場合は、バックエンドサーバーインストール設定 ダイアログで、**次へ** をクリックします。
 - フロントエンドサーバを使用している場合は、**ネットワークのクライアントとの内部通信、または DMZ のクライアントとの外部通信のために、フロントエンドと連携**を選択し、フロントエンドのセキュリティサーバのホスト名を入力します (server.domain.com など)。
 - ホスト名を表示または編集するには、**ホスト名の編集** をクリック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

① **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。

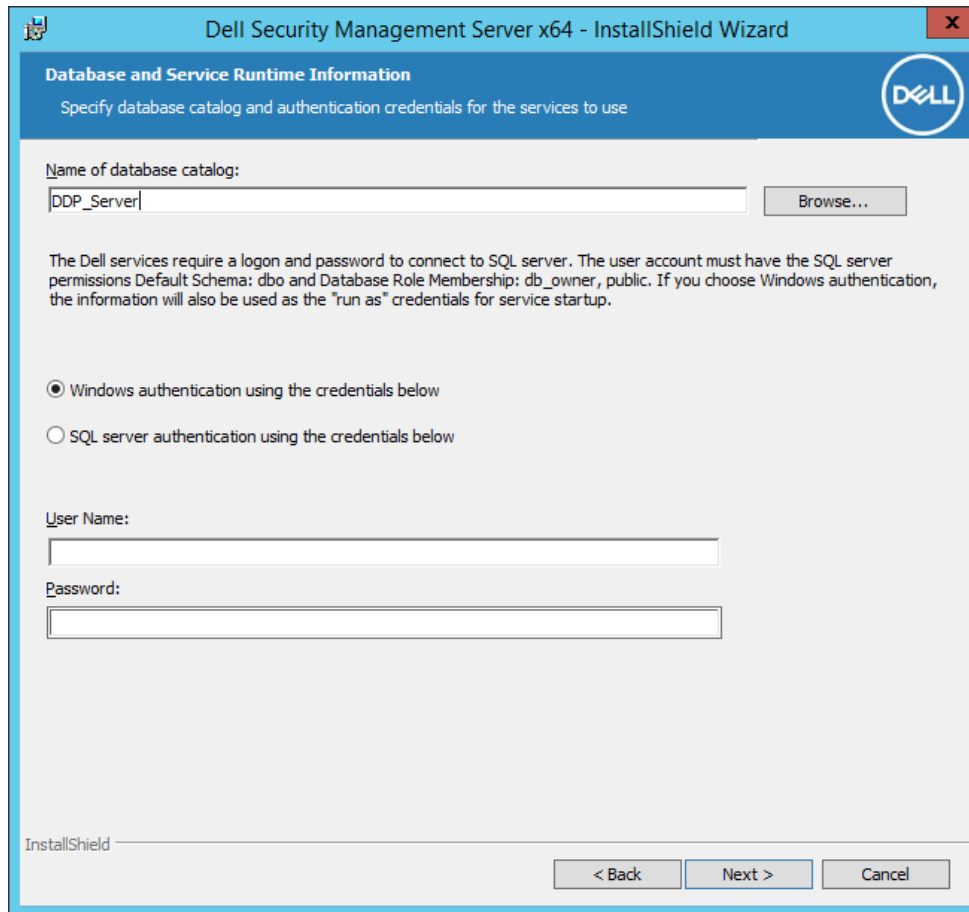
15 製品が使用するための認証メソッドを選択します。このステップによりアカウントと製品が関連付けられます。

- **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のインストール

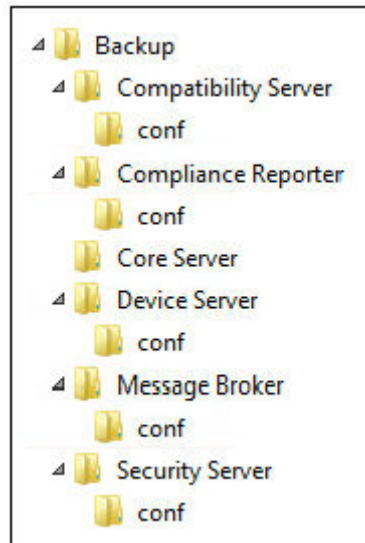
① メモ:

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。

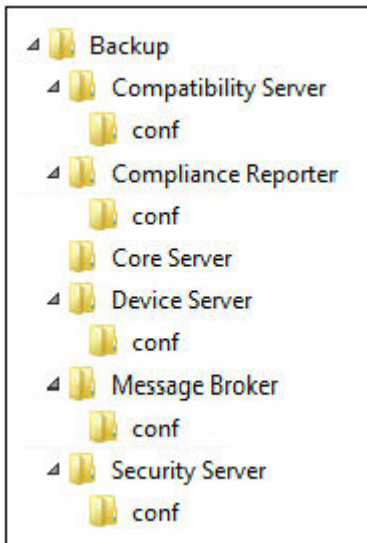
既存のデータベースが Security Management Server で事前にインストールされている場合は、インストールを開始する前に、データベース、設定ファイルおよび secretKeyStore がバックアップされていること、Security Management Server をインストールするサーバからアクセス可能であることを確認します。これらのファイルは、Security Management Server および既存のデータベースを設定するときに必要なになります。インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



- 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使用する情報全体の中でも重要な要素です。

① **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。

① | **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。

① | **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。

- ① **メモ:** このインストールでは、Data Guardian コールバックビーコンをサポートするためのビーコンサービスがインストールされます。これにより、環境内で保護対象 Office ドキュメントを許可または行使する際に、Data Guardian のすべての保護対象ファイルにコールバックビーコンが挿入されます。その結果、任意の場所にある任意のデバイスとフロントエンドサーバの間で通信が可能になります。コールバックビーコンを使用する前に、必要なネットワークセキュリティが設定されていることを確認します。

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。

① | 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。

① | 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：セキュリティ）

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。

① | 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。

① | 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 v9.x は以下をサポートします。

- Encryption Enterprise :
 - Windows クライアント v7.x/8.x
 - Mac クライアント v7.x/8.x
 - SED クライアント v8.x
 - Authentication v8.x
 - BitLocker Manager v7.2x+ および v8.x
 - Data Guardian v1.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprise v1.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** をクリックします。
- 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。

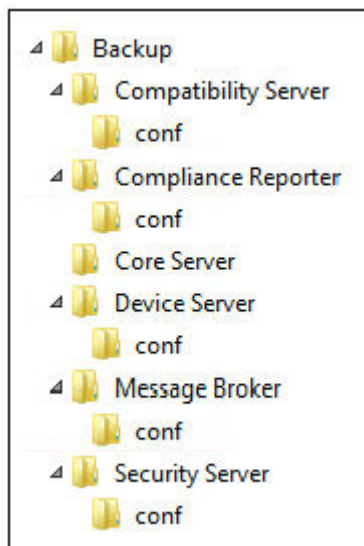
- 6 Windows のスタートメニューから、**スタート > ファイル名を指定して実行** をクリックします。`services.msc` と入力し、**OK** をクリックします。サービスが開いたら、各 Dell サービスに移動し、必要に応じて、**サービスの開始** をクリックします。

