AUTHORIZED DOCUMENTATION

インストールガイド

January 5, 2009

Novell®
ZENworks® Endpoint Security Management

3.5

www.novell.com

保証と著作権

米国 Novell, Inc., およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っていません。また文書の商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc. およびノベル株式会社は、本書の内容を改訂または変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような改訂または変更を個人または事業体に通知する義務を負いません。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。またノベル製ソフトウェアの商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc., およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、すべての輸出規制を遵守して、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出については、「Novell International Trade Services (http://www.novell.com/info/exports/)」の Web ページをご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

米国 Novell, Inc., およびノベル株式会社は、本文書に記載されている製品に実装されている技術に関する知的所有権を保有します。。これらの知的所有権は、「Novell Legal Patents (http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、Novell Documentation の Web ページ (http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて 7

1 ZENworks Endpoint Security Management 概要 9

1.1 システム要件 . . . 10
1.2 『ZENworks Endpoint Security Management マニュアル』について . . . 11

2 ZENworks Endpoint Security Management のインストール 13

2.1 インストール前の注意事項 . . . 13
2.2 インストールパッケージ . . . 13
2.2.1 マスタインストーラプログラムについて . . . 13
2.3 インストールオプション . . . 14
2.4 インストールの順序 . . . 14
2.5 ZENworks Endpoint Security Management をインストールする前に . . . 14

3 シングルサーバインストールの実行 17

3.1 インストール手順 . . . 19
3.2 サービスの起動 . . . 19

4 マルチサーバインストールの実行 21

5 ポリシー配布サービスのインストール 23

5.1 インストール手順 . . . 25
5.1.1 標準インストール . . . 26
5.1.2 カスタムインストール . . . 28
5.2 サービスの起動 . . . 31

6 管理サービスのインストール 33

6.1 インストール手順 . . . 34
6.1.1 標準インストール . . . 35
6.1.2 カスタムインストール . . . 39
6.2 サービスの起動 . . . 43

7 管理コンソールのインストール 45

7.1 インストール手順 . . . 45
7.1.1 標準インストール . . . 46
7.1.2 カスタムインストール . . . 46
7.2 コンソールの起動 . . . 48
7.2.1 eDirectory サービスの追加 . . . 49
7.2.2 管理コンソールの許可設定 . . . 50
7.2.3 ポリシーの公開 . . . 54
7.3 USB リーダのインストール . . . 55

8 クライアントロケーション保証サービスのインストール 57

8.1 インストール手順 58
8.2 CLAS のフェイルオーバインストール 59
8.3 管理サービスへの公開鍵の転送 59

9 Endpoint Security Client 3.5 のインストール 61

9.1 Endpoint Security Client 3.5 の基本インストール. 61
9.2 MSI のインストール 63
9.2.1 コマンドライン変数 66
9.2.2 MSI パッケージによるポリシーの配布 68
9.2.3 ユーザによる Endpoint Security Client 3.5 の MSI インストール 68
9.3 Endpoint Security Client 3.5 の実行. 69

10 ZENworks Endpoint Security Client 4.0 のインストール 71

10.1 Endpoint Security Client 4.0 の基本インストール. 71
10.2 MSI のインストール 74
10.2.1 マスタインストーラの使用 75
10.2.2 Setup.exe ファイルの使用 75
10.2.3 インストールの完了 75
10.2.4 コマンドライン変数 77
10.2.5 MSI パッケージによるポリシーの配布 78
10.3 Endpoint Security Client 4.0 の実行. 78
10.4 Endpoint Security Client 4.0 で未対応の機能. 78

11 非管理対象モードでの ZENworks Endpoint Security Management のインストール 81

11.1 非管理対象の Endpoint Security Client のインストール 81
11.2 スタンドアロン管理コンソ ??. 82
11.3 管理されていないポリシーの配布 82

A マニュアルの更新 83

A.1 2009 年 1 月 5 日. 83

このガイドについて

この『*Novell® ZENworks® Endpoint Security Management インストールガイド*』では、ZENworks Endpoint Security Management コンポーネントのインストール方法、設定方法、および使用方法について、管理者を対象に詳しく説明します。

このガイドの情報は、以下のように構成されます。

- 9 ページの第 1 章「ZENworks Endpoint Security Management 概要」
- 13 ページの第 2 章「ZENworks Endpoint Security Management のインストール」
- 17 ページの第 3 章「シングルサーバインストールの実行」
- 21 ページの第 4 章「マルチサーバインストールの実行」
- 23 ページの第 5 章「ポリシー配布サービスのインストール」
- 33 ページの第 6 章「管理サービスのインストール」
- 45 ページの第 7 章「管理コンソールのインストール」
- 57 ページの第 8 章「クライアントロケーション保証サービスのインストール」
- 61 ページの第 9 章「Endpoint Security Client 3.5 のインストール」
- 71 ページの第 10 章「ZENworks Endpoint Security Client 4.0 のインストール」
- 81 ページの第 11 章「非管理対象モードでの ZENworks Endpoint Security Management のインストール」

対象読者

このガイドは、ZENworks Endpoint Security Management の管理者を対象に作成されています。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか、または Novell Documentation Feedback サイト (http://www.novell.com/documentation/feedback.html) にアクセスして、ご意見をお寄せください。

追加のマニュアル

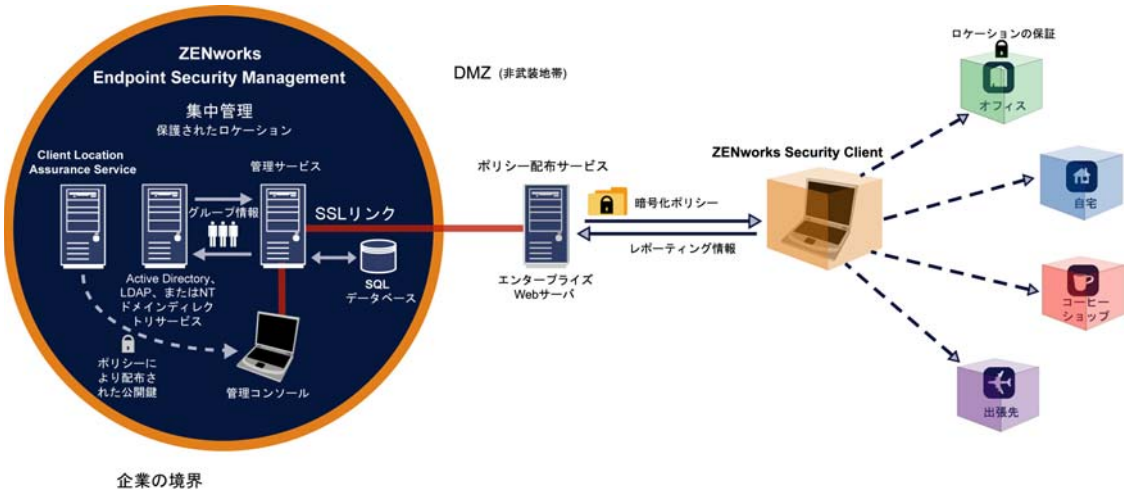
ZENworks Endpoint Security Management には、製品について学習したり、製品を実装したりするために使用できる、その他のマニュアル (PDF 形式および HTML 形式の両方) も用意されています。追加のマニュアルについては、ZENworks Endpoint Security Management 3.5 マニュアルの Web サイト (http://www.novell.com/documentation/zesm35) を参照してください。

ZENworks Endpoint Security Management 概要

1

Novell® ZENworks® Endpoint Security Management は、ポリシー配布サービス、管理サービス、管理コンソール、クライアントロケーション保証サービス、Endpoint Security Client という 5 つの大きな機能コンポーネントで構成されています。次の図は、アーキテクチャにおけるこれらのコンポーネントを示しています。

図 1-1 ZENworks Endpoint Security Management のアーキテクチャ



Endpoint Security Client は、エンドポイントシステムに配布されたセキュリティポリシーを実行します。Endpoint Security Client が企業のすべての PC にインストールされている場合、これらのエンドポイントが企業の境界を越えて外部に移動してもセキュリティを保持できます。その一方で、境界の内部のエンドポイントには境界ファイアウォール内でさらにセキュリティチェックが行われます。

それぞれの集中管理コンポーネントは個別にインストールされます (シングルサーバインストールの場合は例外です)。詳細については、17 ページの第 3 章「シングルサーバインストールの実行」を参照してください。

企業の境界の内部にあるセキュリティで保護されたサーバに、次のコンポーネントがインストールされます。

- **ポリシー配布サービス :** Endpoint Security Client にセキュリティポリシーを配布したり、Endpoint Security Client からレポーティングデータを取得したりします。ポリシー配布サービスを企業ファイアウォールの外部にある DMZ に展開して、モバイルエンドポイントに対する定期的なポリシー更新を確実に行うことができます。
- **管理サービス :** ユーザポリシーの割り当てとコンポーネントの認証、レポーティングデータの取得、ZENworks Endpoint Security Management レポートの作成と配布、セキュリティポリシーの作成と格納を行います。

- **管理コンソール :** 管理サービスをホストするサーバで、または管理サービスサーバに接続された企業ファイアウォール内のワークステーションで直接実行される、可視ユーザインタフェースです。管理コンソールは、管理サービスの環境設定、およびユーザとグループのセキュリティポリシーの作成と管理の両方に使用します。ポリシーの作成、コピー、編集、配布、削除には、管理コンソールを使用します。
- **クライアントロケーション保証サービス :** Endpoint Security Client がインストールされたデバイスが他の既存のネットワーク環境パラメータの示す場所に実際に存在することを暗号的な面から保証します。

1.1 システム要件

サーバのシステム要件	Endpoint (Client) のシステム要件
オペレーティングシステム : Microsoft&thrdmrk; Windows&thrdmrk; 2000 Server SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server **プロセッサ :** 3.0 GHz Pentium&thrdmrk; 4 HT (またはそれ以上) 756 MB RAM 以上 (1GB 以上を推奨) **ディスク容量 :** 500MB : ローカルの Microsoft SQL データベースがない場合 5GB : ローカルの MS SQL データベースがある場合 (SCSI を推奨) **必要なソフトウェア :** サポートされる RDBMS (SQL Server Standard、SQL Server Enterprise、Microsoft SQL Server 2000 SP4、SQL 2005) Microsoft Internet Information Services (SSL 用に構成) サポートされるディレクトリサービス (eDirectory™ または Active Directory&thrdmrk;) .NET Framework 3.5 (サーバおよび管理コンソール専用) **スタンドアロン管理コンソール :** サポートされる RDBMS (SQL Server Standard、SQL Server Enterprise、Microsoft SQL Server 2000 SP4、SQL 2005、SQL Express)	**オペレーティングシステム :** Windows XP SP1 Windows XP SP2 Windows 2000 SP4 Windows Vista SP1 (32 ビット) Windows Server 2008 (32 ビット) **プロセッサ :** 600MHz Pentium 3 (またはそれ以上) 最低 128MB の RAM (256MB 以上を推奨) **ディスク容量 :** 5MB が必要。レポーティングデータ用にさらに 5MB を推奨 **必要なソフトウェア :** Windows 3.1 インストーラ すべての Windows 更新プログラムが最新の状態であること

ポリシー配布サービス、管理サービス、およびクライアントロケーション保証サービスでは、ASP.NET 2.0 用のローカルアカウントが有効になっている必要があります。このアカウントが無効になっていると、サービスが正しく機能しません。

1.2 『ZENworks Endpoint Security Management マニュアル』について

ZENworks Endpoint Security Management マニュアルには、製品のユーザに向けた 3 つのレベルのガイダンスがあります。

- 『*ESM インストールガイド*』: このガイドでは、ZENworks Endpoint Security Management コンポーネントのインストール方法、設定方法、および使用方法について、管理者を対象に詳しく説明します。現在お読みいただいているのがこのガイドです。
- 『*ZENworks Endpoint Security Management 管理ガイド*』: このガイドの対象読者は、サービスの管理、企業のセキュリティポリシーの作成、レポーティングデータの生成と分析、ユーザのトラブルシューティングを行う、ZENworks Endpoint Security Management の管理者です。このマニュアルには、これらのタスクを完了するための手順が記載されています。
- 『*ZENworks Endpoint Security Client 3.5 ユーザガイド*』: このガイドではユーザを対象に、Endpoint Security Client の操作方法を説明します。このガイドを企業内のすべての従業員に配布することで、Endpoint Security Client の使用方法についての理解を深めることができます。

ZENworks Endpoint Security Management のインストール

2

以下の項では、Novell® ZENworks® Endpoint Security Management のインストールについてさらに詳しく説明します。

- 13 ページのセクション 2.1「インストール前の注意事項」
- 13 ページのセクション 2.2「インストールパッケージ」
- 14 ページのセクション 2.3「インストールオプション」
- 14 ページのセクション 2.4「インストールの順序」
- 14 ページのセクション 2.5「ZENworks Endpoint Security Management をインストールする前に」

2.1 インストール前の注意事項

ZENworks Endpoint Security Management インストールソフトウェアは、改ざんまたは不正使用を防ぐために、物理的に保護する必要があります。同様に、管理者はプリインストールおよびインストールについてガイドラインをよく読み、ZENworks Endpoint Security Management システムが中断されることなく機能するように配慮し、あるいは不十分なハードウェア保護によって脆弱性が発生することのないよう注意する必要があります。

このソフトウェアをインストールする管理者は、サーバおよびドメインのプライマリ管理者でなければなりません。エンタープライズ SSL 証明書を使用する場合は、SSL ルートセキュリティ証明書の作成に使用したユーザ名と同じユーザ名を使用する必要があります。

2.2 インストールパッケージ

DVD からインストールする場合、マスタインストーラプログラムが起動され、わかりやすいユーザインタフェースで ZENworks Endpoint Security Management の管理者にインストールプロセスを案内します。それぞれのマシンでインストール DVD をロードし、マスタインストーラプログラムにアクセスして必要なコンポーネントをインストールしてください。

2.2.1 マスタインストーラプログラムについて

マスタインストーラプログラムを起動すると、［*Products (製品)*］と［*Documentation (マニュアル)*］という 2 つのメニューオプションが表示されます。

［*Products (製品)*］リンクをクリックすると、インストールメニューが開きます。この画面のメニュー項目から、指定した各コンポーネントのインストーラを起動できます。Endpoint Security Client 3.5 または Endpoint Security Client 4.0 では、インストールを管理者モードで開始できる追加オプションを利用できます。これにより、ZENworks Endpoint Security Management 管理者は、MSI パッケージを作成して簡単に配布を行うことができます (63 ページの第 9.2 章「MSI のインストール」を参照)。

ZENworks Endpoint Security Management コンポーネントの操作の詳細については、［*Documentation (マニュアル)*］リンクにアクセスして『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

2.3 インストールオプション

ZENworks Endpoint Security Management バックエンドコンポーネントは、シングルサーバインストールまたはマルチサーバインストールのどちらでもインストールできます。シングルサーバインストールは、定期的なポリシー更新を必要としない、小規模な展開に適しています。マルチサーバインストールは、定期的なポリシー更新を必要とする、大規模な展開に適しています。適切なインストールのタイプを判断するには、Novell Professional Services (Novell プロフェッショナルサービス) にお問い合わせください。

Endpoint Security Client は、必要に応じて、ポリシー配布サービスに接続しなくても機能するようにできます。同様に、必要に応じて、スタンドアロン管理コンソールを評価目的でインストールすることもできます。この非管理モードのインストール方法については、81 ページの第 11 章「非管理対象モードでの ZENworks Endpoint Security Management のインストール」で説明します。

2.4 インストールの順序

ZENworks Endpoint Security Management は以下の順序でインストールする必要があります。

1. シングルサーバインストールまたはマルチサーバインストール
   - ポリシー配布サービス
   - 管理サービス
2. 管理コンソール
3. クライアントロケーション保証サービス
4. Endpoint Security Client 3.5 または Endpoint Security Client 4.0

2.5 ZENworks Endpoint Security Management をインストールする前に

インストールの前に ZENworks Endpoint Security Management 管理者は次のような問題を考慮する必要があります。

ユーザが ZENworks Endpoint Security Management のセキュリティポリシーを受信する方法

ポリシー配布センターでは、ユーザがポリシーの更新を中央ネットワークの外部を含めどこでも受け取ることができるようにするか、あるいはセキュリティで保護されたネットワーク内にいる (または VPN を通じて接続している) 場合に限り受け取ることができるようにするかを選択することができます。ZENworks Endpoint Security Management のセキュリティポリシーを頻繁に更新する予定がある組織の場合は、DMZ の外側にある Web サーバにポリシー配布サービスを配置するマルチサーバインストールをお勧めします。

利用可能なサーバ展開のタイプ

少数のサーバしか利用できない組織では、通常はシングルサーバインストールによる展開が適しています。サーバの可用性が問題にならない場合は、クライアント展開の規模と、ファイアウォール外で作業を行うユーザの数を考慮に入れる必要があります。

利用可能な SQL Server 展開

ZENworks Endpoint Security Management はインストール時に 3 つの SQL データベースを作成します。展開の規模が小さい場合は、単一の SQL データベース、つまり 1 つのサーバ側データベースを、ポリシー配布サービスおよび管理サービスのサーバにインストールできます。大規模な展開では、SQL データベースサーバを別途導入し、ポリシー配布サービスおよび管理サービスからデータを受け取ることができるようにします。使用できる RDBMS は次の種類のみです。

- SQL Server Standard
- SQL Server Enterprise
- Microsoft SQL Server 2000 SP4

名前付きインスタンスの場合は、サーバを次のように設定する必要があります。

プロバイダ =sqloledb

Data Source=ServerName\InstanceName (ZENworks Endpoint Security Management をインストールするにはこのように定義する必要があります)

初期カタログ =DatabaseName

ユーザ ID=Username

パスワード =Password

SQL を混合モードに設定します。

インストール時にドメインユーザのユーザ名とパスワードを使用することはできません。SysAdmin 権限を持つ SQL ユーザのユーザ名とパスワードを使用する必要があります。

SSL 通信を確立するために既存の証明書を使用するか、または Novell 自己署名証明書を使用するか

障害復旧やフェイルオーバが可能な設計にするには、ZENworks Endpoint Security Management の完全な展開のために、企業またはその他の認証局 (VeriSign、GeoTrust、Thawte など) が発行した SSL 証明書を使用する必要があります。独自の証明書を使用する場合は、ポリシー配布サービスとして指定されたマシンで Web サービス証明書とルート CA を作成し、適切なマシンに配布します。企業の認証局の作成については、Microsoft Web サイトに示されている認証局の安全なセットアップ方法の段階的な説明を参照してください。

評価用または (ユーザ数が 100 未満の) 小規模な展開には、ZENworks Endpoint Security Management の自己署名証明書を使用できます。Novell SSL 証明書は、標準インストールを実行したときにサーバにインストールされます。

Endpoint Security Client を展開する方法

Endpoint Security Client ソフトウェアは、各エンドポイントに個別に、または MSI プッシュによって展開することができます。MSI パッケージの作成方法については、63 ページの第 9.2 章「MSI のインストール」を参照してください。

ポリシーをマシンベースにするかユーザベースにするか

ポリシーを 1 つのマシンに配布して、ログオンしたすべてのユーザが同じポリシーを受け取るようにしたり、ポリシーを個々のユーザまたはグループ用に設定したりすることができます。

インストールにはそれぞれいくつかの前提条件があります。どのコンポーネントについても、それぞれの前提条件のチェックリストの記入を完了してから、インストールを行うことをお勧めします。次のページのリストを確認してください。

