

Installation Guide

Novell® ZENworks® Endpoint Security Management

4.1

February 4, 2010

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Overview	9
1.1 Endpoint Security Solutions	10
1.2 What's New in This Release	11
1.3 Standard System Architecture	12
1.4 Optional System Architecture	13
1.5 User-Based Policies and Computer-Based Policies	14
2 Deployment Scenarios and System Requirements	15
2.1 Deployment Scenarios	15
2.1.1 Consolidated Configuration (Single Server)	16
2.1.2 Distributed Configuration (Multiple Servers)	16
2.1.3 Non-Directory Service Configuration	18
2.2 System Requirements	19
2.2.1 Server Requirements	19
2.2.2 Client Requirements	20
2.2.3 Management Console Requirements	20
2.2.4 Directory Services Requirements	21
2.2.5 SQL Server Requirements	22
3 Preparing for Installation	23
3.1 Configuring SQL Server 2005 or 2008	23
3.2 Ensuring Server Name Resolution	26
3.3 Configuring Secure (SSL) Communication	26
3.4 Securing the Management and Policy Distribution Servers	27
4 Installing the Services to a Single Server	29
5 Installing the Services on Multiple Servers	35
5.1 Installing the Policy Distribution Service	35
5.2 Installing the Management Service	39
6 Installing the Management Console	45
6.1 Installing the Management Console for Use with the Management and Policy Distribution Services	45
6.1.1 Installing the Software	45
6.1.2 Creating a Directory Service Configuration	48
6.2 Installing the Standalone Management Console	54
7 Installing the Security Client	57
7.1 Using the Installation Program (SETUP.EXE)	57
7.2 Using an MSI Package	60

7.2.1	Creating the MSI Package	60
7.2.2	Adding a Policy to the MSI Package	63
7.2.3	Distributing the MSI Package	63
7.3	Logging In	64
7.3.1	Windows 2000/XP	64
7.3.2	Windows Vista/7	65

8 Upgrading 67

About This Guide

This *Novell® ZENworks® Endpoint Security Management Installation Guide* provides complete installation instructions for the ZENworks Endpoint Security Management components and assists administrators in getting those components up and running.

The information in this guide is organized as follows:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Deployment Scenarios and System Requirements,” on page 15
- ♦ Chapter 3, “Preparing for Installation,” on page 23
- ♦ Chapter 4, “Installing the Services to a Single Server,” on page 29
- ♦ Chapter 5, “Installing the Services on Multiple Servers,” on page 35
- ♦ Chapter 6, “Installing the Management Console,” on page 45
- ♦ Chapter 7, “Installing the Security Client,” on page 57
- ♦ Chapter 8, “Upgrading,” on page 67

Audience

This guide is written for ZENworks Endpoint Security Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the [Novell Documentation Feedback site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks Endpoint Security Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks Endpoint Security Management 4.1 documentation Web site \(http://www.novell.com/documentation/zesm41\)](http://www.novell.com/documentation/zesm41).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Overview

1

In today's computing environments, the majority of new data is on endpoint devices. These devices are mobile and not always behind your perimeter security. Laptops, smart phones, MP3 players, thumb drives and other portable endpoint devices are especially vulnerable to loss and theft. Through wireless connections, endpoint devices can access networks that might not be secure.

At the same time, many users are not aware of the variety of security risks associated with their devices. Other users struggle to understand, implement, and maintain their security software.

Novell® ZENworks® Endpoint Security Management simplifies endpoint security by putting you, not your users, in control of endpoint security. The ZENworks approach is simple: help you protect your network and mobile data by enforcing endpoint security policies that address both known and unknown security risks, whether users are within or beyond the office walls.