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。

① 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。

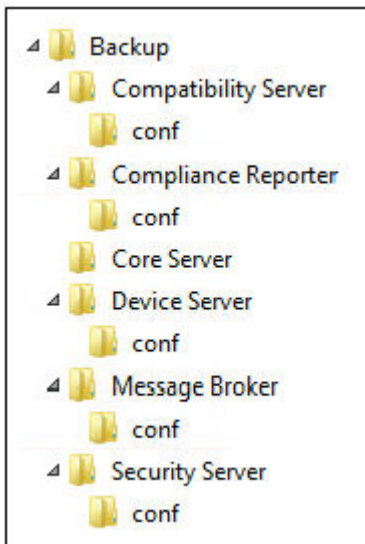


バックエンドサーバーのアップグレード / 移行

- 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。

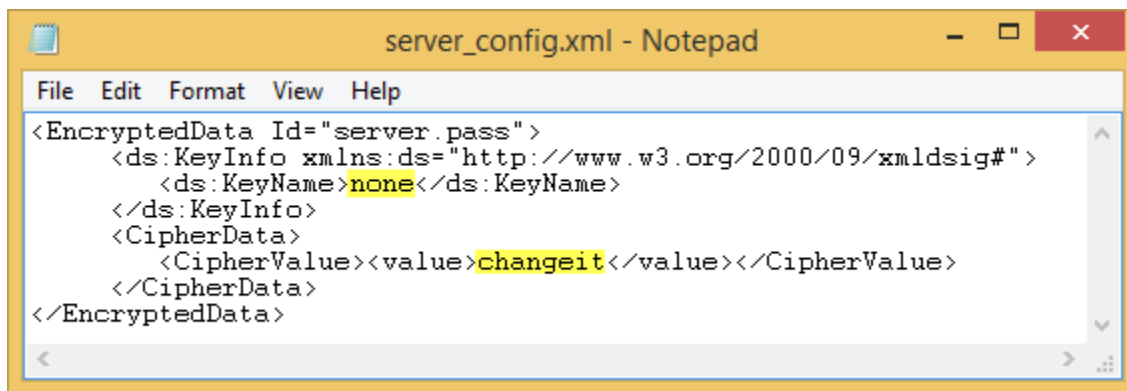
- 12 バックアップされたインストールで、<Compatibility Server install dir>\conf\secretKeyStore を新しいインストールにコピー / 貼り付けします。
<Compatibility Server install dir>\conf\secretKeyStore に貼り付けます。
- 13 新しいインストールで、<Compatibility Server install dir>\conf\server_config.xml を開き、次のように、**server.pass** 値を、バックアップした <Compatibility Server 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。

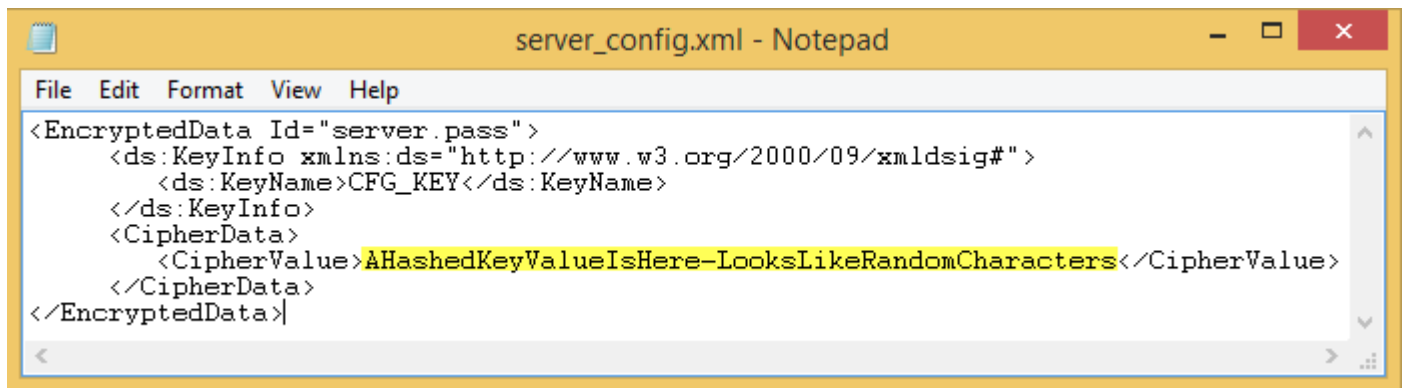
既知のパスワード



```
server_config.xml - Notepad
File Edit Format View Help
<EncryptedData Id="server.pass">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>none</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue><value>changeit</value></CipherValue>
  </CipherData>
</EncryptedData>
```

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



```
server_config.xml - Notepad
File Edit Format View Help
<EncryptedData Id="server.pass">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>CFG_KEY</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue>AHashedKeyValueIsHere-LooksLikeRandomCharacters</CipherValue>
  </CipherData>
</EncryptedData>
```