- 17 ページの第 3 章「シングルサーバインストールの実行」
- 23 ページの第 5 章「ポリシー配布サービスのインストール」
- 33 ページの第 6 章「管理サービスのインストール」
- 45 ページの第 7 章「管理コンソールのインストール」
- 57 ページの第 8 章「クライアントロケーション保証サービスのインストール」
- 61 ページの第 9 章「Endpoint Security Client 3.5 のインストール」

シングルサーバインストールの実行 3

ZENworks® Endpoint Security Management のシングルサーバインストール (SSI) により、ポリシー配布サービスと管理サービスが同じサーバ上で共存できます (このインストールオプションを使用した場合のみ)。セキュリティ上の理由から、このサーバはファイアウォール内部に展開する必要があります。これによりユーザは、企業のインフラストラクチャ内部にいる場合、または VPN を通じて接続している場合のみ、ポリシーの更新を受け取ることができます。

セキュリティ上および機能上の理由から、プライマリドメインコントローラ (PDC) にシングルサーバインストールを展開することはできません。

注 : サーバの目的の機能には必要ないすべてのアプリケーション、サービス、アカウント、および他のオプションが無効になるように、SSI サーバを設定 (強化) することをお勧めします。このための手順はローカル環境の仕様によって異なるため、前もって説明しておくことはできません。管理者は、Microsoft Technet セキュリティセンターの Web ページ (http://www.microsoft.com/technet/security/default.mspx) の該当するセクションを参照することをお勧めします。アクセス制御に関するその他の推奨事項は、『*ZENworks Endpoint Security Management 管理ガイド*』に記載されています。

信頼されたマシンに対するアクセスのみを保護するために、仮想ディレクトリおよび IIS に ACL を設定できます。次の記事を参照してください。

- 「Granting and Denying Access to Computers (コンピュータへのアクセスの許可および拒否) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)」
- 「Restrict Site Access by IP Address or Domain Name (IP アドレスまたはドメイン名によるサイトアクセスの制限) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)」
- 「IIS FAQ: 2000 IP address and domain name restrictions (IIS FAQ: 2000 IP アドレスおよびドメイン名の制限) (http://www.iisfaq.com/default.aspx?View=A136&P=109)」
- 「Working With IIS Packet Filtering (IIS パケットフィルタリングの使用) (http://www.15seconds.com/issue/011227.htm)」

セキュリティ上の理由から、次のデフォルトのフォルダを IIS のインストールから削除することを強くお勧めします。

- IISHelp
- IISAdmin
- スクリプト
- プリンタ

microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) で入手可能な IIS Lockdown Tool 2.1 を使用することもお勧めします。

バージョン 2.1 は、IIS に依存する主要なマイクロソフト製品用に提供されたテンプレートによって駆動されます。このサーバの役割に最も厳密に適合したテンプレートを選択してください。どれが適切かわからない場合は、Dynamic Web サーバテンプレートを使用することをお勧めします。

インストールを始める前に、次の前提条件が満たされていることを確認してください。

- サポートされているディレクトリサービス (eDirectory™、Active Directory、または NT ドメイン) にアクセスできるようにします。NT ドメインがサポートされるのは、Microsoft Windows 2000 Advanced server (SP4) に Single Server Service がインストールされている場合だけです。
- eDirectory サービスを使用して展開する場合は、Novell Client™ がサーバにインストールされ、eDirectory を正しく認証できることを確認してください。管理コンソールの認証用に使用される、変更されることのないアカウントパスワードを作成します (49 ページのセクション 7.2.1「eDirectory サービスの追加」を参照)。
- Endpoint Security Client がシングルサーバのサーバ名を解決できるようにするためには、Endpoint Security Client のインストール先のコンピュータが、SSI サーバ名に対して ping を実行できることを確認します。ping に応答がない場合は、インストールを続行する前に問題を解決する必要があります (SSI サーバ名を FQDN/NETBIOS に変更する、FQDN/NETBIOS を使用するように AD を変更する、DNS 設定を変更する、正しい MS 情報が含まれるようにターゲットコンピュータのローカルホストファイルを変更するなど)。
- Microsoftインターネットインフォメーションサービス(IIS)を有効にするかインストールして、Secure Socket Layer(SSL) 証明書を受諾するように設定します。

重要 :［セキュリティで保護された通信］ページの［*セキュリティで保護されたチャネルを要求する (SSL)*］チェックボックスは有効にしないでください (Microsoft コンピュータの管理ユーティリティで、［*サービスとアプリケーション*］>［*Internet Information Services (ISS) Manager (インターネットインフォメーションサービス (IIS) マネージャ)*］>［*Web サイト*］の順に展開し、［*既定の Web サイト*］を右クリックし、［*プロパティ*］>［*ディレクトリセキュリティ*］タブ >［セキュリティで保護された通信］グループボックスの［*編集*］ボタンの順にクリックします)。このオプションを有効にすると、Zenworks Endpoint Security Management サーバとエンドポイント上の Zenworks Endpoint Security Client との通信が遮断されます。

- 独自のSSL証明書を使用する場合は、Webサービス証明書とルートCAがマシンにロードされていることと、前の手順で確認済みのサーバ名 (NETBIOS または FQDN) が、IIS で設定されている証明書の「*Issued to*」値に一致していることを確認します。
- 独自の証明書を使用する場合、または Novell 自己署名証明書をインストール済みの場合は、Endpoint Security Client がインストールされているマシンから次の URL にアクセスして SSL を検証することもできます。https://*SSI_SERVER_NAME*/AuthenticationServer/UserService.asmx (ここで *SSI_SERVER_NAME* はサーバ名です) これにより、証明書警告ではなく有効なデータ (HTML ページ) が返されます。証明書警告が返された場合は、インストールの前に解決する必要があります。ただし、Novell 自己署名証明書を使用する場合を除きます。
- サポートされている RDBMS(Microsoft SQL Server 2000 SP4、SQL Server Standard、SQL Server Enterprise) にアクセスできるようにします。データベースを混合モードに設定します。

3.1 インストール手順

マスタインストーラメニューから、[Single Server Installation (シングルサーバインストール)] を選択します。このインストールでは、ポリシー配布サービス用のインストールと管理サービス用のインストールが組み合わされます。詳細については、23 ページの第 5 章「ポリシー配布サービスのインストール」および 33 ページの第 6 章「管理サービスのインストール」を参照してください。

個々のインストールの場合と同様に、標準設定では、サービスのデフォルトと Novell 自己署名 SSL 証明書がインストールされます。カスタムインストールでは、管理者はディレクトリパスを決定し、企業が所有する認証局を使用することができます。

3.2 サービスの起動

配布サービスと管理サービスはいずれもインストール後に直ちに起動されます。サーバを再起動する必要はありません。管理コンソールは、設定機能を使用した配布サービスと管理サービスの両方の管理に使用されます。詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

このインストールが完了したら、管理コンソールとクライアントロケーション保証サービスの両方をこのサーバにインストールすることができます。個別のマシンに管理コンソールをインストールする場合は、指定された管理コンソールのマシンに ZENworks Endpoint Security Management の Setup Files フォルダをコピーして、インストールを完了します。

23 ページの第 5 章「ポリシー配布サービスのインストール」に進みます。

マルチサーバインストールの実行

4

マルチサーバインストールは、大規模な展開の場合や、ポリシー配布サービスを企業ファイアウォールの外部に置いて、境界外にいるユーザが定期的にポリシーの更新を受け取るようにする場合に適しています。マルチサーバインストールは、少なくとも異なる 2 台のサーバに対して行う必要があります。個別のポリシー配布サービスと管理サービスを同じサーバにインストールしようとすると、インストールは失敗します。シングルサーバインストールの詳細については、17 ページの第 3 章「シングルサーバインストールの実行」を参照してください。

マルチサーバインストールでは、最初に、企業ファイアウォールの内部または外部にあるセキュリティで保護されたサーバに、ポリシー配布サービスをインストールします。詳細については、23 ページの第 5 章「ポリシー配布サービスのインストール」を参照してください。

ポリシー配布サービスをインストールしたら、次に管理サービスをインストールします。詳細については、33 ページの第 6 章「管理サービスのインストール」を参照してください。

管理コンソールもこのサーバにインストールすることをお勧めします。詳細については、45 ページの第 7 章「管理コンソールのインストール」を参照してください。

「23 ページの第 5 章「ポリシー配布サービスのインストール」」に進みます。

5 ポリシー配布サービスのインストール

ZENworks® Endpoint Security Management のポリシー配布サービスをホストするサーバは、ユーザがネットワークの内部にいる場合でも DMZ の外部にいる場合でもアクセスできなければなりません。インストールの前に、必要なソフトウェアがサーバにインストールされていることを確認してください (10 ページの 「システム要件」 を参照)。サーバを選択したら、サーバの名前 (NETBIOS と完全修飾ドメイン名 (FQDN) の両方) をメモします。

セキュリティ上および機能上の理由から、プライマリドメインコントローラ (PDC) にポリシー配布サービスを展開することはできません。

注 : サーバの目的の機能には必要ないすべてのアプリケーション、サービス、アカウント、および他のオプションが無効になるように、SSI サーバを設定 (強化) することをお勧めします。このための手順はローカル環境の仕様によって異なるため、前もって説明しておくことはできません。管理者は、Microsoft Technet セキュリティセンターの Web ページ (http://www.microsoft.com/technet/security/default.mspx) の該当するセクションを参照することをお勧めします。アクセス制御に関するその他の推奨事項は、『*ZENworks Endpoint Security Management 管理ガイド*』に記載されています。

信頼されたマシンに対するアクセスのみを保護するために、仮想ディレクトリおよび IIS に ACL を設定できます。次の記事を参照してください。

- 「Granting and Denying Access to Computers (コンピュータへのアクセスの許可および拒否) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)」
- 「Restrict Site Access by IP Address or Domain Name (IP アドレスまたはドメイン名によるサイトアクセスの制限) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)」
- 「IIS FAQ: 2000 IP address and domain name restrictions (IIS FAQ: 2000 IP アドレスおよびドメイン名の制限) (http://www.iisfaq.com/default.aspx?View=A136&P=109)」
- 「Working With IIS Packet Filtering (IIS パケットフィルタリングの使用) (http://www.15seconds.com/issue/011227.htm)」

セキュリティ上の理由から、次のデフォルトのフォルダを IIS のインストールから削除することを強くお勧めします。

- IISHelp
- IISAdmin
- スクリプト
- プリンタ

microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) で入手可能な IIS Lockdown Tool 2.1 を使用することもお勧めします。

バージョン 2.1 は、IIS に依存する主要なマイクロソフト製品用に提供されたテンプレートによって駆動されます。このサーバの役割に最も厳密に適合したテンプレートを選択してください。どれが適切かわからない場合は、Dynamic Web サーバテンプレートを使用することをお勧めします。

インストールを開始する前に、次の前提条件を確認してください。

- 管理サービス (MS) によるポリシー配布サービス (DS) サーバ名の解決の確認 : MS のインストール先コンピュータが DS サーバ名に対して ping を実行できることを確認します (DS サーバ名は、DS がネットワークファイアウォール内に設定される場合は NETBIOS、ファイアウォール外部の DMZ にインストールされる場合は FQDN になります)。
- ping に正しい応答があった場合は、その名前がインストール時に入力されるサーバ名になります。ping に応答がない場合は、インストールを続行する前にこの問題を解決する必要があります。
- Endpoint Security Client による DS サーバ名の解決の確認 : Endpoint Security Client のインストール先のエンドポイントクライアントが、上記で使用されたものと同じ DS サーバ名に対して ping を実行できることを確認します。ping に応答がない場合は、インストールを続行する前にこの問題を解決する必要があります。
- Microsoft インターネットインフォメーションサービス (IIS) を有効にするかインストールして、ASP.NET を有効にし、Secure Socket Layer(SSL) 証明書を受諾するように設定します。

  重要 : ［セキュリティで保護された通信］ページの［*セキュリティで保護されたチャネルを要求する (SSL)*］チェックボックスは有効にしないでください (Microsoft コンピュータの管理ユーティリティで、［*サービスとアプリケーション*］>［*Internet Information Services (ISS) Manager (インターネットインフォメーションサービス (IIS) マネージャ)*］>［*Web サイト*］の順に展開し、［*既定の Web サイト*］を右クリックし、［*プロパティ*］>［*ディレクトリセキュリティ*］タブ >［セキュリティで保護された通信］グループボックスの［*編集*］ボタンの順にクリックします)。このオプションを有効にすると、Zenworks Endpoint Security Management サーバとエンドポイント上の Zenworks Endpoint Security Client との通信が切断されます。

- 独自の SSL 証明書を使用している場合は、「Web サービス」証明書がマシンにロードされていることと、前の手順で確認済みのサーバ名 (NETBIOS または FQDN) が、IIS で設定されている証明書の「Issued to」値に一致していることを確認します。
- 独自の SSL 証明書を使用している場合は、MS サーバから DS サーバへの SSL を確認してください。このためには、管理サービスで Web ブラウザを開き、URL として「https://DSNAME」(DSNAME は DS のサーバ名) と入力します。これにより、証明書警告ではなく有効なデータが返されます (有効なデータが「Page under Construction (このページは現在作成中です)」である場合もあります)。証明書警告が返された場合は、インストールの前に解決する必要があります。ただし、Novell 自己署名証明書を使用する場合を除きます。
- サポートされている RDBMS(Microsoft SQL Server 2000 SP4、SQL Server Standard、SQL Server Enterprise、SQL Server 2005) にアクセスできるようにします。データベースを混合モードに設定します。このデータベースは、管理サービスサーバ、または企業のファイアウォールの背後で保護されている共有サーバでホストする必要があります。

5.1 インストール手順

［Installation Interface (インストールインタフェース)］メニューの［Policy Distribution Service Installation (ポリシー配布サービスのインストール)］をクリックします。ポリシー配布サービスのインストールが開始されます。

起動時にインストーラは、必要なすべてのソフトウェアがサーバ上にあるかどうかを確認します。必要なソフトウェアがインストールされていない場合は、［Welcome (ようこそ)］画面に移行する前に自動的にインストールされます (追加するソフトウェアのライセンス契約の受諾が必要になる場合があります)。Microsoft Data Access Components (MDAC) 2.8 をインストールする必要がある場合は、MDAC のインストール後にサーバを再起動しないと、ZENworks Endpoint Security Management のインストールを続行できません。Windows 2003 Server を使用している場合は、ASP.NET 2.0 を実行するように設定されます。

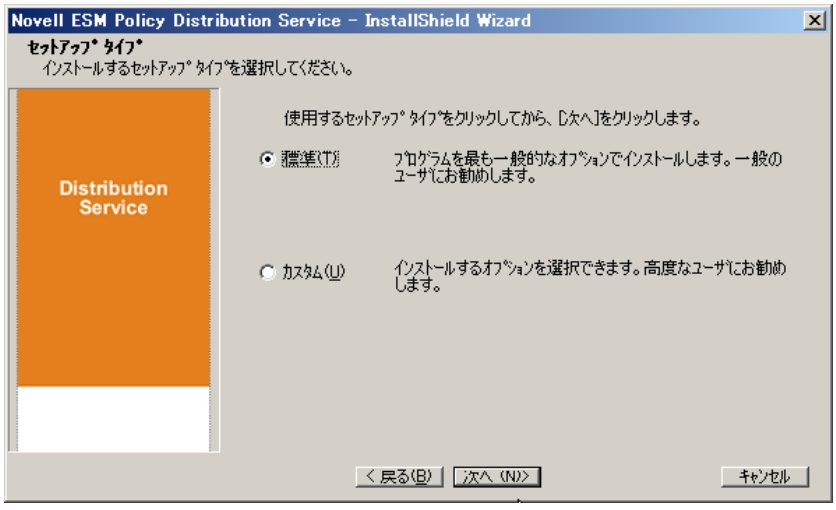
ポリシー配布サービスのインストールが開始されたら、次の手順を実行します。

注 : インストールプロセスを完了するためには、管理者は次の各手順を実行する必要があります。インストール作業中に内部処理の進行状況が表示されますが、インストールを正しく行うために必要となる特定のアクションや情報以外は文書に解説されていません。

---

1. ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。
2. 使用許諾書に同意して、［次へ］をクリックします。
3. ［Typical (標準)］インストールまたは［Custom (カスタム)］インストールを選択します。>

図 5-1 標準インストールまたはカスタムインストールの選択



次に、両方のインストールパスについて説明します。

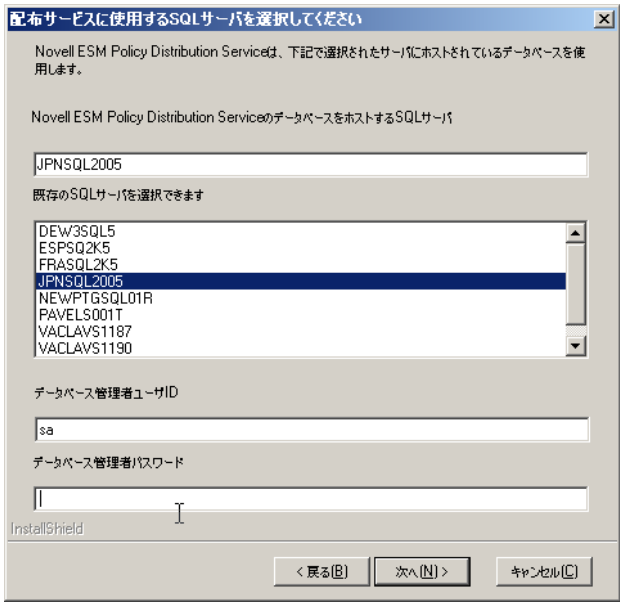
- 26 ページのセクション 5.1.1「標準インストール」
- 28 ページのセクション 5.1.2「カスタムインストール」

5.1.1 標準インストール

標準インストールでは、ポリシー配布サービスソフトウェアのファイルは、デフォルトのディレクトリである \Program Files\Novell\ESM Policy Distribution Service に置かれます。SQL データベースには STDSDB という名前が割り当てられます。3 つの SQL データベースファイル (data、index、log) は、\Program Files\Microsoft SQL Server\mssql\Data に置かれます。

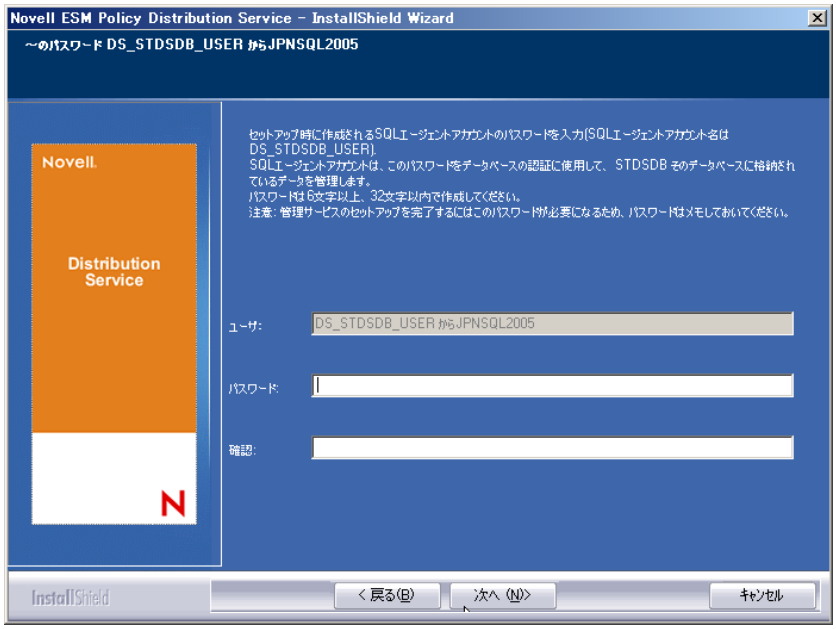
1. Novell SSL 証明書がインストール用に作成されます。独自の SSL 証明書を使用する場合は、カスタムインストールを実行してください。これらの証明書は、すべてのユーザに配布する必要があります。
2. インストーラによって、マシンおよびネットワーク上の使用可能な SQL データベースが検出されます。ポリシー配布サービス用にセキュリティで保護された SQL データベースを選択し、データベース管理者の名前とパスワードを入力します (パスワードが 0 のみの連続である場合、セキュリティ上の問題が発生する可能性があることを示す警告が表示されます)。ドメインユーザのユーザ名とパスワードを使用することはできません。SysAdmin 権限を持つ SQL ユーザのユーザ名とパスワードを使用する必要があります。