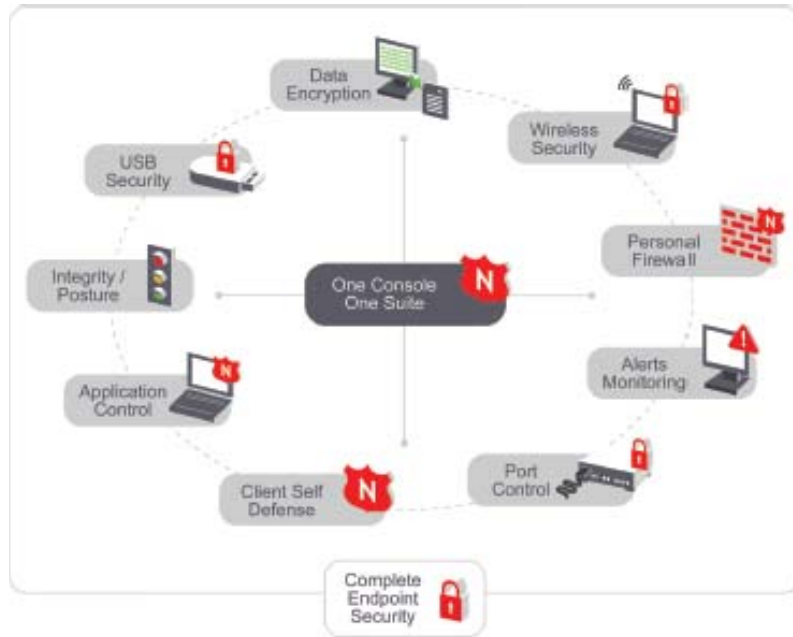
The following sections introduce you to security solutions provided by ZENworks Endpoint Security Management, the components that make up the product architecture, and the basic concepts and terminology you should know before implementing your system.

- ♦ [Section 1.1, “Endpoint Security Solutions,” on page 10](#)
- ♦ [Section 1.2, “What’s New in This Release,” on page 11](#)
- ♦ [Section 1.3, “Standard System Architecture,” on page 12](#)
- ♦ [Section 1.4, “Optional System Architecture,” on page 13](#)
- ♦ [Section 1.5, “User-Based Policies and Computer-Based Policies,” on page 14](#)

1.1 Endpoint Security Solutions

ZENworks Endpoint Security Management provides extensive endpoint security through a variety of solutions. Together, the solutions provide a fully integrated suite for perimeter-to-core endpoint protection.

Figure 1-1 Solutions Provided by ZENworks Endpoint Security Management



- ◆ **Personal Firewall:** Protects the endpoint device against hackers, malware, protocol attacks, and more. Because ZENworks Endpoint Security Management is integrated into the Network Driver Interface Specification (NDIS) driver for each network interface card (NIC), security protection is assured from the moment traffic enters the device.
- ◆ **Wireless Security:** Controls where, when, and how users can connect. You can limit wireless connectivity to authorized access points, establish a minimum level of encryption strength, or even disable wireless networking completely. You can also automatically enforce VPN policies, requiring VPN software to be running while devices connect to foreign networks such as those in hotels, hot spots and coffee shops. Rogue access point detection helps ensure wireless security in and around the office.
- ◆ **Port Control:** Secures all your endpoint communication ports and adapters, including LAN, USB, modem, Bluetooth*, infrared, 1394 (FireWire*), and serial and parallel ports.
- ◆ **Data Encryption:** Secures data stored on endpoint devices, including information stored on both fixed and removable media, by encrypting files so they can only be read by authorized users. Keys are managed transparently throughout the enterprise, requiring no end-user involvement other than getting work done in the usual way.
- ◆ **USB and Storage Device Security:** Prevents intentional or inadvertent transmission of data to removable storage devices. Storage devices such as thumb drives, iPods, cameras, printers, CD and DVD drives can be placed in read-only mode or fully disabled, while the endpoint hard drive and all network drives remain accessible and operational. White lists of specifically approved USB devices can be employed.

- ♦ **Application Control:** Determines the applications that can and cannot be used, ensuring that only approved applications run on your corporate endpoints. You can create both white lists (allowed applications) and black lists (prohibited applications), and force applications such as a VPN client to run prior to network connection.
- ♦ **Integrity and Remediation:** Verifies that designated endpoint antivirus and anti-spyware software is running and is up-to-date, whether the endpoint connects to the corporate network or the Internet. ZENworks Endpoint Security Management takes immediate action if endpoints fall out of compliance by placing them into safe, customizable quarantine states, preventing the spread of viruses or other contamination to the network. Remediation actions can also be initiated, and after compliance is confirmed, endpoints are taken out of quarantine.
- ♦ **Client Self-Defense:** Prevents the endpoint security client from being altered, hacked, or uninstalled.
- ♦ **Alerts Monitoring:** Ensures that attempts to compromise corporate security policies are reported to the Management Console so that you can promptly remediate the risk. You also get a complete suite of reporting and audit tools to ensure that users are complying with internal security policies and to document compliance of your endpoint security controls with SOX, HIPAA, and other regulatory mandates.