ファイルを保存して閉じます。

① 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 **メモ:** v9.5 で開始すると、ビーコンサービスはデフォルトのホスト名とポート 8446 を使用して、このアップグレードの一部としてインストールされます。ビーコンサービスは、その環境内で保護 Office ドキュメントを許可または行使する際に、Data Guardian によって保護されるすべてのファイルにコールバックビーコンを挿入する Data Guardian コールバックビーコンをサポートします。その結果、任意の場所にある任意のデバイスとフロントエンドサーバの間で通信が可能になります。コールバックビーコンを使用する前に、必要なネットワークセキュリティが設定されていることを確認します。

- 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 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がフロントエンドサーバと通信するように設定します。
 - a バックエンドサーバで、<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

オプション

意味

/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。

① | 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

パラメータ

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。

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。

- ① **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。

- ① **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。

- ① **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。

パラメータ

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。

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。

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 (<textthere>)`

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 (<textthere>)`
- 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。

① 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
- Data Guardian または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、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、パイロットや POC などに適しています。実稼働環境では、デルは、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を推奨します。
- **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。パブリック認証機関（CA）により署名された証明書の場合は、通常、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）
- 起動前認証用を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。これらの種類の接続の場合は、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。

- 起動前認証用を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。
- 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、デルは、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を推奨します。
- **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。

証明書のセットアップが完了しました。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。

証明書のセットアップが完了しました。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て、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、**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ず（オプション **現在の設定の使用** 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て、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、**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。

これで証明書のセットアップが完了しました。

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。

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。

① **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

サーバ設定ツールで、**SMTP** タブをクリックします。

このタブでは、Data Guardian、製品情報、通知、および Advanced Threat Prevention の Threat Relay メッセージの SMTP 設定を構成します。

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、真 または 偽 のいずれかを選択します。

① **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](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。

① 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](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。

① **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。

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ーでそのユーザーの 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 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、「<https://www.postgresql.org/docs/9.5/static/backup.html>」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。

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
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。
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) が必要です。
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、Data Guardian、SED-PBA 通信、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。
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。
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バスを提供します。

名前	デフォルトポート	説明
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)	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。
	TCP/ 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리케이션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
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。
コールバックビーン	HTTP/TCP 8446	Data Guardian の保護付き Office モードを実行するときに、コールバックビーンが保護付きの各 Office ファイルに挿入されることを許可します。

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、「Understanding Pages and Extents」（ページとエクステントについて）を検索してください。

- Microsoft SQL Server 2008 R2 - [http://technet.microsoft.com/en-us/library/ms190969\(v=sql.105\).aspx](http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx)

- 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「Server Memory Server Configuration Options」（サーバメモリに関するサーバ設定オプション）を検索してください。

- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29>
- Microsoft SQL Server 2012 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.110\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.110))
- Microsoft SQL Server 2014 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.120\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.120))
- Microsoft SQL Server 2016 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.130\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.130))
- Microsoft SQL Server 2017 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.130\)](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、「Trace Flags (Transact-SQL)」（トレースフラグ (Transact-SQL)）を検索してください。

- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29>
- 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。

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-server-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いない変更に関連する問題が、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。

- キースタアのパスワード：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タ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。

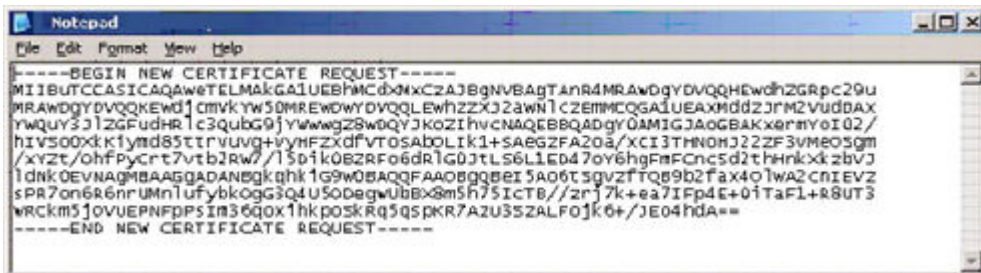
- 1 <certificatealias> で以前に使用した値と同じ値を代入します。

```
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。

- 署名付き証明書を受信したら、ファイルに保存します。
- 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。

- 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。
- 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)。
- 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。

- 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。
- 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

- 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

- 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

- 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。