図 5-2 SQL Server の選択



3. ポリシー配布サービスエージェントのパスワードを指定します。これは、サービスが SQL データベースへのログインに使用するユーザ名とパスワードです。

図 5-3 配布サービスの SQL パスワード



4 ポリシー配布サービスのドメイン名を指定します。サーバが企業のファイアウォールの外部にある場合、このドメイン名は完全修飾ドメイン名でなければなりません。それ以外の場合は、サーバの NETBIOS 名だけが必要になります。

図 5-4 ポリシー配布サービスのドメイン名の入力

5 [Copy Files (ファイルのコピー)] 画面で [次へ] をクリックするとインストールが開始されます。

6 インストールディレクトリに ESM Setup Files フォルダが生成されます。このフォルダには、管理サービスが必要とするセットアップ ID ファイルと ESM-DS.cer ファイル (Novell 自己署名 SSL 証明書) が含まれています。このファイルを、netshare を介

してコピーするか、あるいはファイルをディスクまたはサムドライブに保存してから、サーバのインストールディレクトリに手動でロードするいずれかの方法で管理サービスのホストとして指定されたマシンに直接コピーします。

7 これで、ポリシー配布サービスがインストールされました。［終了］をクリックするとインストールプログラムが終了し、パフォーマンスモニタが起動されます。

5.1.2 カスタムインストール

カスタムインストールでは、標準インストールで使用されるデフォルト値が表示されます。管理者は、ソフトウェアファイルを保存する別のディレクトリを指定するかブラウズして、そのディレクトリに移動することができます。

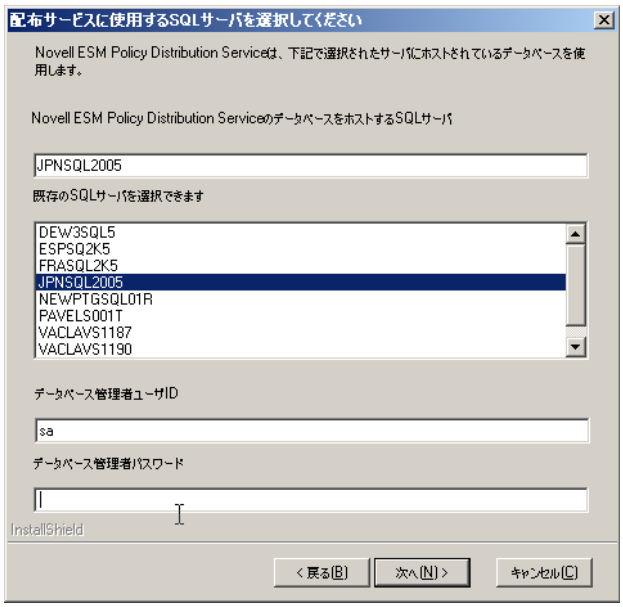
管理者は、Novell 自己署名 SSL 証明書をインストールするか、または独自の証明書を使用するかを選択できます。

1 ポリシー配布サービスと管理サービスの間、および DS とすべての Novell Security Client の間にセキュリティで保護された通信を確立するには、SSL 証明書が必要です。すでに認証局が設定されている場合は、［IIS に設定されている既存の証明書を使用してください。］をクリックします。証明書が必要な場合は、［Novell 独自の自己署名ルート証明書の作成、インストールおよび使用を許可します。］をクリックします。インストーラによって、証明書と署名局が作成されます。証明書のタイプに関係なく、これらの証明書をすべてのユーザに配布する必要があります。

図 5-5 信頼されたルートのセットアップ

2 インストーラによって、マシンおよびネットワーク上の使用可能な SQL データベースが検出されます。ポリシー配布サービス用にセキュリティで保護された SQL データベースを選択し、データベース管理者の名前とパスワードを入力します (パスワードが 0 のみの連続である場合、セキュリティ上の問題が発生する可能性があることを示す警告が表示されます)。ドメインユーザのユーザ名とパスワードを使用することはできません。SysAdmin 権限を持つ SQL ユーザのユーザ名とパスワードを使用する必要があります。

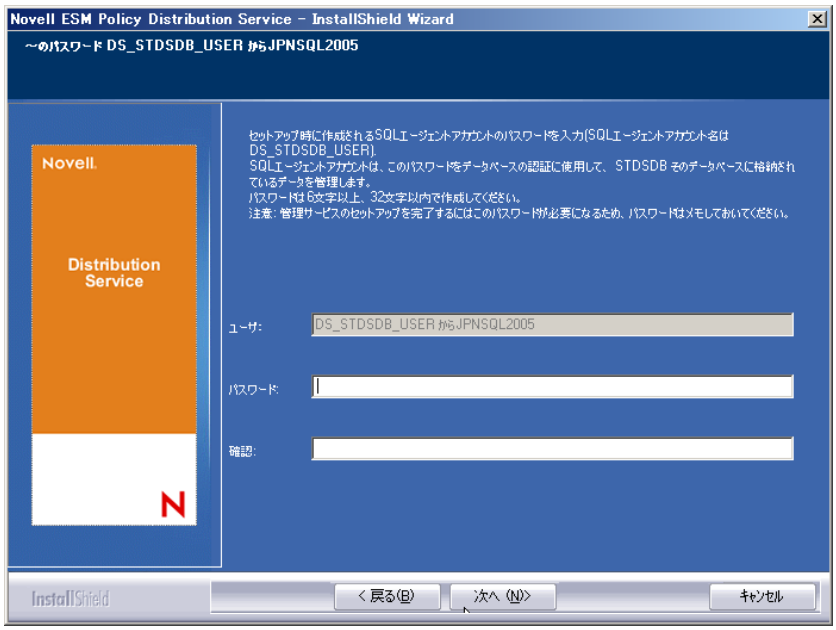
図 5-6 SQL Server の選択



3 データベース名を設定します (デフォルトでは STDSDB と入力されます)。

4 ポリシー配布サービスエージェントのパスワードを指定します。これは、サービスが SQL データベースへのログインに使用するユーザ名とパスワードです。

図 5-7 配布サービスの SQL パスワード



5 ポリシー配布サービスのドメイン名を指定します。サーバが企業のファイアウォールの外部にある場合、このドメイン名は完全修飾ドメイン名でなければなりません。それ以外の場合は、サーバの NETBIOS 名だけが必要になります。

図 5-8 ポリシー配布サービスのドメイン名の入力

6 ［Copy Files (ファイルのコピー)］画面で［次へ］をクリックするとインストールが開始されます。

7 データ、インデックス、およびログファイルのファイルパスを指定します。

8 インストールディレクトリに ESM Setup Files フォルダが生成されます。このフォルダには、管理サービスが必要とするセットアップ ID ファイルと ESM-DS.cer ファイル (選択している場合は Novell 自己署名 SSL 証明書) が含まれています。［Browse (参照)］を使用して、このファイルを保存するサーバ上の場所を指定します (デフォルトではインストールディレクトリになっています)。

図 5-9 セットアップファイルの保存

9 エンタープライズ SSL 証明書の使用を選択した場合は、このファイルのコピーを ESM Setup Files フォルダに保存します。

10 ESM Setup Files フォルダ全体を、netshare を介してコピーするか、あるいはファイルをディスクまたはサムドライブに保存してから、サーバのインストールディレクトリに手動でロードするかのいずれかの方法で管理サービスのホストとして指定されたマシンに直接コピーします。

11 これで、ポリシー配布サービスがインストールされました。［終了］をクリックするとインストールプログラムが終了し、パフォーマンスモニタが起動されます。

5.2 サービスの起動

ポリシー配布サービスは、インストール後直ちに起動されます。サーバを再起動する必要はありません。管理コンソールでは、環境ツールを使用して配布サービスのアップロードの時刻を調整します。詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

33 ページの第 6 章「管理サービスのインストール」に進みます。

管理サービスのインストール

6

管理サービスは、ファイアウォールの背後のセキュリティで保護されたサーバにインストールしてください。ポリシー配布サービスと同じサーバを共有することはできません (シングルサーバインストールの場合を除きます。17 ページの第 3 章「シングルサーバインストールの実行」を参照してください)。セキュリティ上の理由から、管理サービスをネットワークファイアウォールの外部にはインストールしないでください。サーバを選択したら、サーバの名前 (NETBIOS と完全修飾ドメイン名 (FQDN) の両方) をメモします。セキュリティ上および機能上の理由から、プライマリドメインコントローラ (PDC) に管理サービスを展開することはできません。

注 : サーバの目的の機能には必要ないすべてのアプリケーション、サービス、アカウント、および他のオプションが無効になるように、SSI サーバを設定 (強化) することをお勧めします。このための手順はローカル環境の仕様によって異なるため、前もって説明しておくことはできません。管理者は、Microsoft Technet セキュリティセンターの Web ページ (http://www.microsoft.com/technet/security/default.mspx) の該当するセクションを参照することをお勧めします。アクセス制御に関するその他の推奨事項は、『*ZENworks Endpoint Security Management 管理ガイド*』に記載されています。

信頼されたマシンに対するアクセスのみを保護するために、仮想ディレクトリおよび IIS に ACL を設定できます。次の記事を参照してください。

- 「Granting and Denying Access to Computers (コンピュータへのアクセスの許可および拒否) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)」
- 「Restrict Site Access by IP Address or Domain Name (IP アドレスまたはドメイン名によるサイトアクセスの制限) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)」
- 「IIS FAQ: 2000 IP address and domain name restrictions (IIS FAQ: 2000 IP アドレスおよびドメイン名の制限) (http://www.iisfaq.com/default.aspx?View=A136&P=109)」
- 「Working With IIS Packet Filtering (IIS パケットフィルタリングの使用) (http://www.15seconds.com/issue/011227.htm)」

セキュリティ上の理由から、次のデフォルトのフォルダを IIS のインストールから削除することを強くお勧めします。

- IISHelp
- IISAdmin
- スクリプト
- プリンタ

microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) で入手可能な IIS Lockdown Tool 2.1 を使用することもお勧めします。

バージョン 2.1 は、IIS に依存する主要なマイクロソフト製品用に提供されたテンプレートによって駆動されます。このサーバの役割に最も厳密に適合したテンプレートを選択してください。どれが適切かわからない場合は、Dynamic Web サーバテンプレートを使用することをお勧めします。

インストールを始める前に、次の前提条件が満たされていることを確認してください。

- サポートされているディレクトリサービス (eDirectory、Active Directory、または NT ドメイン *) にアクセスできるようにします。* 管理サービスが Microsoft Windows 2000 Advanced Server(SP4) にインストールされている場合のみサポートされます。
- eDirectory™ サービスを使用して展開する場合は、Novell Client™ がサーバにインストールされ、eDirectory を正しく認証できることを確認してください。管理コンソールの認証用に使用される、変更されることのないアカウントパスワードを作成します (49 ページのセクション 7.2.1「eDirectory サービスの追加」を参照)。
- Endpoint Security ClientによるMSサーバ名の解決の確認: Endpoint Security Clientのインストール先のコンピュータが、MS サーバ名に対して ping を実行できることを確認します。ping に正しい応答があった場合は、この値がインストール時に入力する値になります。ping に応答がない場合は、インストールを続行する前にこの問題を解決する必要があります。
- Microsoftインターネットインフォメーションサービス(IIS)を有効にするかインストールして、ASP.NET を有効にし、Secure Socket Layer(SSL) 証明書を受諾するように設定します。

重要 :［セキュリティで保護された通信］ページの［*セキュリティで保護されたチャネルを要求する (SSL)*］チェックボックスは有効にしないでください (Microsoft コンピュータの管理ユーティリティで、［*サービスとアプリケーション*］>［*Internet Information Services (ISS) Manager (インターネットインフォメーションサービス (IIS) マネージャ)*］>［*Web サイト*］の順に展開し、［*既定の Web サイト*］を右クリックし、［*プロパティ*］>［*ディレクトリセキュリティ*］タブ >［セキュリティで保護された通信］グループボックスの［*編集*］ボタンの順にクリックします)。このオプションを有効にすると、Zenworks Endpoint Security Management サーバとエンドポイント上の Zenworks Endpoint Security Client との通信が切断されます。

- 独自の SSL 証明書を使用する場合は、ルート CA がマシンにロードされていることと、前の手順で確認済みのサーバ名 (NETBIOS または FQDN) が、IIS で設定されている証明書の「*Issued to*」値に一致していることを確認します。
- 独自の証明書を使用する場合、または Novell 自己署名証明書をインストール済みの場合は、Endpoint Security Client がインストールされているマシンから次の URL にアクセスして SSL を検証することもできます。https://*MS_SERVER_NAME*/AuthenticationServer/UserService.asmx (ここで *MS_SERVER_NAME* はサーバ名です) これにより、証明書警告ではなく有効なデータ (HTML ページ) が返されます。証明書警告が返されたら、インストールの前に解決する必要があります。
- サポートされている RDBMS(Microsoft SQL Server 2000 SP4、SQL Server Standard、SQL Server Enterprise、SQL 2005) にアクセスできるようにします。データベースを混合モードに設定します。
- ポリシー配布サービスのセットアップ ID とルート SSL 証明書が格納されている ESM Setup Files ディレクトリを、このサーバのインストールディレクトリにコピーします。

6.1 インストール手順

［Installation Interface (インストールインタフェース)］メニューの［Management Service Installation (管理サービスのインストール)］をクリックします。管理サービスのインストールが開始されます。

起動時にインストーラは、必要なすべてのソフトウェアがサーバ上にあるかどうかを確認します。必要なソフトウェアがインストールされていない場合は、［Welcome (ようこそ)］画面に移行する前に自動的にインストールされます (追加するソフトウェアのライセンス契約の受諾が必要になる場合があります)。Microsoft Data Access Components (MDAC) 2.8 をインストールする必要がある場合は、MDAC のインストール後にサーバを再起動しないと、ZENworks Endpoint Security Management のインストールを続行できません。Windows 2003 Server を使用している場合は、ASP.NET 2.0 を実行するように設定する必要があります。

管理サービスのインストールが開始されたら、次の手順を実行します。

注 : インストールプロセスを完了するためには、管理者は次の各手順を実行する必要があります。インストール作業中に内部処理の進行状況が表示されますが、インストールを正しく行うために必要となる特定のアクションや情報以外は文書に解説されていません。

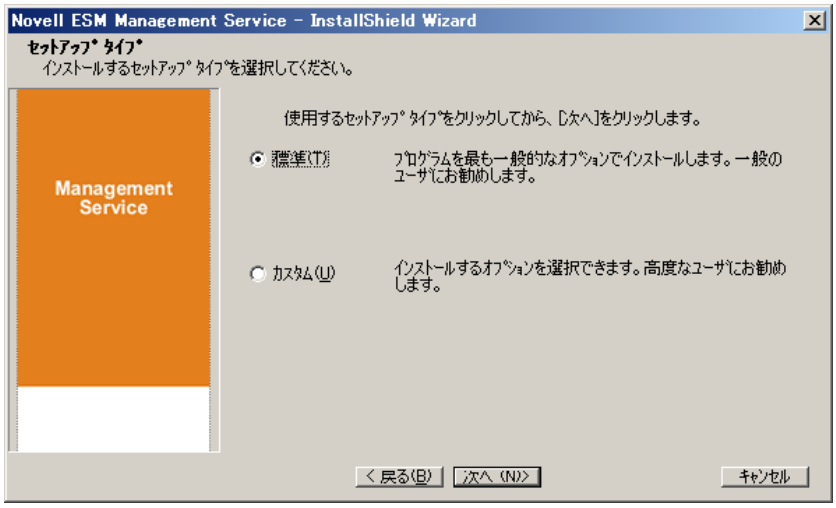
---

1 ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。

2 使用許諾書に同意して、［次へ］をクリックします。

3 ［Typical (標準)］インストールまたは［Custom (カスタム)］インストールを選択します。>

図 6-1 標準またはカスタムの選択



次に、両方のインストールパスについて説明します。

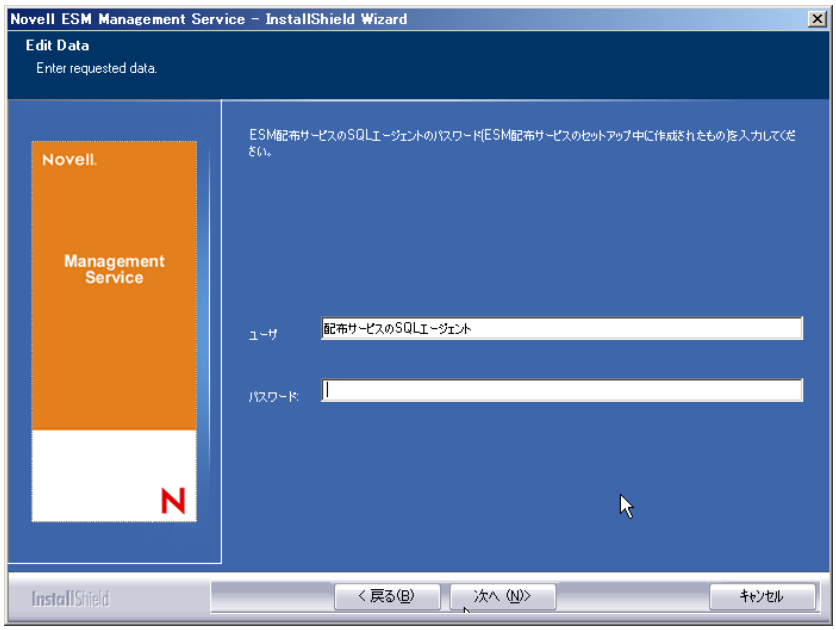
- 35 ページのセクション 6.1.1「標準インストール」
- 39 ページのセクション 6.1.2「カスタムインストール」

6.1.1 標準インストール

標準インストールでは、管理サービスソフトウェアのファイルは、デフォルトのディレクトリである \Program Files\Novell\ESM Management Service に置かれます。SQL データベースには STMSDB という名前が割り当てられます。3 つの SQL データベースファイル (data、index、log) は、\Program Files\Microsoft SQL Server\mssql\Data に置かれます。