For additional information about these solutions, see the [ZENworks Endpoint Security Management technical white paper](http://www.novell.com/rc/docrepository/public/37/basedocument.2007-08-10.2324835973/4622065PRINT_en.pdf) (http://www.novell.com/rc/docrepository/public/37/basedocument.2007-08-10.2324835973/4622065PRINT_en.pdf).

For specific use cases for each of these solutions, see the online [ZENworks Endpoint Security Management product introduction](http://www.novell.com/products/zenworks/endpointsecuritymanagement/demo/overview/index.html) (<http://www.novell.com/products/zenworks/endpointsecuritymanagement/demo/overview/index.html>).

1.2 What's New in This Release

If you have ZENworks Endpoint Security Management 3.5, you should be aware of the following major enhancements to this 4.1 release:

- ♦ **Windows 7 Support:** The Security Client can be installed on Windows 7 computers. For a list of Security Client features that are available on Windows 7, see “[Security Client Differences Based on Windows Version](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.
- ♦ **Single-Sign On Support:** The Security Client login (on Windows XP*) integrates with the Novell Client™ to provide single sign on. When a Windows XP user logs in through the Novell Client, he or she is also logged in to the Security Client.

Single-sign on requires the Novell Client 4.91 SP5 for Windows XP/2003 with patch 491psp5_login_6.zip. You can download the client and the patch from the following sites:

- ♦ [Novell Client 4.91 SP5](http://download.novell.com/Download?buildid=qmMAWSRy5q4~) (<http://download.novell.com/Download?buildid=qmMAWSRy5q4~>)
- ♦ [Patch 491psp5_login6.zip](http://download.novell.com/Download?buildid=U_rsMN4DRnY~) (http://download.novell.com/Download?buildid=U_rsMN4DRnY~)

For additional information, see [Novell TID 7005278](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005278&sliceId=1&docTypeID=DT_TID_1_1&dialogID=119482435&stateId=0%20%20119478813) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005278&sliceId=1&docTypeID=DT_TID_1_1&dialogID=119482435&stateId=0%20%20119478813).

- ♦ **Workstation Support in Novell eDirectory:** If you have ZENworks 7 Desktop Management installed and have registered Windows 2000/XP workstations in Novell eDirectory, you can synchronize those workstations with your ZENworks Endpoint Security Management system. This enables publishing of workstation-based policies to Windows 2000/XP workstations.

Because ZENworks 7 Desktop Management does not support Windows Vista/7 workstations, publishing of workstation-based policies to Windows Vista/7 workstations is not supported.

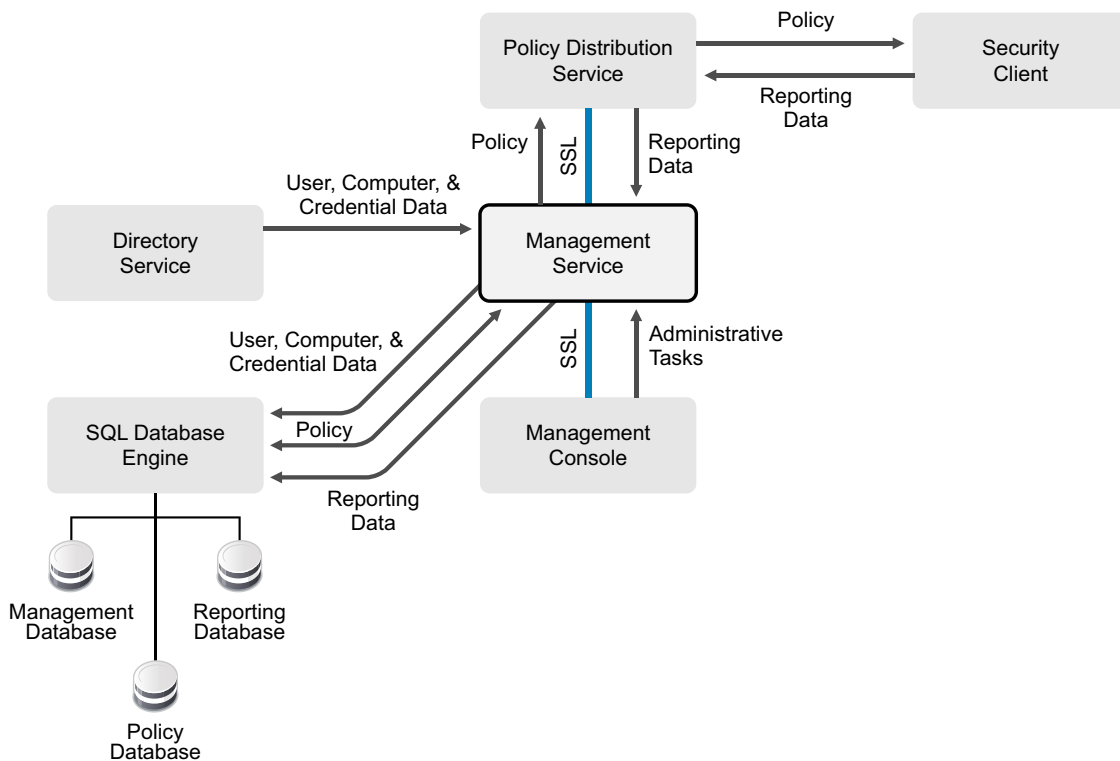
- ♦ **Device Scanner:** This utility lets you scan an endpoint device to discover USB device data. You can then import the USB device data into the Management Console for use in Storage Device Control security policies.