1 ポリシー配布のインストール時に作成されたポリシー配布サービスのエージェントパスワードを指定します。

図 6-2 SQL パスワードの入力



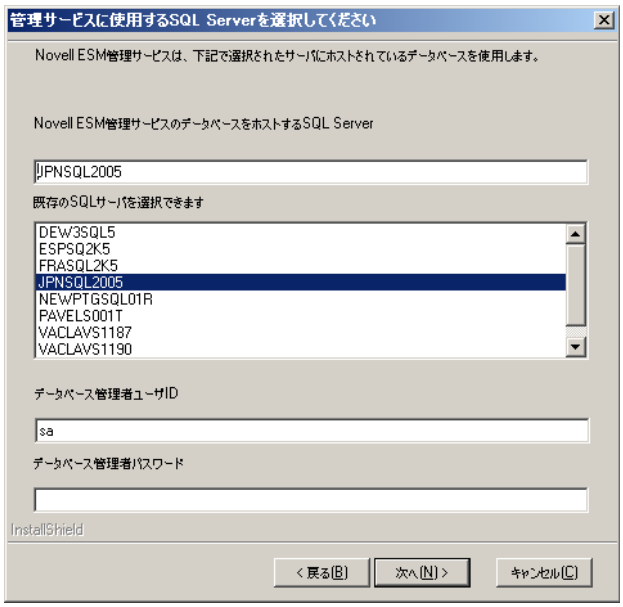
2 管理サービスをホストするサーバの名前を指定します。

図 6-3 MS サーバ名の入力

3 Novell SSL 証明書がインストール用に作成されます。独自の SSL 証明書を使用する場合は、カスタムインストールを実行してください。これらの証明書は、すべてのユーザに配布する必要があります。

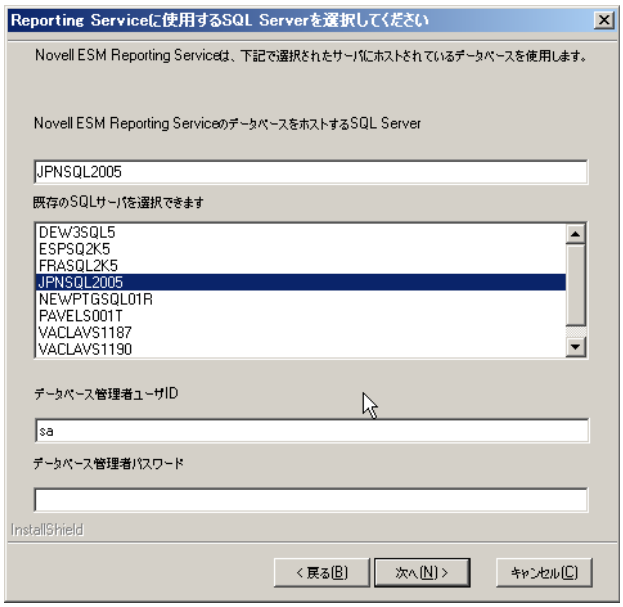
4 インストーラによって、マシンおよびネットワーク上の使用可能な SQL データベースが検出されます。管理サービス用に SQL データベースを選択し、データベース管理者のユーザ名とパスワードを指定します (パスワードが 0 のみの連続である場合、セキュリティ上の問題が発生する可能性があることを示す警告が表示されます)。ドメインユーザのユーザ名とパスワードを使用することはできません。SysAdmin 権限を持つ SQL ユーザのユーザ名とパスワードを使用する必要があります。

図 6-4 MS SQL データベースの選択



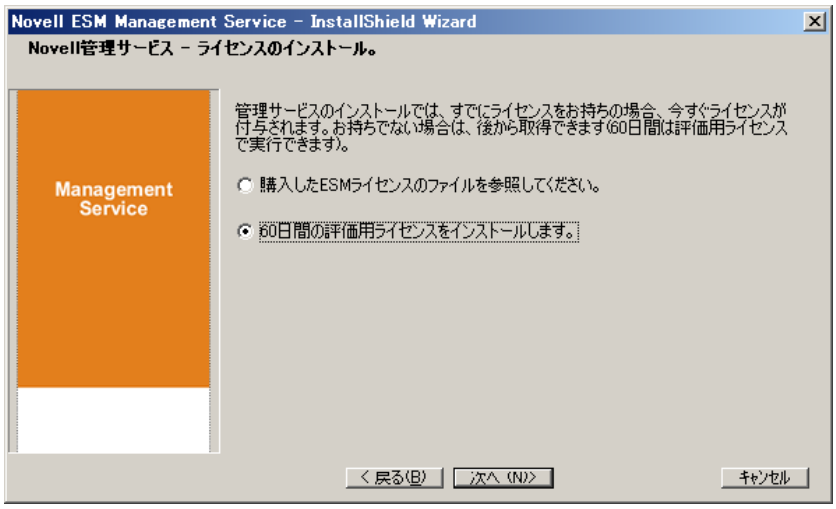
5 レポートサービスの SQL データベースを選択し、そのデータベースのデータベース管理者のパスワードを指定します。多数のレポートをキャプチャして格納する場合は、レポートサービスデータベースに独自の SQL サーバを割り当てることをお勧めします。

図 6-5 レポートサービスデータベースの選択



6 ZENworks Endpoint Security Management をすでに購入されている場合は、個別のライセンスファイルが提供されます。このサーバにライセンスファイルをコピーし、参照します (詳細については、ライセンスファイルに付属している説明ページを参照してください)。ZENworks Endpoint Security Management ライセンスをまだ購入されてない場合は、[60 日間の評価用ライセンスをインストールします。] を選択して操作を続行します。

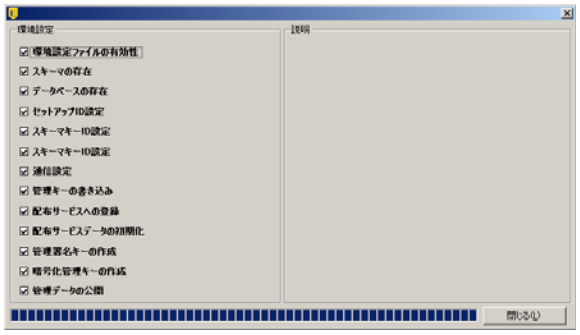
図 6-6 Novell ライセンスファイルの参照



7 ［Copy Files (ファイルのコピー)］画面で［次へ］をクリックするとインストールが開始されます。

8 管理サービスによって、SQL データベースとポリシー配布サービスの両方に対して、通信チェックが実行されます。通信を確認できない場合は、インストーラによって問題が通知されます。インストールを正常に完了するには、すべてのチェックボックスをオンにする必要があります。

図 6-7 通信の確認



9 eDirectory をディレクトリサービスとしてインストールする場合は、ステップ 10 およびステップ 11 をスキップしてください。

10 このインストールが、Active Directory または NT ドメインディレクトリサービスが置かれているドメインのメンバサーバで実行されている場合、セキュリティで保護された読み取り専用の接続を使用して、次のデータが自動的に検出され、インストールに追加されます。

- ルートドメイン名またはマシン名
- 適切な読み取り許可を持つドメイン管理者の名前またはリソースアカウント

11 指定され 1 た領域に管理者のパスワードを指定し、［テスト］をクリックして、接続を確立できるかどうかを確認します。テストが正常に実行されたら、［保存］をクリックします。テストが失敗した場合、または正しいドメインが検出されなかった場合は、管理コンソールを使用して手動で追加する必要があります (49 ページのセクション 7.2.1「eDirectory サービスの追加」を参照)。

注 : 入力したパスワードは期限がないように設定される必要があります。また、このアカウントは無効にならないように設定する必要があります。

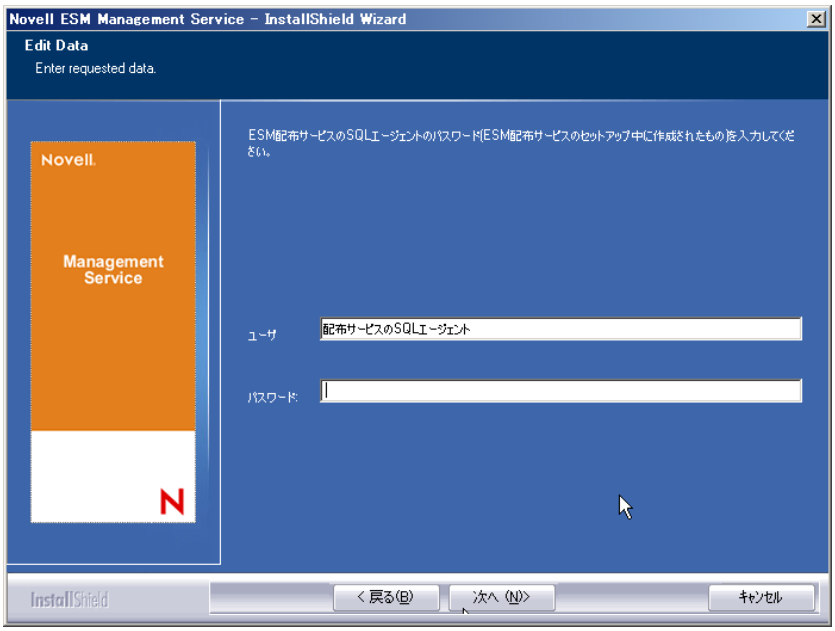
12 これで、管理サービスがインストールされました。[完了] をクリックして通信チェックを終了し、[終了] をクリックしてインストールプログラムを終了します。>

6.1.2 カスタムインストール

カスタムインストールでは、標準インストールで使用されるデフォルト値が表示されます。管理者は、別の場所を入力して、その場所に移動することができます。

1 ポリシー配布のインストール時に作成されたポリシー配布サービスのエージェントパスワードを指定します。

図 6-8 SQL パスワードの入力



2 ポリシー配布サービスのインストールで使用された SSL 証明書のタイプを選択します。既存の (エンタープライズ) 認証局を使用している場合は、[証明書 IIS を使用した Novell 配布サービスは、すでに設定されています。] をクリックします。配布サービスのインストーラで Novell 証明書を作成した場合は、[Novell 配布サービスにより、Novell 自己署名ルート証明書がインストールされました。] をクリックします。

3 管理サービスをホストするサーバの名前を指定します。

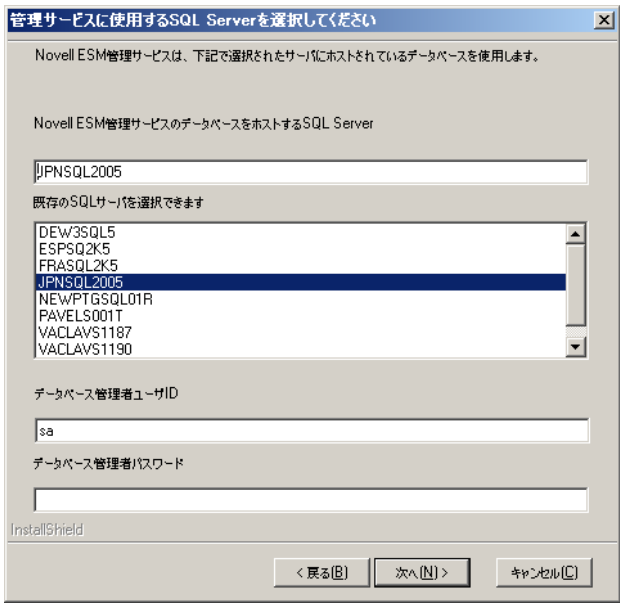
図 6-9 MS サーバ名の入力

4 管理サービスとすべての Endpoint Security Client との間にセキュリティで保護された通信を確立するには、SSL 証明書が必要です。すでに認証局が設定されている場合は、［IIS に設定されている既存の証明書を使用してください。］をクリックします。証明書が必要な場合は、［Novell 独自の自己署名ルート証明書の作成、インストールおよび使用を許可します。］をクリックします。> インストーラによって、証明書と署名局が作成されます。証明書のタイプに関係なく、これらの証明書をすべてのユーザに配布する必要があります。

5 Novell 証明書を選択する場合は、証明書を簡単に配布できる保存場所を選択します (デフォルトはインストールディレクトリ)。

6 インストーラによって、マシンおよびネットワーク上の使用可能な SQL データベースが検出されます。管理サービス用に SQL データベースを選択し、データベース管理者のユーザ名とパスワードを指定します (パスワードが 0 のみの連続である場合、セキュリティ上の問題が発生する可能性があることを示す警告が表示されます)。ドメインユーザのユーザ名とパスワードを使用することはできません。SysAdmin 権限を持つ SQL ユーザのユーザ名とパスワードを使用する必要があります。

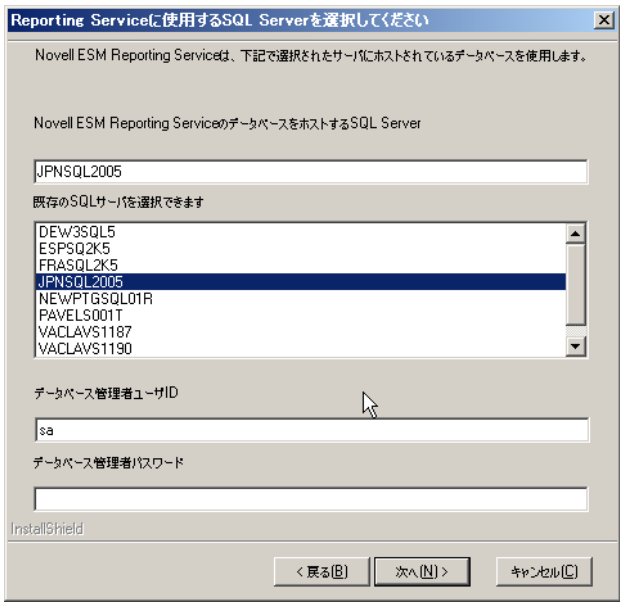
図 6-10 MS SQL データベースの選択



7 データベース名を設定します (デフォルトでは STMSDB と入力されます)。

8 レポートサービスの SQL データベースを選択し、そのデータベースのデータベース管理者のパスワードを指定します。

図 6-11 レポートサービスデータベースの選択

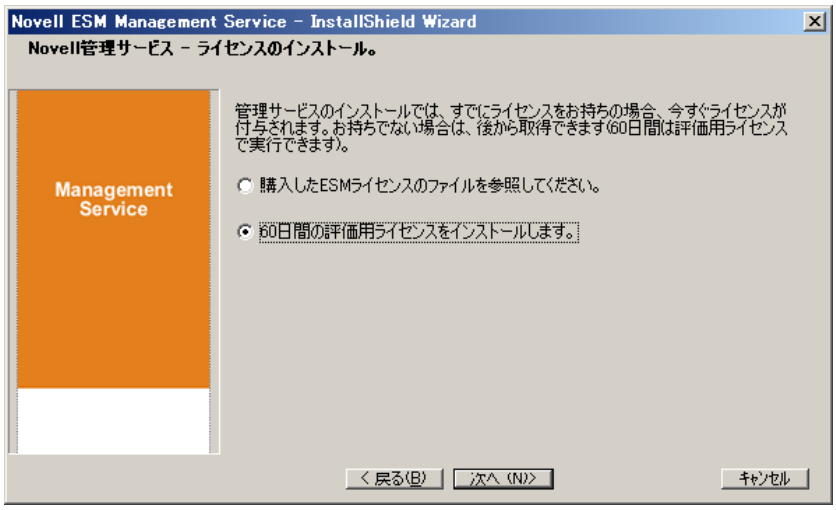


9 データベース名を設定します (デフォルトでは STRSDB と入力されます)。

10 ZENworks Endpoint Security Management をすでに購入されている場合は、個別のライセンスファイルが提供されます。このサーバにライセンスファイルをコピーし、参照します (詳細については、ライセンスファイルに付属している説明ページを参照して

ください)。ZENworks Endpoint Security Management ライセンスをまだ購入されてない場合は、［60 日間の評価用ライセンスをインストールします。］を選択して操作を続行します。

図 6-12 Novell ライセンスファイルの参照



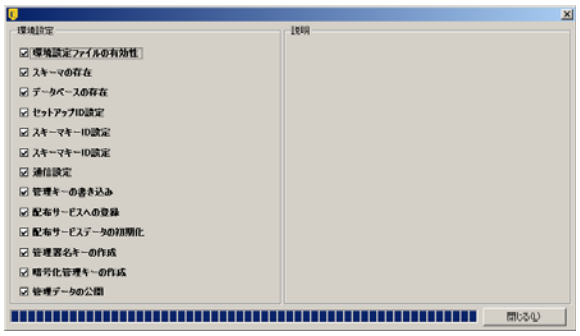
11 ［Copy Files (ファイルのコピー)］画面で［次へ］をクリックするとインストールが開始されます。

12 管理サービスデータベースのデータ、インデックス、およびログファイルのファイルパスを選択します。

13 レポートサービスデータベースのデータ、インデックス、およびログファイルのファイルパスを選択します。

14 管理サービスによって、SQL データベースとポリシー配布サービスの両方に対して、sa 通信チェックが実行されます。通信を確認できない場合は、インストーラによって問題が通知されます。インストールを正常に完了するには、すべてのチェックボックスをオンにする必要があります。

図 6-13 通信の確認



15 eDirectory をディレクトリサービスとしてインストールする場合は、ステップ 16 およびステップ 17 をスキップしてください。

16 このインストールが、Active Directory または NT ドメインディレクトリサービスが置かれているドメインのメンバサーバで実行されている場合、セキュリティで保護された読み取り専用の接続を使用して、次のデータが自動的に検出され、インストールに追加されます。

- ルートドメイン名またはマシン名
- 適切な読み取り許可を持つドメイン管理者の名前またはリソースアカウント

17 指定され 1 た領域に管理者のパスワードを指定し、[テスト] をクリックして、接続を確立できるかどうかを確認します。テストが正常に実行されたら、[保存] をクリックします。テストが失敗した場合、または正しいドメインが検出されなかった場合は、管理コンソールを使用して手動で追加する必要があります (49 ページのセクション 7.2.1「eDirectory サービスの追加」を参照)。

注 : 指定するパスワードには期限がないように設定される必要があります。また、このアカウントは無効にならないように設定する必要があります。

---

18 これで、管理サービスがインストールされました。[完了] をクリックして通信チェックを終了し、[終了] をクリックしてインストールプログラムを終了します。>

6.2 サービスの起動

管理サービスは、インストール後直ちに起動されます。サーバを再起動する必要はありません。管理コンソールは、管理サービスでデータを管理するために使用されます (『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください)。

管理コンソールはこのサーバにインストールすることをお勧めします。管理コンソールを別のマシンにインストールする場合は、netshare を通じて、またはファイルをディスクまたはサムドライブに保存することで、管理コンソールをホストするマシンに ESM Setup Files ディレクトリをコピーします。

45 ページの第 7 章「管理コンソールのインストール」に進みます。

管理コンソールのインストール 7

管理コンソールは、管理サービスサーバ、または管理サービスサーバと直接通信を行うセキュリティで保護された PC にインストールできます。複数の管理コンソールインストールが 1 つの管理サービスと通信するように設定できます。ただし、管理コンソールへのアクセスを特定のユーザに限定することを強くお勧めします。

セキュリティ上の理由から、管理コンソールは管理サービス用のサーバに直接インストールすることをお勧めします。

別のワークステーションに管理コンソールをインストールする場合は、インストールを開始する前に、以下の前提条件が満たされていることを確認してください。

- 管理コンソールのインストール先デバイスが次の要件を満たすことを確認してください。
  - Windows XP SP1、Windows XP SP2、または Windows 2000 SP4。
  - 256MB以上のRAMと100MBのディスク空き容量を備えた1.0GHzプロセッサの使用をお勧めします。
- ポリシー配布サービスと管理サービス用の SSL ルート証明書が格納されている ESM Setup Files フォルダを、STInstParam.id ファイルと共に PC にコピーします。
- 管理コンソールを管理サービスサーバにインストールする場合は、Microsoft Internet Explorer のバージョンが 5.5 以上であることを確認してください。

7.1 インストール手順

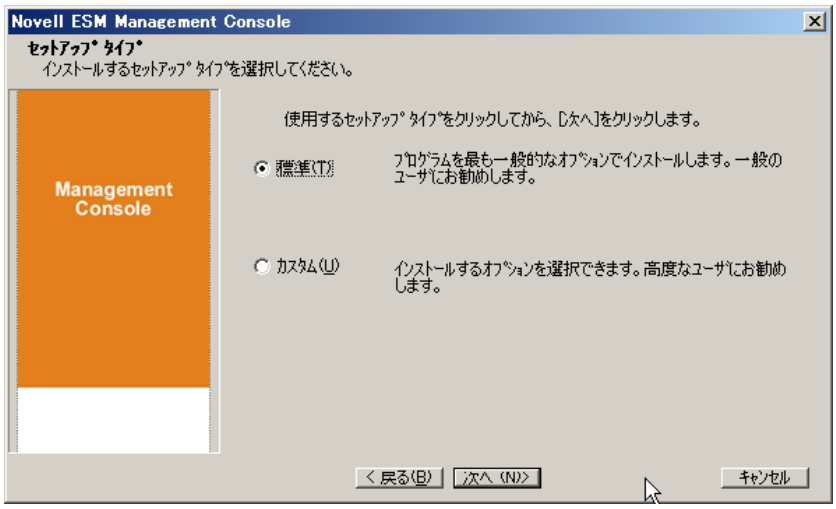
［Installation Interface (インストールインタフェース)］メニューの［Management Console Installation (管理コンソールのインストール)］をクリックします。

起動時にインストーラは、必要な .NET Framework 3.5 と WSE 2.0 SP2 がマシン上にあるかどうかを確認します。そのいずれか、またはどちらもない場合は、［Welcome (ようこそ)］画面に移行する前に自動的にインストールされます (.NET 3.5 のライセンス契約の受諾が必要になります)。

管理コンソールをインストールするには次の操作を実行します。

1. ［次へ］をクリックします。
2. 使用許諾書に同意して、［次へ］をクリックします。
3. ［Typical (標準)］インストールまたは［Custom (カスタム)］インストールを選択します。>

図 7-1 標準またはカスタムの選択



次に、両方のインストールパスについて説明します。

- 46 ページのセクション 7.1.1「標準インストール」
- 46 ページのセクション 7.1.2「カスタムインストール」

7.1.1 標準インストール

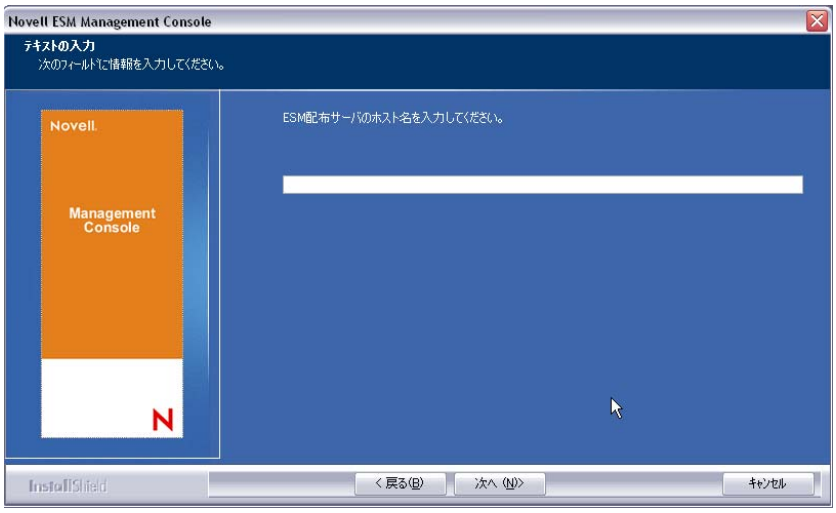
標準インストールでは、STInstParam.id ファイルに含まれているすべてのデフォルトサーバおよび SSL 情報が使用され、デフォルトのディレクトリである \Program Files\Novell\ESM Management Console が使用されます。ESM Setup Files ディレクトリがマシン上にある場合、管理コンソールのインストールではその他の選択を行う必要はありません。

7.1.2 カスタムインストール

カスタムインストールでは、標準インストールで使用される STInstParam.id のデフォルト値が表示されますが、管理者はその情報を変更することができます。

1 ポリシー配布サービスのホスト名を指定します。配布サーバが企業ファイアウォールの外部に展開されている場合、このホスト名は完全修飾ドメイン名でなければなりません。

図 7-2 配布サービスのホスト名の入力



2 管理サービスのホスト名を指定します。

3 管理サービスの SQL データベースのホスト名を指定します。

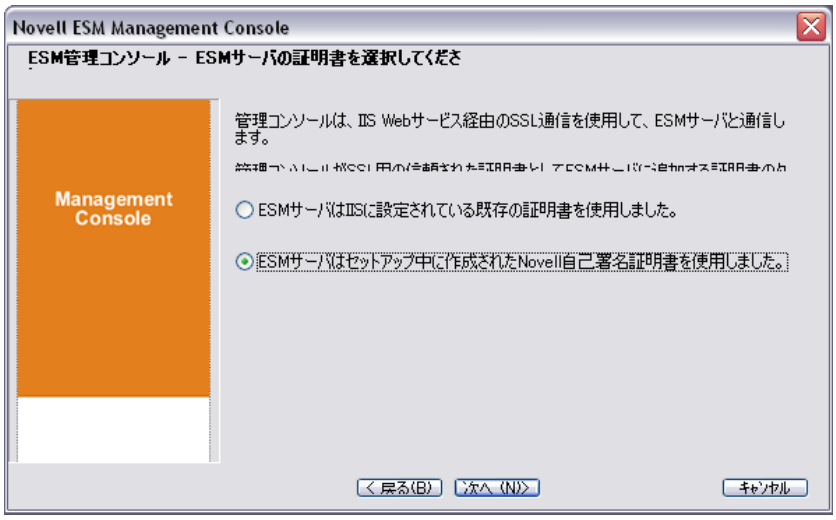
4 管理サービスの SQL データベース名を指定します。

図 7-3 MS の SQL データベース名の入力

5 管理サービスのインストール時に特定された、SQL SA のユーザ名とパスワードを指定します。

6 ポリシー配布サービスと管理サービスにインストールされた SSL 証明書のタイプを選択します。

図 7-4 サーバ証明書の選択



7 管理コンソールのインストール先ディレクトリを選択します。デフォルトのロケーションは \Program Files\Novell\ESM Management Console です。

ZENworks Endpoint Security Management をインストールしたら、システム内でデバイスの管理を開始する前に、ディレクトリサービスを作成して設定する必要があります。

ディレクトリサービスの環境設定の作成ウィザードでは、Endpoint Security クライアントインストールのスコープを定義するディレクトリサービスの環境設定を作成できます。新しい環境設定は、ユーザベースおよびコンピュータベースのクライアントインストールの論理境界を定義するために、既存のディレクトリサービスを使用します。

このウィザードに従って操作すると、ディレクトリサービスと、現在および将来のクライアントアカウントが配置されるコンテキストを選択できます。

また、このウィザードでは、新しい環境設定に含めるディレクトリエントリを同期することもできます。この同期はバックグラウンドで実行されるため、直ちに新しい環境設定の使用を開始できます。

ZENworks Endpoint Security Management のインストール後に、ディレクトリサービスの環境設定の作成ウィザードが自動的に表示されます。ディレクトリサービスの作成と環境設定の詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』の「Configuring the Directory Service (ディレクトリサービスを設定する)」を参照してください。“”

7.2 コンソールの起動

管理コンソールのログインウィンドウを開くには、[スタート] > [すべてのプログラム] > [Novell] > [ESM 管理コンソール] > [管理コンソール] の順にクリックします。> > > >

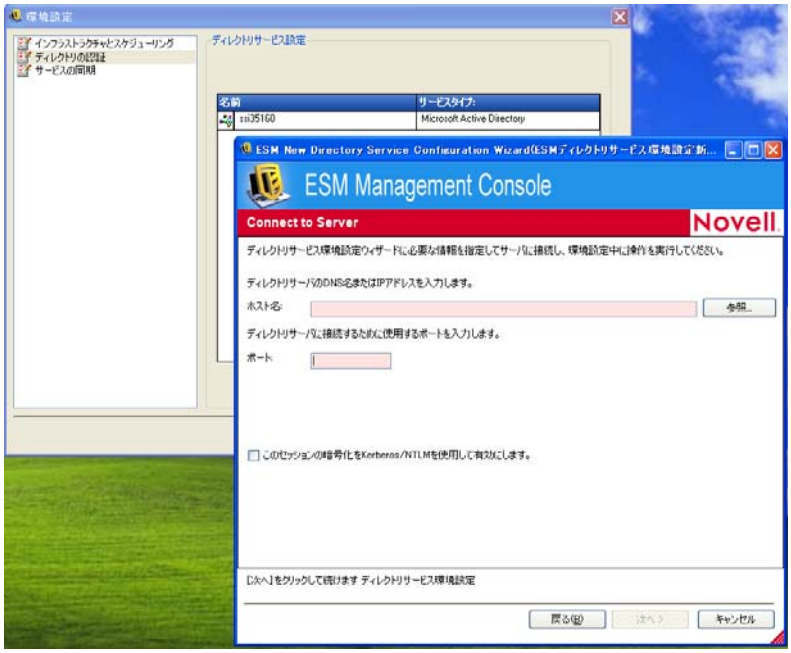
管理者の名前とパスワードを入力し、管理コンソールにログインします。ユーザ名とパスワードを入力する前に、ディレクトリサービスのドメインに接続する必要があります (49 ページのセクション 7.2.1「eDirectory サービスの追加」を参照)。ユーザ名は、管理サービスドメイン上のユーザでなければなりません。

図 7-5 ZENworks Endpoint Security Management の管理コンソールにログインします。

7.2.1 eDirectory サービスの追加

1 ログイン画面の［オプション］ボタンをクリックすると［Configuration (環境設定)］ウィンドウが表示されます。

図 7-6 ディレクトリの認証



2 ディレクトリサービスに対してわかりやすい名前を入力して、［Service Type (サービスタイプ)］ドロップダウンリストから［eDirectory］を選択します。

3 ［Host/DN (ホストサーバ / ドメイン名)］フィールドで eDirectory サーバの IP アドレスを指定し、［Domain tree (ドメインツリー)］にツリー名を指定します。>

4 ［Available for User Authentication (ユーザ認証に使用)］チェックボックスをオンにすると、ログインのドロップダウンメニューにこのドメインが表示されます。

5 ［Service Connection Options (サービス接続オプション)］の［Secure Authentication (セキュリティで保護された認証)］チェックボックスをオフにします。>

6 アカウント名を LDAP 形式で指定します。たとえば「cn=admin,o=acmeserver」の場合、cn はユーザ、o はユーザアカウントが格納されるオブジェクトです。

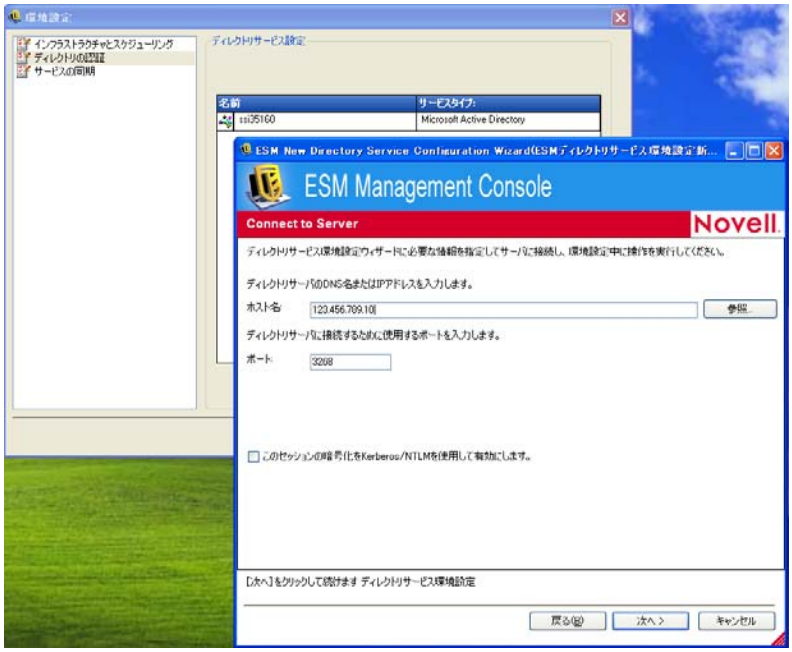
7 アカウントのパスワードを指定します。

注 : パスワードは期限がないように設定される必要があります。また、このアカウントは無効にならないように設定する必要があります。

---

8 ［テスト］をクリックし、このディレクトリサービスに対する通信を確認します。通信を確立できない場合、ユーザにエラーが通知されます。不正確な情報がある場合、可能であればテスト時にインタフェースにより修正されます。

図 7-7 入力が完了したディレクトリ画面



9 ［保存］をクリックしてこのディレクトリサービスをデータベースに追加し、［New (新規)］をクリックして別のディレクトリサービスをデータベースに追加します。>

10 ［OK］をクリックします。または［キャンセル］をクリックすると、［環境設定］ウィンドウが終了し、ログイン画面に戻ります。>

サポートされている Active Directory および NT ドメインサービスを含む、他のディレクトリサービスに対するリッスンの設定については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

7.2.2 管理コンソールの許可設定

［Permissions (許可)］は管理コンソールの［Tools (ツール)］メニューにあり、管理サービスのプライマリ管理者と、その管理者がアクセス許可を与えたユーザだけがアクセスできます。> このコントロールは、スタンドアロン管理コンソールの実行中は使用できません (詳細については 81 ページの第 11 章「非管理対象モードでの ZENworks Endpoint Security Management のインストール」を参照してください)。

許可設定では、管理コンソールへのアクセスと、「Publish Policies (ポリシーの公開)」および「Change Permission (許可の変更)」の設定を許可するユーザまたはユーザのグループを定義します。

管理サーバのインストール時に、管理者またはリソースアカウントの名前を設定フォームに入力します。テストが正常に実行され、ユーザ情報が保存されると、許可がユーザに自動的に付与されます。

管理コンソールをインストールすると、ドメイン内のすべてのユーザグループに完全な許可が与えられます。リソースユーザは、アクセスを許可するグループおよびユーザ以外の許可を取り消す必要があります。リソースユーザは、指定したユーザに対し、他の許可を設定することができます。パーミッションが付与されると、次のような結果になります。

- **管理コンソールへのアクセス :** ユーザはポリシーとコンポーネントを表示したり、既存のポリシーを編集したりすることができます。この特権しか付与されていないユーザは、ポリシーを追加または削除することはできません。また、公開および許可のオプションを使用することはできません。
- **ポリシーの公開 :** ユーザは割り当てられたユーザおよびグループに対してのみ、ポリシーを公開できます。
- **許可の変更 :** ユーザはすでに定義されている他のユーザの許可設定にアクセスして、その設定を変更することができます。また、新しいユーザに許可を付与することができます。
- **ポリシーの作成 :** ユーザは管理コンソールで新しいポリシーを作成できます。
- **ポリシーの削除 :** ユーザは管理コンソールで任意のポリシーを削除できます。

注 : セキュリティ上の理由から、「Change Permission (許可の変更)」および「Delete Policies (ポリシーの削除)」許可は、リソースユーザまたはごく少数の管理者にのみ付与することをお勧めします。

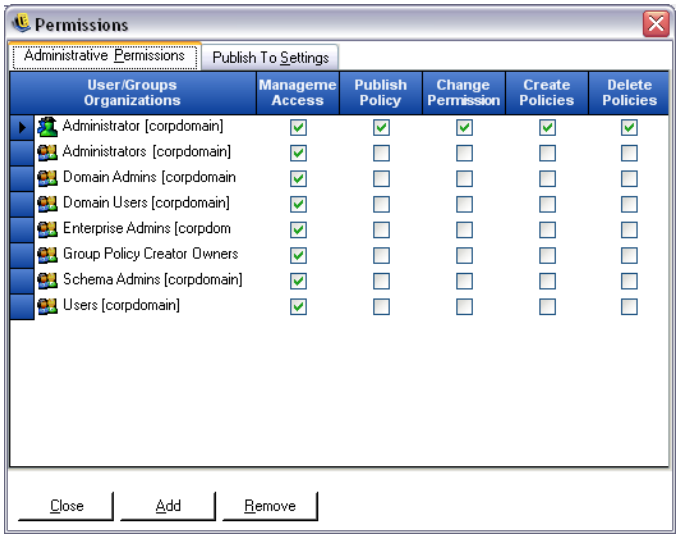
詳細情報については、以下を参照してください。

- 51 ページの 「管理に関する許可の設定」
- 53 ページの 「[Publish To Settings (公開先の設定)] の設定」

管理に関する許可の設定

1 [ツール] > [Permissions (許可)] をクリックします。>
このドメインに関連付けられているグループが表示されます。

図 7-8 管理コンソールの許可設定ウィンドウ



注 : デフォルトでは、すべてのグループに管理コンソール内での完全な許可が与えられます。管理者は、認証されていないグループについて、すべてのポリシータスクのチェックボックスを直ちにオフに必要があります。コンソールに対するアクセスの許可は、その許可チェックボックスをオフにすることで取り消すことができます。

2 (オプション) ユーザおよび新規グループをこのリストにロードするには、次の操作を実行します。

2a 画面下部の［追加］ボタンをクリックすると、［Organization (構成)］テーブルが表示されます。

図 7-9 パーミッションの設定の組織テーブル

2b リストから適切なユーザとグループを選択します。複数のユーザを選択する場合は、<Ctrl> キーまたは <Shift> キーを使用します。

2c すべてのユーザとグループを選択したら、［OK］ボタンをクリックして［Permissions (許可)］フォームの欄にユーザとグループを追加します。

3 使用可能なユーザとグループに許可を割り当てます。

選択したユーザまたはグループを削除するには、名前を選択して［削除］をクリックします。

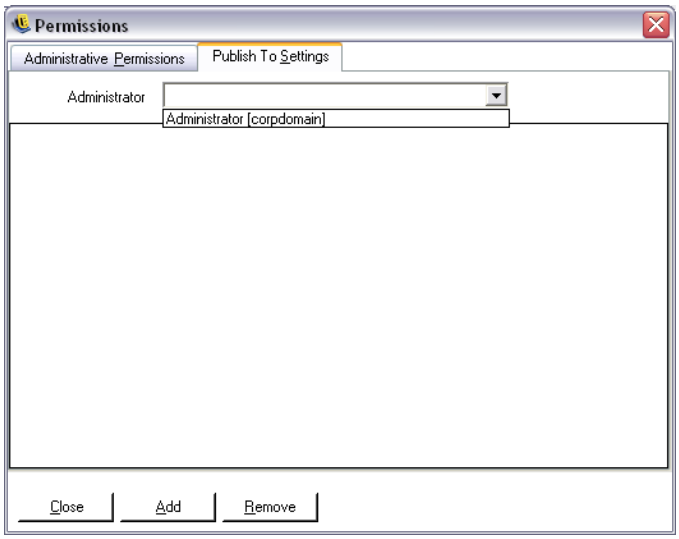
［Publish To Settings (公開先の設定)］の設定

「Publish Policy (ポリシーの公開)」がオンになっているユーザとグループは、公開先のユーザまたはグループとして割り当てる必要があります。［Publish To Settings (公開先の設定)］を設定するには、次の操作を実行します。