The Device Scanner is not included on the media image. You can download the utility from the [Novell download site](http://download.novell.com/Download?buildid=7fu1r6aVpc8~) (<http://download.novell.com/Download?buildid=7fu1r6aVpc8~>).

For information about installing and using the Device Scanner after you have downloaded it, see the [ZENworks Endpoint Security Management 4.1 Device Scanner Guide](#).

1.3 Standard System Architecture

ZENworks Endpoint Security Management consists of four primary components: the Management Service, the Policy Distribution Service, the Management Console, and the Security Client. These components combine with a directory service and an SQL database engine to form the standard system architecture.



Management Service: The central service for the Endpoint Security Management system. The Management Service interoperates with the other components to perform the following functions:

- ◆ Connects to the directory service to retrieve user, computer, and credential data. The user and computer data is used to assign policies to users and computers. The credential data is used to authenticate users or computers to the system so that they can receive their assigned policies. The Management Service retrieves the data from the directory service and stores it in the system's Management and Policy databases.
- ◆ Enables the Management Console to store created policies and policy assignments in the Management and Policy databases.
- ◆ Transfers compliance reporting data from the Policy Distribution Service and stores the data in the Reporting database.
- ◆ Transfers security policies to the Policy Distribution Service for distribution to the Security Client.
- ◆ Authenticate the Security Client (as users or computers) to the system.

Management Console: The administrative interface used to create security policies and assign them to users or computers.

Policy Distribution Service: Receives security policies from the Management Service and distributes them to the Security Client. Retrieves reporting data from the client and stores it until the Management Service transfers it to the Reporting database.

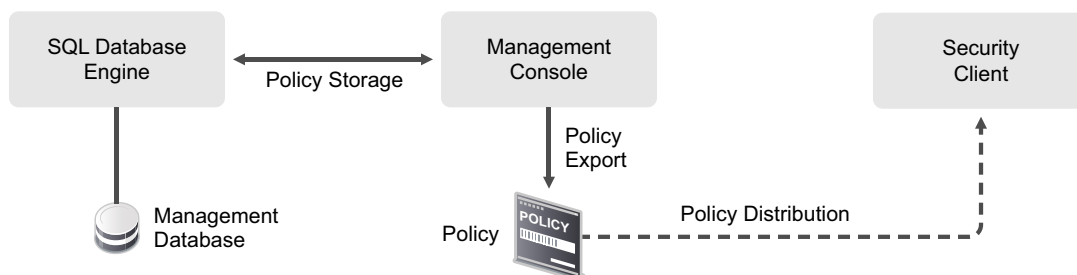
Security Client: Receives security policies from the Policy Distribution Service and enforces the policies on the device. Transfers compliance reporting data to the Policy Distribution Service.

Directory Service: Provides the user, computer, and credential data used by the Endpoint Security Management system. The Management Service uses read-only access to the directory to populate the Management database with the data required to assign security policies to users or computers and to authenticate the users or computers to the system. Microsoft* Active Directory* and Novell eDirectory are the supported directory services.

SQL Database Engine: Provides the engine for the three SQL databases (Management database, Policy database, and Reporting database) used with ZENworks Endpoint Security Management.