1 ［Publish To Settings (公開先の設定)］タブをクリックします。

2 ドロップダウンリストから公開の許可が付与されているユーザとグループを選択します。

図 7-10 *公開先の設定*



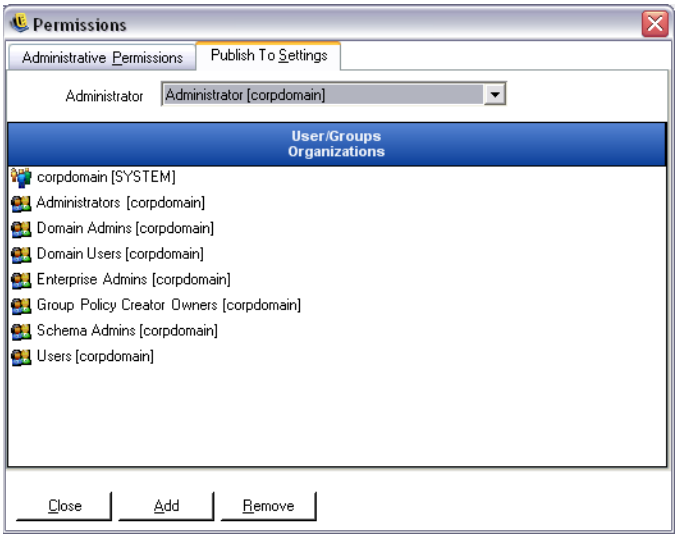
3 ユーザとグループを、このユーザまたはグループに割り当てるには、次の操作を実行します。

3a 画面下部の［追加］ボタンをクリックすると、［Organization (構成)］テーブルが表示されます。

3b リストから適切なユーザとグループを選択します。複数のユーザを選択する場合は、<Ctrl> キーおよび <Shift> キーを使用します。

3c すべてのユーザまたはグループを選択したら、［OK］ボタンをクリックします。

図 7-11 公開先リスト



選択したユーザまたはグループを削除するには、リストから名前を選択して［削除］をクリックします。

許可の設定は直ちに実装されるので、管理者が行うのは［閉じる］をクリックし、変更を承認してエディタに戻るだけです。

新しいディレクトリサービスが追加されると、リソースアカウントに対し、上記のように完全な許可が与えられます。

7.2.3 ポリシーの公開

デフォルト設定のセキュリティポリシーを公開するには、次の操作を実行します。

1. ［Create New Policy (ポリシーの新規作成)］をクリックします。
2. ポリシーの名前を指定し、［作成］をクリックします。
3. ポリシーを保存し、［公開］タブをクリックします。
4. Endpoint Security Client のユーザがツリーに表示されるようにするにはチェックインする必要があるため、左側のツリーの最上位を選択し、公開フィールドをダブルクリックして現在のすべてのグループとユーザを入力します。
5. ポリシーをポリシー配布サービスに送信するには、［公開］をクリックします。

この方法で生成されたポリシーには、次の特性があります。

- 1 つのロケーション (不明) が作成されます。
- CD/DVD ROM ドライブが許可されます。
- リムーバブルストレージデバイスが許可されます。
- すべての通信ポート (Wi-Fi を含む) が許可されます。
- ［ファイアウォール設定］、［すべてに適応］(ネットワークポートを通じたすべての送信トラフィックが許可されますが、ネットワークポートを通じた望ましくない受信トラフィックは許可されません) が含まれます。

より強力なセキュリティポリシーの作成の詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

57 ページの第 8 章「クライアントロケーション保証サービスのインストール」に進みます。

7.3 USB リーダのインストール

インストールパッケージには、管理者が許可された USB デバイスリストを作成する際に使用できる、Novell USB リーダが含まれています。

リーダをインストールするには、次の操作を実行します。

1. ［セットアップ］をクリックして、インストールを開始します。
2. ［Welcome (ようこそ)］画面で、［次へ］をクリックして続行します。
3. 使用許諾書に同意して、［次へ］をクリックします。
4. 顧客情報画面で、適当なユーザ名と組織情報を指定し、このソフトウェアへのアクセスを、このコンピュータ上のすべてのユーザに許可するか、指定したユーザだけに許可するかを選択します。
5. ［*インストール*］をクリックします。
6. ［*完了*］をクリックします。

USB リーダの使用方法の詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください。

クライアントロケーション保証サービスのインストール

8

制御されているネットワーク環境にユーザが入ったときにのみこのサーバにアクセスできるようにし、ユーザが確実に ZENworks® Security Client によって特定された環境内にいないと操作ができません。フェイルオーバおよび冗長性の設定方法については後で説明します。クライアントロケーション保証サービス (CLAS) は必要に応じて、シングルサーバインストールまたはマルチサーバ管理サービスインストールをホストするサーバと同じサーバに展開できます。

暗号化の検証を必要とするネットワーク環境にある場合にのみエンドポイントを検出できるサーバに CLAS をインストールします。

セキュリティ上および機能上の理由から、プライマリドメインコントローラ (PDC) に CLAS を展開することはできません。

注 : サーバの目的の機能には必要ないすべてのアプリケーション、サービス、アカウント、および他のオプションが無効になるように、SSI サーバを設定 (強化) することをお勧めします。このための手順はローカル環境の仕様によって異なるため、前もって説明しておくことはできません。管理者は、Microsoft Technet セキュリティセンターの Web ページ (http://www.microsoft.com/technet/security/default.mspx) の該当するセクションを参照することをお勧めします。アクセス制御に関するその他の推奨事項は、『*ZENworks Endpoint Security Management 管理ガイド*』に記載されています。

信頼されたマシンに対するアクセスのみを保護するために、仮想ディレクトリおよび IIS に ACL を設定できます。次の記事を参照してください。

- 「Granting and Denying Access to Computers (コンピュータへのアクセスの許可および拒否) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)」
- 「Restrict Site Access by IP Address or Domain Name (IP アドレスまたはドメイン名によるサイトアクセスの制限) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)」
- 「IIS FAQ: 2000 IP address and domain name restrictions (IIS FAQ: 2000 IP アドレスおよびドメイン名の制限) (http://www.iisfaq.com/default.aspx?View=A136&P=109)」
- 「Working With IIS Packet Filtering (IIS パケットフィルタリングの使用) (http://www.15seconds.com/issue/011227.htm)」

セキュリティ上の理由から、次のデフォルトのフォルダを IIS のインストールから削除することを強くお勧めします。

- IISHelp
- IISAdmin
- スクリプト
- プリンタ

microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx) で入手可能な IIS Lockdown Tool 2.1 を使用することもお勧めします。

バージョン 2.1 は、IIS に依存する主要なマイクロソフト製品用に提供されたテンプレートによって駆動されます。このサーバの役割に最も厳密に適合したテンプレートを選択してください。どれが適切かわからない場合は、Dynamic Web サーバテンプレートを使用することをお勧めします。

インストールを開始する前に、次の前提条件が満たされていることを確認してください。

- 管理サービス (MS) によるポリシー配布サービス (DS) サーバ名の解決の確認 : MS のインストール先コンピュータが DS サーバ名に対して ping を実行できることを確認します (DS サーバ名は、DS がネットワークファイアウォール内に設定される場合は NETBIOS、ファイアウォール外部の DMZ にインストールされる場合は FQDN になります)。
- Microsoftインターネットインフォメーションサービス(IIS)を有効にするかインストールして、ASP.NET が確実に動作するようにします。

  重要 :［セキュリティで保護された通信］ページの［*セキュリティで保護されたチャネルを要求する (SSL)*］チェックボックスは有効にしないでください (Microsoft コンピュータの管理ユーティリティで、［*サービスとアプリケーション*］>［*Internet Information Services (ISS) Manager (インターネットインフォメーションサービス (IIS) マネージャ)*］>［*Web サイト*］の順に展開し、［*既定の Web サイト*］を右クリックし、［*プロパティ*］>［*ディレクトリセキュリティ*］タブ >［セキュリティで保護された通信］グループボックスの［*編集*］ボタンの順にクリックします)。このオプションを有効にすると、Zenworks Endpoint Security Management サーバとエンドポイント上の Zenworks Endpoint Security Client との通信が切断されます。

［Installation Interface (インストールインタフェース)］メニューの［Client Location Assurance Service Installation (クライアントロケーション保証サービスのインストール)］をクリックします。CLAS のインストールが開始されます。

起動時にインストーラは、必要なすべてのソフトウェアがサーバ上にあるかどうかを確認します。必要なソフトウェアがインストールされていない場合は、［Welcome (ようこそ)］画面に移行する前に自動的にソフトウェアがインストールされます (追加するソフトウェアのライセンス契約の受諾が必要になる場合があります)。Microsoft Data Access Components 2.8 がインストールされていない場合は、MDAC のインストール後にサーバを再起動しないと、ZENworks Endpoint Security Management のインストールを続行できません。Windows 2003 Server を使用している場合は、ASP.NET 2.0 を実行するように設定されます。

8.1 インストール手順

CLAS をインストールしてライセンスキーを作成するには、次の操作を実行します。

1. ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。
2. 使用許諾書に同意して、［次へ］をクリックします。
3. デフォルトのディレクトリである \Program Files\Novell\ESM CLAS に、ファイルがコピーされます。
4. クライアントロケーション保証サービスをインストールすると、privatekey (プライベートキー) と publickey (パブリックキー) という 2 つのキーが生成されます。publickey ファイルは、デスクトップまたは別のディレクトリに格納できます。

publickey ファイルを別のディレクトリに格納する場合は、［はい］をクリックし、目的のフォルダに移動します。デフォルト値を受け入れて publickey ファイルを privatekey ファイルと同じ場所に格納する場合は、［いいえ］をクリックします。

5 ［終了］をクリックし、インストールプログラムを終了します。

パブリックキーは管理サービスからアクセスできるようにする必要があります。

8.2 CLAS のフェイルオーバインストール

CLAS を企業全体の複数のサーバにインストールして、企業の複数のロケーションを暗号化により保証したり、プライマリ CLAS サーバがダウンしたときにロケーションを保証したりすることができます。

2 番目のシナリオでは、秘密鍵は IP アドレスではなく URL に基づいて配置されます。したがって、1 つの URL を共有する複数のサーバのブロックを設定することができます。CLAS を 1 台のサーバにインストールして、そのサーバのイメージを他のサーバにコピーできます。また、CLAS を各サーバに個別にインストールして、プライベートキーとパブリックキーを他のサーバにコピーすることもできます。同じ URL を共有するサーバはすべて、同じプライベートキーとパブリックキーを持っていなければなりません。

8.3 管理サービスへの公開鍵の転送

インストールが完了すると、生成された公開鍵は、セキュリティポリシーを通じて Endpoint Security Client に転送され、サーバの \Program Files\Novell\Novell ESM CLAS ディレクトリに置かれます。パブリックキーは、publickey というファイル名で識別されます。このファイル名は任意の名前に変更できます。

次に、publickey ファイルをコピーして管理サービス (サービスの任意の場所) に転送する必要があります。これにより、管理コンソールがセキュリティポリシーを通じてすべての Endpoint Security Client に公開鍵を配布できるようになります。ZENworks Endpoint Security Management 管理コンソールが動作している PC に publickey ファイルをロードすることもできます。

61 ページの第 9 章「Endpoint Security Client 3.5 のインストール」に進みます。

Endpoint Security Client 3.5 のインストール

9

Windows XP (SP1 と SP2) および Windows 2000 SP4 クライアント用の Novell ZENworks Endpoint Security Client 3.5 を使用します。［*Installation Interface (インストールインタフェース)*］メニューで、適切な ZENworks Security Client インストーラをクリックします。Endpoint Security Client のインストールが開始されます。以降のページでは、基本インストールと MSI インストールの両方のインストールプロセスについて説明します。

- 基本インストールでは、現在のマシンにのみ Endpoint Security Client 3.5 がインストールされます。
- MSI インストールでは、インストーラが管理モード (/a) で起動され、ソフトウェアの MSI パッケージが作成されます。このパッケージはその場で適用できます。また、必要なユーザ入力情報を事前に設定した上で、指定したネットワークロケーションで使用できるようにすることもできます。これにより、個々のユーザは、定義済みのサーバの値を使用してソフトウェアをインストールできるようになります。

9.1 Endpoint Security Client 3.5 の基本インストール

この手順では、現在のマシンにのみ Endpoint Security Client 3.5 がインストールされます。

Microsoft およびウィルス対策ソフトウェア用のすべてのセキュリティパッチがインストールされ、最新の状態になっていることを確認してください。

管理サービスの SSL ルート証明書 (ESM-MS.cer またはエンタープライズ証明書) をローカルマシンにインストールします。

注 : Endpoint Security Client 3.5 のインストール中は、有効なレジストリ機能と対話しているウイルス対策またはスパイウェア対策ソフトウェアをシャットダウンすることをお勧めします。

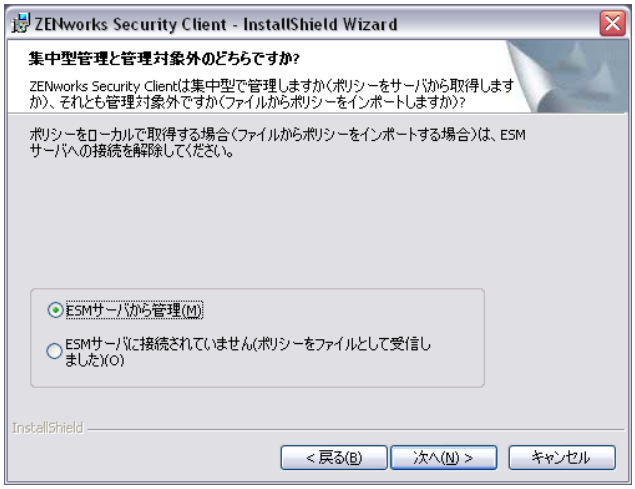
---

1. ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。
2. 使用許諾書に同意して、［次へ］をクリックします。
3. インストールパスワードを入力します。これにより、［*プログラムの追加と削除*］を使用して Endpoint Security Client 3.5 がアンインストールされるのを防止できます (推奨)。

図 9-1 アンインストールパスワード

4 ポリシーを受け取る方法を選択します (管理対象クライアントの場合は配布サービスから、非管理対象設定の場合はローカルで取得します。非管理対象の詳細については 81 ページの第 11 章「非管理対象モードでの ZENworks Endpoint Security Management のインストール」を参照してください)。

図 9-2 管理設定



5 管理サービス情報を指定します。

6 ユーザ用またはマシン用 (マシンベースポリシー) のどちらのポリシーを取得するかを選択します。

図 9-3 ユーザベースポリシーまたはマシンベースポリシー

7 ［*インストール*］をクリックします。

ソフトウェアがインストールされると、マシンを再起動するよう求められます。

注 : インストールを実行する前に、setup.exe と同じフォルダに、管理サービス用の証明書をコピーすることもできます。その場合は、証明書が自動的にマシンにインストールされます (たとえばすべてのユーザに対して)。Novell の license.dat ファイルに対してもこの手順を実行することができます。

9.2 MSI のインストール

この手順により、Endpoint Security Client 3.5 用の MSI パッケージが作成されます。このパッケージは、システム管理者が Active Directory ポリシーまたはその他のソフトウェア配布方法を通じてインストールをユーザのグループに公開する際に使用されます。

MSI パッケージを作成するには、次の操作を実行します。

CD または ISO マスタインストーラを使用してインストールを行い、コマンドライン変数 (66 ページのセクション 9.2.1「コマンドライン変数」を参照) を実行しない場合の手順は、次のとおりです。

1 CD を挿入し、マスタインストーラが起動するまで待ちます。
2 ［Product Installation (製品のインストール)］をクリックします。
3 ［Security Client］をクリックします。
4 ［Create ZSC MSI Package (ZSC MSI パッケージの作成)］をクリックします。

インストールに setup.exe ファイルのみを使用する場合の手順は、次のとおりです (実行可能プログラムは CD の D:\ESM32\ZSC にあります)。

1 setup.exe を右クリックします。
2 ［ショートカットの作成］を選択します。
3 ショートカットを右クリックし、［プロパティ］をクリックします。

4 ［リンク先］フィールドの最後の二重引用符の後に、スペースバーを 1 回押して、?/a? と入力します。

例 : "C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a

MSI インストールではいくつかのコマンドライン変数を使用できます。詳細については、66 ページのセクション 9.2.1「コマンドライン変数」を参照してください。

5 *［OK］*をクリックします。

6 ショートカットをダブルクリックすると、MSI インストーラが起動されます。

インストールが開始されたら、次の操作を実行します。

1 ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。

2 使用許諾書に同意して、［次へ］をクリックします。

3 アンインストールパスワードが必要かどうかを選択し、パスワードを入力します (パスワードを必要とするよう設定することをお勧めします)。

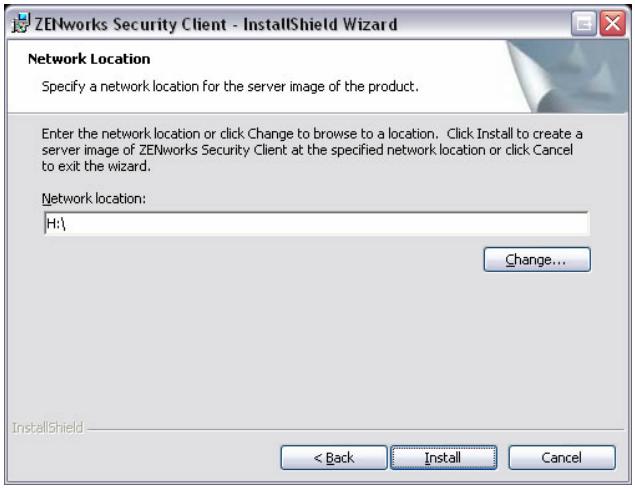
4 ポリシーを受け取る方法を選択します (管理対象クライアントの場合は配布サービスから、非管理対象設定の場合はローカルで取得します)。管理対象クライアントを選択した場合は、次の操作を行います。

- 管理サービス情報を入力します (管理サービスのインストール時に指定した方法に従い、FQDN または NETBIOS 名を指定してください)。
- これらのポリシーをユーザベースポリシーにするかマシンベースポリシーにするかを選択します。

5 (オプション) 表示されているフィールドに、インストールが失敗した場合の通知先電子メールアドレスを指定します。

6 MSI イメージが作成されるネットワークのロケーションを指定するか、［Change (変更)］ボタンをクリックしてそのロケーションに移動します。

図 9-4 *MSI イメージのネットワークロケーションの選択*

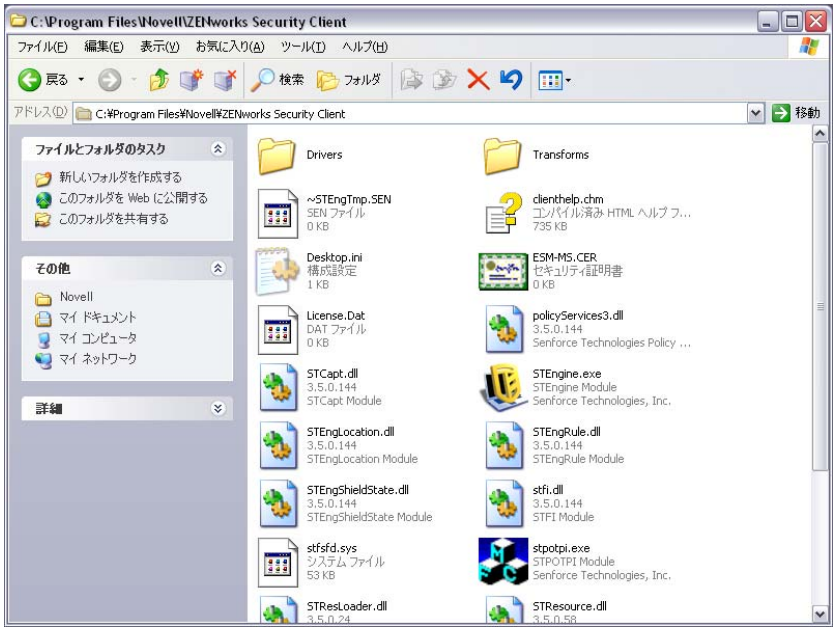


7 ［Install (インストール)］をクリックして MSI イメージを作成します。

8 作成した MSI イメージに移動し、「\program files\Novell\ZENworks Security Client\」フォルダを開きます。

9 管理サービスの SSL 証明書 (ESM-MS.cer またはエンタープライズ証明書) と Novell ライセンスキーをこのフォルダにコピーして、現在フォルダにあるデフォルトの 0KB のファイルと置き換えます。ESM-MS SSL 証明書は、ZENworks Endpoint Security Management Setup Files フォルダにあります。ライセンスキーは、別途電子メールで送信されます (30 日間の評価版を使用している場合は、この時点でライセンスキーは必要ありません)。

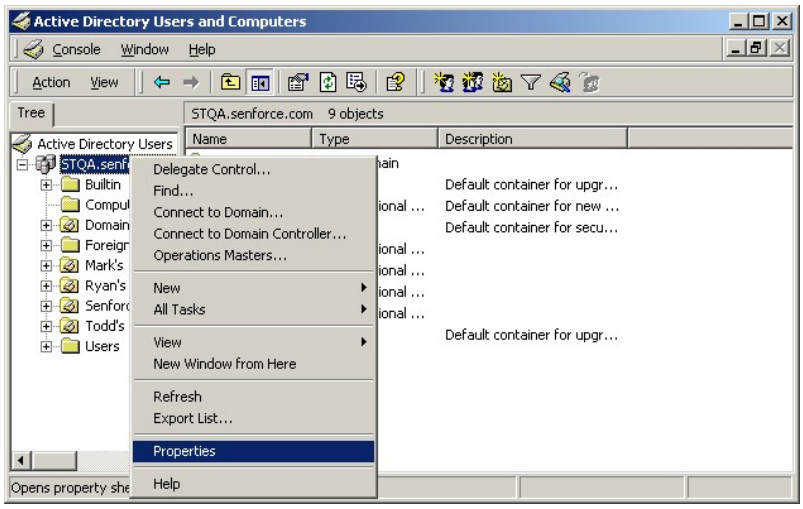
図 9-5 MSI パッケージのデフォルトファイルの置き換え



MSI パッケージをグループポリシーなどのユーザグループに渡すには、次の操作を実行します。

1 管理ツールを開き、Active Directory ユーザとコンピュータを開いて、ルートドメインのプロパティまたは OU のプロパティを開きます。> >

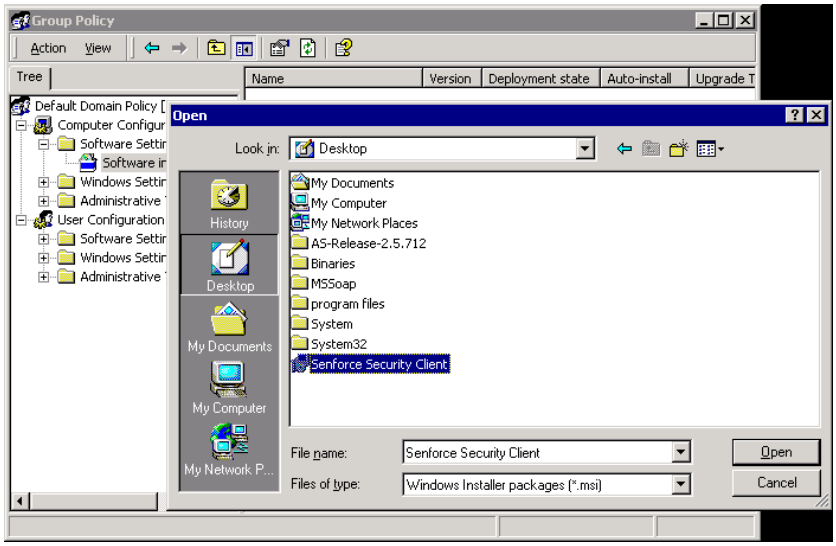
図 9-6 ルートドメインまたは OU のプロパティを開く



2 ［グループ ポリシー］タブをクリックし、［編集］をクリックします。>

3 MSI パッケージをコンピュータ設定に追加します。

図 9-7 追加する MSI パッケージの選択



9.2.1 コマンドライン変数

MSI のインストールでは、コマンドライン変数オプションを使用できます。これらの変数は、管理者モードで実行するように設定されている実行可能プログラムのショートカットで指定しなければなりません。変数を使用する場合は、MSI ショートカットに次のコマンドラインを入力する必要があります。“...\setup.exe” /a /V"variables"。

次のいずれかのコマンドを入力し、疑問符で囲みます。変数が複数ある場合は、間にスペースを 1 つ入力して変数を区切ります。

例 : 「setup.exe /a /V"STDRV=stateful STBGL=1"」を使用すると、MSI パッケージが作成されます。このパッケージでは、厳格なホワイトリストが適用され、Endpoint Security Client 3.5 が［All Stateful (すべてステートフル)］で起動します。

注 : ステートフルで起動した場合、相互運用性に関する問題が発生する可能性があります (DHCP アドレスの遅延、Novell ネットワークの相互運用性の問題など)。

次のコマンドライン変数を使用できます。

表 9-1 *コマンドライン変数*

コマンドライン変数	説明	メモ
STDRV=stateful	起動時に NDIS ドライバをすべてステートフルにします。	Endpoint Security Client 3.5 によってそのロケーションが決定されるまで、起動時に NDIS ドライバのデフォルトの状態を［すべて開く］から、すべてのネットワークトラフィックを許可する［All Stateful (すべてステートフル)］に変更します。
/qn	クワイエットインストールを実行します。	標準の MSI インストールプロセスを非表示にするために使用します。Endpoint Security Client 3.5 は、ユーザが次回再起動を行った場合に有効になります。
STRBR=ReallySuppress	インストールの完了後に再起動されることはありません。	セキュリティ強制とクライアントセルフディフェンスは、最初に再起動されるまで完全には機能しません。
STBGL=1	アプリケーション制御に対して厳格なホワイトリストを適用します。	ホワイトリストに対するアプリケーションを特定するポリシーを作成し、このポリシーによって配布する必要があります。
STUPGRADE=1	Endpoint Security Client 3.5 をアップグレードします。	Endpoint Security Client 3.5 をアップグレードする場合に使用します。
STUNINSTALL=1	Endpoint Security Client 3.5 をアンインストールします。	Endpoint Security Client 3.5 をアンインストールする場合に使用します。
STUIP=”パスワード”	パスワードを使用してアンインストールします。	アンインストールパスワードが有効になっている場合に使用します。
STNMS=”MS 名”	管理サービスの名前を変更します。	Endpoint Security Client 3.5 用の管理サービス名を変更します。
POLICYTYPE=1	Endpoint Security Client 3.5 をマシンベースポリシーに切り替えます。	MSI でインストールした Endpoint Security Client を、ユーザベースポリシーではなくマシンベースポリシーを受諾するように変更するために使用します。

コマンドライン変数	説明	メモ
POLICYTYPE=2	Endpoint Security Client 3.5 をユーザベースポリシーに切り替えます。	MSI でインストールした Endpoint Security Client を、マシンベースポリシーではなくユーザベースポリシーを受諾するように変更するために使用します。
STVA=”アダプタ名”	仮想アダプタを追加します。	仮想アダプタでポリシー制御を有効にするために使用します。
/L*v c:\log.txt	ログ出力を有効にします。	インストール時にログ出力を有効にするために使用します。インストール時に有効にしなかった場合は、Endpoint Security Client 診断ツールを使用して有効にする必要があります (『Administrator’s Manual (管理者マニュアル)』を参照してください)。

9.2.2 MSI パッケージによるポリシーの配布

MSI インストールに含まれるデフォルトのポリシーを、企業で設定したポリシーに置き換えることができます。特定のポリシーを MSI イメージに適用するには、次の操作を実行します。

1. 管理コンソールを通じてすべてのユーザに配布されるポリシーを作成します (ポリシー作成の詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください)。
2. ポリシーをエクスポートし、policy.sen として保存します。

   注 : この方法で配布されたすべてのポリシー (非管理対象) には、Endpoint Security Client 3.5 が受諾できるように policy.sen という名前を付ける必要があります。名前が policy.sen でないポリシーは、Endpoint Security Client 3.5 によって実装されません。
3. ポリシーのエクスポート先のフォルダを開き、policy.sen および setup.sen ファイルをコピーします。
4. 作成した MSI イメージに移動し、「\program files\Novell\ZENworks Security Client\」フォルダを開きます。
5. policy.sen および setup.sen ファイルをフォルダに貼り付けます。これにより、デフォルトの policy.sen および setup.sen ファイルが置き換えられます。

9.2.3 ユーザによる Endpoint Security Client 3.5 の MSI インストール

(マシンを再起動して) ドメインに対するユーザの再認証が行われる際には、ログインの前に MSI インストールパッケージが実行されます。MSI インストールが完了すると、マシンが再起動され、ユーザはコンピュータにログインすることができます。Endpoint Security Client 3.5 はマシンにインストールされ、動作するようになります。

9.3 Endpoint Security Client 3.5 の実行

Endpoint Security Client 3.5 はシステムの起動時に自動的に起動されます。Endpoint Security Client 3.5 の詳細については、『*ZENworks Endpoint Security Client 3.5 ユーザガイド*』を参照してください。

ユーザが新しいエンドポイントセキュリティソフトウェアの操作について理解を深めることができるように、このユーザガイドをすべてのユーザに配布することをお勧めします。

ZENworks Endpoint Security Client 4.0 のインストール

10

Novell® ZENworks® Endpoint Security Client 4.0 は、32 ビット版 Microsoft Windows Vista Support Pack 1 および 32 ビット版 Windows Server 2008 をサポートするクライアント向けリリースです。Endpoint Security Client 4.0 では、ZENworks Endpoint Security Management 3.5 Server と管理コンソールを使用します。この結果、Windows XP は 3.5 クライアントで、Windows Vista は 4.0 クライアントでそれぞれ管理するという体制が整います。

以降のページでは、基本インストールと MSI インストールの両方のインストールプロセスについて説明します。

基本インストールでは、現在のマシンにのみ Endpoint Security Client 4.0 がインストールされます。

MSI インストールでは、インストーラが管理モード (/a) で起動され、ソフトウェアの MSI パッケージが作成されます。このパッケージはその場で適用できます。また、必要なユーザ入力情報を事前に設定した上で、指定したネットワークロケーションで使用できるようにすることもできます。これにより、個々のユーザは、定義済みのサーバの値を使用してソフトウェアをインストールできるようになります。

- 71 ページのセクション 10.1「Endpoint Security Client 4.0 の基本インストール」
- 74 ページのセクション 10.2「MSI のインストール」
- 78 ページのセクション 10.3「Endpoint Security Client 4.0 の実行」
- 78 ページのセクション 10.4「Endpoint Security Client 4.0 で未対応の機能」

10.1 Endpoint Security Client 4.0 の基本インストール

この手順では、現在のマシンにのみ ZENworks Endpoint Security Client 4.0 がインストールされます。

開始準備 :

- Microsoftおよびウィルス対策ソフトウェア用のすべてのセキュリティパッチがインストールされ、最新の状態になっていることを確認してください。Endpoint Security Client 4.0 ソフトウェアは、Windows Vista Support Pack 1 および Windows Server 2008(どちらも 32 ビット版) にインストールできます。
- Endpoint Security Client 4.0 のインストール中は、有効なレジストリ機能と対話しているウイルス対策またはスパイウェア対策ソフトウェアをシャットダウンすることをお勧めします。
- Managed Endpoint Security Client は、ZENworks Endpoint Security 管理サービスコンポーネントへの SSL 通信を必要とします。管理サービスまたはシングルサーバのインストール中に「自己署名証明書」を選択した場合は、Security Client を実行するエンドポイントに適切なコンテキスト (ローカルコンピュータコンテキストが望ましい) で証明書がインストールされている必要があります。

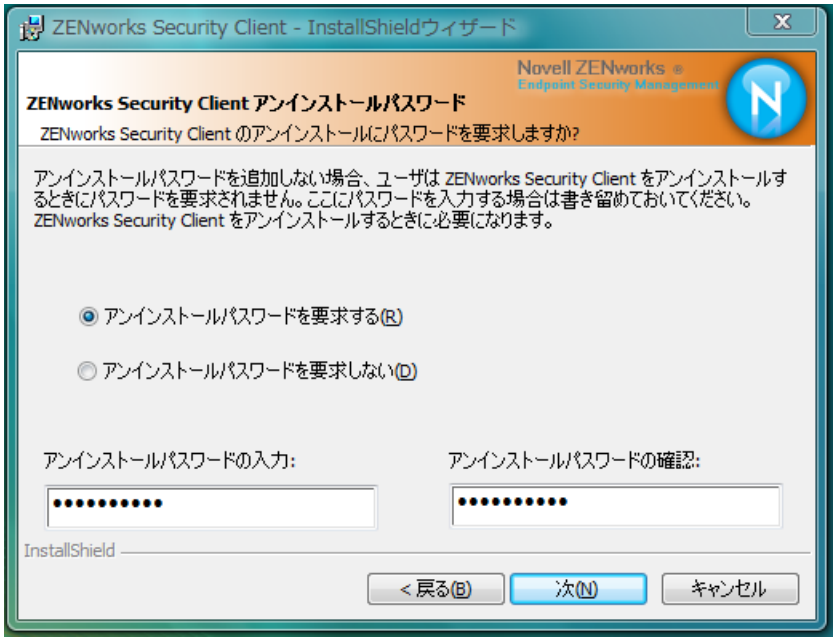
これを自動的に行うには、ESM-MS.cer ファイルを Endpoint Security Client インストーラの Setup.exe ファイルと同じフォルダに置きます。または、管理サービスインストール (またはシングルサーバインストール) の ESM Setup Files フォルダ全体を Endpoint Security Client インストーラの Setup.exe を含むフォルダにコピーすることができます (ESM-MS.cert が ESM Setup Files フォルダにあり、フォルダの名前が ESM Setup Files であることを確認してください)。その場合は、証明書が自動的にマシンにインストールされます (たとえばすべてのユーザに対して)。Novell の license.dat ファイルに対してもこの手順を実行することができます。

［Installation Interface (インストールインタフェース)］メニューで、適切な *ZENworks Security Client* インストーラディレクトリをクリックします。

1. Setup.exe をダブルクリックしてインストール処理を開始します。
2. このインストールに使用する言語を選択し、［*OK*］をクリックします。

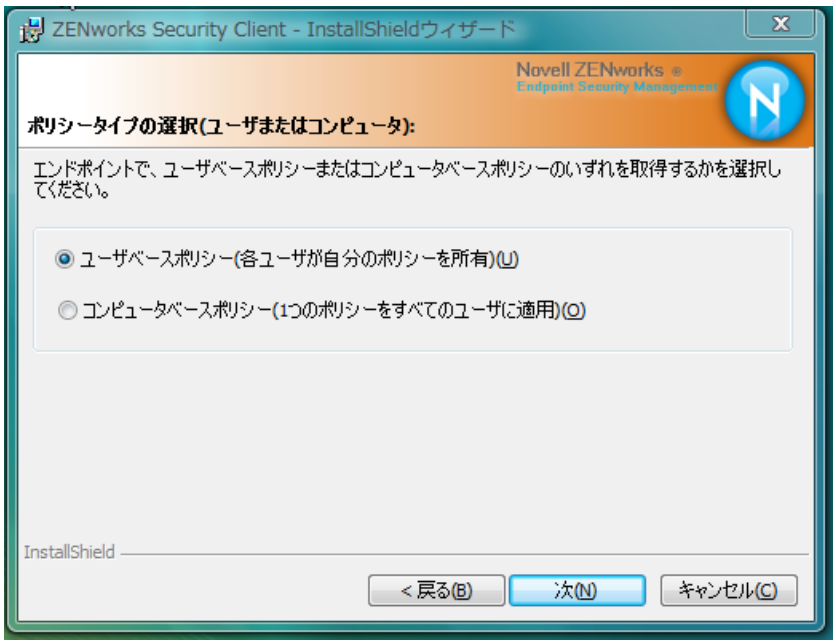
   言語の選択肢は次のとおりです。

   - 簡体字中国語
   - 繁体字中国語
   - 英語 (デフォルト)
   - フランス語
   - ドイツ語
   - イタリア語
   - 日本語
   - ポルトガル語
   - スペイン語 (トラディショナル)
3. Endpoint Security Client 4.0 では、クライアントをインストールする前に、Service Pack 3 が適用された Microsoft Web Services Enhancements (WSE) 2.0 と Microsoft Visual C++ 2008 がコンピュータにインストールされていることが必要です。インストール処理でこれらのコンポーネントが検出されない場合は、次の画面が表示されます。［*インストール*］をクリックして、これらの要件をインストールします。
4. まだ行っていない場合は、［Welcome (ようこそ)］画面で［*次へ*］をクリックする前にウイルス対策およびスパイウェア対策ソフトウェアを無効にします。
5. 使用許諾書に同意して、［*次へ*］をクリックします。



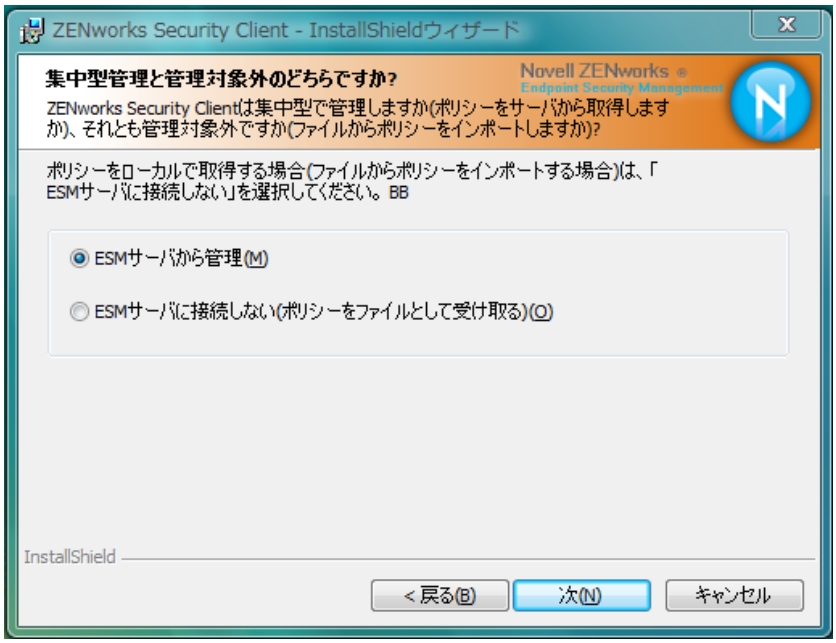
6 ［*アンインストールパスワードを要求する*］を選択します。これにより、ユーザによって Endpoint Security Client 4.0 がアンインストールされるのを防止します (推奨)。

7 アンインストールパスワードを追加し、パスワードを確認入力して、［*次へ*］をクリックします。



8 ポリシータイプ (ユーザベースポリシー (各ユーザが個別のポリシーを持つ)、またはコンピュータベースポリシー (すべてのユーザに対して 1 つのポリシーが使用される)) を選択します。［*次へ*］をクリックします。

注 : ネットワークが eDirectory をディレクトリサービスとして使用する場合はユーザベースポリシーを選択します。eDirectory はコンピュータベースポリシーをサポートしません。



9 ポリシーの受信方法 (管理対象クライアント用に ESM サーバ経由で管理されるか、管理対象外 (スタンドアロン) 環境設定用にローカルに取得されるか) を選択します。［*次へ*］をクリックします。

管理対象外インストールの詳細については、81 ページの第 11 章「非管理対象モードでの ZENworks Endpoint Security Management のインストール」を参照してください。

10 (オプション) ステップ 9 で［*ESM サーバから管理*］を選択した場合は、管理サービスをサポートするサーバの名前を入力します。

入力するサーバ名は、ZENworks Endpoint 管理サービスまたはシングルサーバをインストールしたサーバで使用される信頼できるルート証明書で指定されている「Issued To」名と一致する必要があります。これは、ZENworks Endpoint 管理サービスコンポーネントを実行しているサーバの NETBIOS 名または完全修飾ドメイン名 (FQDN) です。入力したら、［*次へ*］をクリックします。

11 インストールを開始するには、［*インストール*］をクリックします。

12 ソフトウェアがインストールされたら、指示されたところでマシンを再起動します。

Vista 用の 4.0 Client で使用できない機能の一覧については、78 ページのセクション 10.4「Endpoint Security Client 4.0 で未対応の機能」を参照してください。

10.2 MSI のインストール

この手順により、Endpoint Security Client 4.0 用の MSI パッケージが作成されます。このパッケージは、システム管理者が Active Directory ポリシーまたはその他のソフトウェア配布方法を通じてインストールをユーザのグループに発行する際に使用されます。

- 75 ページのセクション 10.2.1「マスタインストーラの使用」

- 75 ページのセクション 10.2.2「Setup.exe ファイルの使用」
- 75 ページのセクション 10.2.3「インストールの完了」
- 77 ページのセクション 10.2.4「コマンドライン変数」
- 78 ページのセクション 10.2.5「MSI パッケージによるポリシーの配布」

10.2.1 マスタインストーラの使用

CD または ISO マスタインストーラを使用してインストールを行い、コマンドライン変数を実行しない場合の手順は、次のとおりです。

1. CD を挿入し、マスタインストーラが起動するまで待ちます。
2. ［Product Installation (製品のインストール)］をクリックします。
3. ［Security Client］をクリックします。
4. ［Create ZSC MSI Package (ZSC MSI パッケージの作成)］をクリックします。
5. 75 ページのセクション 10.2.3「インストールの完了」に進みます。

10.2.2 Setup.exe ファイルの使用

インストールに setup.exe ファイルのみを使用する場合 :

1. setup.exe を右クリックします。

   実行可能ファイルは CD の D:\ESM32\ZSC にあります。
2. ［ショートカットの作成］を選択します。
3. ショートカットを右クリックし、［プロパティ］をクリックします。
4. ［*Target (ターゲット)*］フィールドの末尾の引用符の後ろで、スペースバーを 1 回押してスペースを挿入し、「/a」を入力します。

   例 : "C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a

   MSI インストールでは複数のコマンドライン変数を使用できます。詳しくは「66 ページのセクション 9.2.1「コマンドライン変数」」を参照してください。
5. *［OK］*をクリックします。
6. ショートカットをダブルクリックすると、MSI インストーラが起動されます。
7. 75 ページのセクション 10.2.3「インストールの完了」に進みます。

10.2.3 インストールの完了

マスタインストーラの使用または Setup.exe ファイルの使用を完了し、この手順を使用してクライアントのインストールを完了します。

1. ［Welcome (ようこそ)］画面で［次へ］をクリックして続行します。
2. ［*アンインストールパスワードを要求する*］(推奨) を選択し、パスワードを入力します。［*次へ*］をクリックします。

注 : MSI パッケージを通じて Endpoint Security Client をアンインストールする場合は、MSI のプロパティでアンインストールパスワードを指定する必要があります (77 ページの 図 表 10-1 を参照)。

---

3 ポリシータイプ (ユーザベースポリシー (各ユーザが個別のポリシーを持つ)、またはコンピュータベースポリシー (すべてのユーザに対して 1 つのポリシーが使用される)) を選択します。［*次へ*］をクリックします。

注 : ネットワークが eDirectory をディレクトリサービスとして使用する場合はユーザベースポリシーを選択します。eDirectory はコンピュータベースポリシーをサポートしません。

---

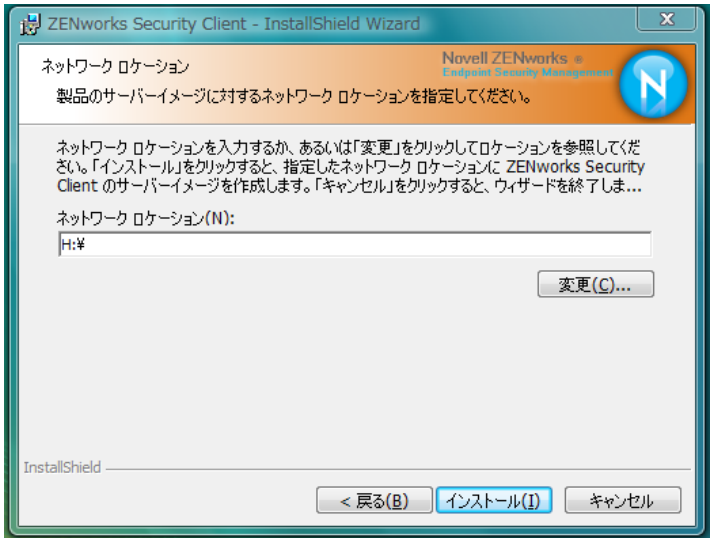
4 ポリシーの受信方法 (管理対象クライアント用に ESM サーバ経由で管理されるか、管理対象外 (スタンドアロン) 環境設定用にローカルに取得されるか) を選択します。

5 (オプション) ステップ 4 で［*ESM サーバから管理*］を選択した場合 :

- 入力するサーバ名は、ZENworks Endpoint 管理サービスまたは Single Server をインストールしたサーバで使用される信頼できるルート証明書で指定されている「Issued To」名と一致する必要があります。これは、ZENworks Endpoint 管理サービスコンポーネントを実行しているサーバの NETBIOS 名または完全修飾ドメイン名 (FQDN) です。

6 (オプション) 表示されているフィールドに、インストールが失敗した場合の通知先電子メールアドレスを指定します。

7 MSI イメージを作成するネットワークロケーションを指定するか、［*変更*］ボタンをクリックしてそのロケーションに移動して選択します。



8 ［*インストール*］をクリックして MSI イメージを作成します。［*終了*］をクリックし、セットアッププログラムを終了します。

9 MSI イメージを作成したロケーションに移動し、「\Program Files\Novell ZENworks\Endpoint Security Client\」フォルダを開きます。

10 管理サービスの SSL 証明書 (ESM-MS.cer またはエンタープライズ証明書) と Novell ライセンスキーをこのフォルダにコピーして、現在フォルダにあるデフォルトの 0KB のファイルと置き換えます。

ESM-MS SSL 証明書は、ZENworks Endpoint Security Management Setup Files フォルダにあります。ライセンスキーは別途電子メールで送信されます。60 日間の評価版を使用する場合は、ライセンスキーは必要ありません。

10.2.4 コマンドライン変数

MSI インストールではコマンドライン変数オプションを使用できます。これらの変数は、管理者モードで実行するように設定されている実行可能プログラムのショートカットで指定しなければなりません。変数を使用する場合は、MSI ショートカットに次のコマンドラインを入力する必要があります。

“...\setup.exe” /a /V"variables" 次のいずれかのコマンドを入力し、疑問符で囲みます。変数が複数ある場合は、間にスペースを 1 つ入力して変数を区切ります。

次のコマンドライン変数を使用できます。

表 10-1 *コマンドライン変数*

コマンドライン変数	説明	メモ
/qn	クワイエットインストールを実行します。	通常の MSI インストールプロセスを抑制します。Endpoint Security Client はユーザが次に再起動したときに有効になります。
SESMSG=1	暗号化ポリシーが導入されている場合は「セーフハーバー」内のファイルの暗号化を自動的に削除できないことを示すメッセージをエンドユーザに表示します。	アンインストールを「サイレント」にするために、デフォルト値は 0(メッセージを表示しない) になっています。
STRBR=ReallySuppress	インストールの完了後に再起動されることはありません。	セキュリティ強制とクライアントセルフディフェンスは、最初に再起動されるまで完全には機能しません。
STUPGRADE=1	Endpoint Security Client 4.0 をアップグレードします。	Endpoint Security Client 4.0 をアップグレードします。
STUNINSTALL=1	Endpoint Security Client 4.0 をアンインストールします。	Endpoint Security Client 4.0 をアンインストールします。
STUIP=”パスワード”	パスワードを使用してアンインストールします。	アンインストールパスワードが有効になっている場合にこの変数を使用します。
STNMS=”MS 名”	管理サービスの名前を変更します。	Endpoint Security Client 4.0 用の管理サービス名を変更します。
POLICYTYPE=1	マシンベースポリシー用に Endpoint Security Client 4.0 を変更します。	MSI によってインストールされた Endpoint Security Client を、ユーザベースポリシーではなくマシンベースポリシーを受諾するように変更します。
POLICYTYPE=2	ユーザベースポリシー用に Endpoint Security Client 4.0 を変更します。	MSI によってインストールされた Vista 用の ZENworks Security 4.0 Client を、マシンベースポリシーではなくユーザベースポリシーを受諾するように変更します。
STVA=”アダプタ名”	仮想アダプタを追加します。	仮想アダプタに対するポリシー制御を有効にします。

コマンドライン変数	説明	メモ
/L*v c:\log.txt	ログ出力を有効にします。	インストール時のログ出力を有効にします。この変数を使用しない場合、ログ出力は Endpoint Security Client 診断ツールから行う必要があります。

10.2.5 MSI パッケージによるポリシーの配布

MSI インストールに含まれるデフォルトのポリシーを、企業で設定したポリシーに置き換えることができます。特定のポリシーを MSI イメージに適用するには、次の操作を実行します。

1. 管理コンソールを通じてすべてのユーザに配布されるポリシーを作成します (ポリシー作成の詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください)。
2. ポリシーをエクスポートし、名前を policy.sen に変更します。

   この方法で配布されたすべてのポリシー (非管理対象) には、Endpoint Security Client 4.0 が受諾できるように policy.sen という名前を付ける必要があります。名前が policy.sen でないポリシーは、Endpoint Security Client 4.0 によって実装されません。
3. ポリシーのエクスポート先のフォルダを開き、policy.sen および setup.sen ファイルをコピーします。
4. 作成した MSI イメージに移動し、「\program files\Novell\ZENworks\Endpoint Security Client\」フォルダを開きます。
5. policy.sen および setup.sen ファイルをフォルダに貼り付けます。これにより、デフォルトの policy.sen および setup.sen ファイルが置き換えられます。

10.3 Endpoint Security Client 4.0 の実行

Endpoint Security Client 4.0 はシステムの起動時に自動的に起動されます。Endpoint Security Client 4.0 の詳細については、『*ZENworks Endpoint Security Client 4.0 ユーザガイド*』を参照してください。

ユーザが新しいエンドポイントセキュリティソフトウェアの操作について理解を深めることができるように、このユーザガイドをすべてのユーザに配布することをお勧めします。

10.4 Endpoint Security Client 4.0 で未対応の機能

Endpoint Security Client 4.0 で未対応の機能 (または一部のみ対応の機能) は次のとおりです。

- クライアントセルフディフェンス。
- モデム対応。
- スクリプト作成。
- ロケーション内のファイアウォールの手動変更。
- ロケーション内の複数のファイアウォールの視覚化。デフォルトのファイアウォールのみ利用可能にする機能。

- 整合性ルール。
- アプリケーションのブロック。
- マウスを置いたときの通知領域アイコンの情報が変更された。アイコンがポリシーおよびロケーション情報しか表示しない。
- USB 接続。
- Wi-Fi キーの管理。
- 有線接続が無線接続より重視されることがなくなった。
- Endpoint Security Client の更新プログラム (ポリシー別)。
- VPN 認証のタイムアウト。
- ストレージデバイスコントロールの自動再生。
- ネットワーク環境内の電話帳エントリ。

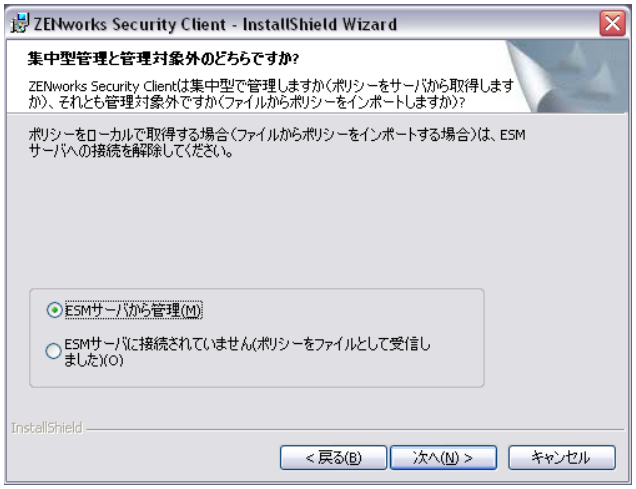
11 非管理対象モードでの ZENworks Endpoint Security Management のインストール

ZENworks® Security Client と管理コンソールを、(ポリシー配布サービスまたは管理サービスに接続されていない) 非管理対象モードで実行することができます。これは主に、単なる評価版をセットアップするためのインストールオプションとして使用できます。このオプションは、サーバスペースがほとんどまたはまったくない企業や、最低限のセキュリティを必要とする企業に適しています。ただし、クイックポリシー更新およびコンプライアンスレポートは、この設定では使用できません。

11.1 非管理対象の Endpoint Security Client のインストール

非管理対象の Endpoint Security Client をインストールするには、61 ページの第 9 章「Endpoint Security Client 3.5 のインストール」の手順に従い、[*Not Connected to ZENworks Endpoint Security Management Servers (policies received as files) (ZENworks Endpoint Security Management サーバに接続されていません (ポリシーをファイルとして受信しました))*] オプションを選択します。このインストールでは、サーバ名についての質問はバイパスされ、このマシンに Endpoint Security Client がインストールされます (非管理対象の Endpoint Security Client の場合は MSI パッケージも作成できます)。

図 11-1 *[Not Connected to ZENworks Endpoint Security Management Servers (ZENworks Endpoint Security Management Servers に接続されていません)] の選択*



11.2 スタンドアロン管理コンソ ??

この設定により、ZENworks Endpoint Security Management 管理コンソールをインストールして、外部の管理サービスに接続せずに、あるいはポリシー配布サービスを通じてポリシーを配布せずに、ポリシーを作成することができます。マスタインストーラメニューから［Stand-Alone Management Console Installation (スタンドアロン管理コンソールのインストール)］を選択し、45 ページの第 7 章「管理コンソールのインストール」の指示に従います。

インストールが開始されると、SQL データベースがインストールされます (マシン上にすでに存在する場合は、インストーラによって、代わりに適切なデータベースがセットアップされます)。データベースがインストールされると、インストール処理が停止されます。SQL データベースを有効にするには、マシンを再起動する必要があります。再起動すると、インストールが再開されます。

レポートを除き、ほとんどのポリシー機能を展開に使用できます。エクスポートされたすべてのポリシーファイルを、Endpoint Security Client の \Program Files\Novell\ZENworks Security Client\ ディレクトリに配布する必要があります。

11.3 管理されていないポリシーの配布

管理されていないポリシーを配布するには、次の操作を実行します。

1. 管理コンソールの setup.sen ファイルを探して別のフォルダにコピーします。

   setup.sen ファイルは、管理コンソールのインストール時に生成され、\Program Files\Novell\ESM Management Console\ ディレクトリに配置されます。
2. 管理コンソールでポリシーを作成します (詳細については、『*ZENworks Endpoint Security Management 管理ガイド*』を参照してください)。
3. ［*エクスポート*］コマンドを使用して、setup.sen ファイルが含まれているフォルダにポリシーをエクスポートします。Endpoint Security Client が受諾できるように、配布されるすべてのポリシーに policy.sen という名前を付ける必要があります。
4. policy.sen と setup.sen ファイルを配布します。これらのファイルは、すべての非管理対象クライアントの \Program Files\Novell\ZENworks Security Client\ ディレクトリにコピーする必要があります。

   setup.sen ファイルは、最初のポリシーと共に、非管理対象のデバイスに 1 回だけコピーする必要があります。その後、新しいポリシーのみを配布する必要があります。

非管理対象の Endpoint Security Client がスタンドアロン管理コンソールと同じマシンにインストールされている場合は、setup.sen ファイルも \Program Files\Novell\ZENworks Security Client\ ディレクトリにコピーする必要があります。非管理対象の Endpoint Security Client がスタンドアロンエディタの後にマシンにインストールされている場合は、すでに説明したように、ファイルを手動で転送する必要があります。

［*公開*］ボタンをクリックすると、直ちにポリシーがそのマシンの非管理対象の Endpoint Security Client に公開されます。複数の非管理対象ユーザにポリシーを配布するには、前に説明したエクスポート機能を使用してください。

マニュアルの更新

A

この節では、バージョン 3.5 の最初のリリース後にこの『*Novell ZENworks Endpoint Security Management インストールガイド*』の内容に加えられた変更について説明します。変更は公開された日付順に記載されています。

この製品のドキュメントは、HTML および PDF の 2 つの形式で Web にて提供されています。HTML および PDF ドキュメントにはこのセクションに一覧表示された変更が反映され、最新の状態に保たれています。

使用している PDF ドキュメントが最新のものであるかどうかを知る必要がある場合、PDF ドキュメントの表紙の発行日を参照してください。

このドキュメントは次の日付に更新されました。

- 83 ページのセクション A.1「2009 年 1 月 5 日」

A.1 2009 年 1 月 5 日

次の節が更新されました。

ディレクトリ	Update
すべての節	ガイド全体でクライアントの名前が変更されました。現在、正式名は Novell ZENworks Endpoint Security Client です。それぞれの章で、各クライアントは Endpoint Security Client 3.5(Windows XP 用) および Endpoint Security Client 4.0(Windows Vista 用) と呼ばれています。
10 ページのセクション 1.1「システム要件」	新しい Vista クライアントおよびスタンドアロン管理コンソールのシステム要件が追加されました。
61 ページの第 9 章「Endpoint Security Client 3.5 のインストール」	Endpoint Security Client 3.5 が Windows XP 用であることを明記する情報および名前の変更が追加されました。
71 ページの第 10 章「ZENworks Endpoint Security Client 4.0 のインストール」	Endpoint Security Client 4.0(Windows Vista 用) に関する章が追加されました。