1.4 Optional System Architecture

ZENworks Endpoint Security Management provides an optional system architecture that does not include directory service integration. This system architecture supports environments that don't use one of the supported directory services (either Microsoft Active Directory or Novell eDirectory), don't want to integrate with a directory service, or want to evaluate the product without installing all of the components.



In this architecture, the Management Service and Policy Distribution Service are not used. Security policies are exported directly from the Management Console's database and must be copied to endpoint devices. Policy compliance reporting is not provided.

1.5 User-Based Policies and Computer-Based Policies

If you deploy the standard system architecture that provides integration with a directory service, ZENworks Endpoint Security Management supports assigning of policies to both users and computers that reside in the directory service.

A user-assigned policy is applied whenever the user logs in. If three different users log in to the same endpoint device, each user receives his or her policy during the logged-in session.

A computer-assigned policy is applied when the endpoint device authenticates to the directory service. Even if three different users log in to the same endpoint, each user receives the same policy.

When you install the Security Client on an endpoint device, you configure the client to use either user-based policies or computer-based policies. The Security Client cannot apply both types of policies to the same endpoint; you must configure it to apply one or the other.

Because user and computer data is provided by your directory service, the type of policy you use depends in part on your directory service:

- ◆ Microsoft Active Directory provides both User and Computer objects as base functionality.
- ◆ Novell eDirectory provides User objects as base functionality. Workstation objects are available only if 1) Novell ZENworks 7 Desktop Management is installed with the eDirectory schema extended to support Workstation objects, 2) the ZENworks 7 Desktop Management Agent is installed on the endpoint devices, and 3) the devices are registered as ZENworks workstations in eDirectory. Because The ZENworks 7 Desktop Management Agent is supported only on Windows 2000/XP devices, you cannot assign security policies to Windows Vista/7 devices.

For more information about directory service support, see [Section 2.2.4, "Directory Services Requirements,"](#) on page 21.

Deployment Scenarios and System Requirements

2

The following sections describe the various configurations you can use to deploy the ZENworks® Endpoint Security Management components and list the hardware and software requirements for the configurations:

- ♦ [Section 2.1, “Deployment Scenarios,” on page 15](#)
- ♦ [Section 2.2, “System Requirements,” on page 19](#)

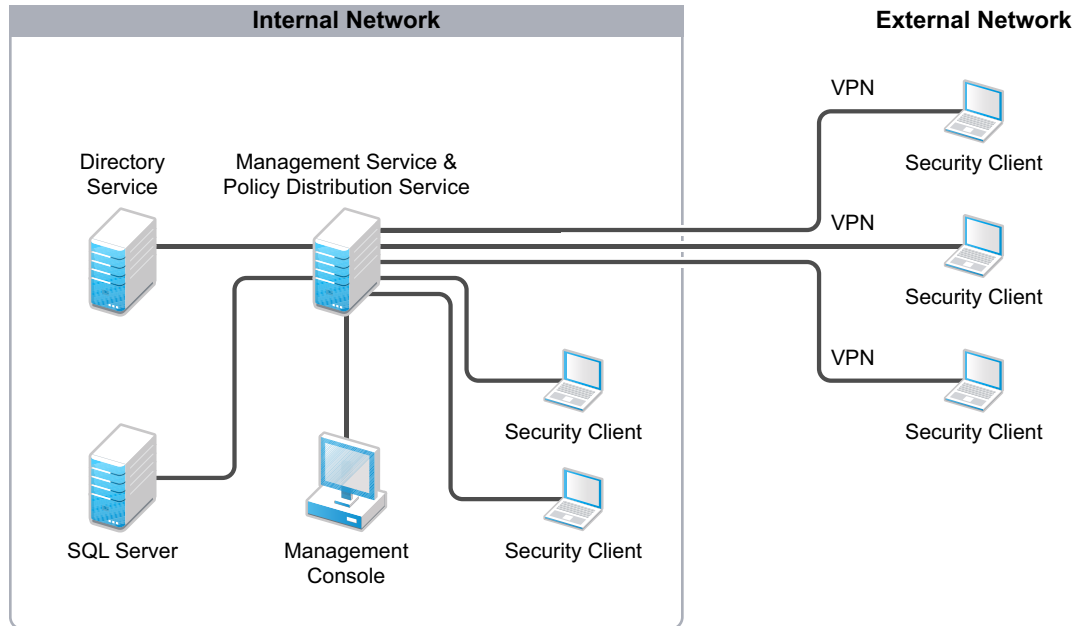
2.1 Deployment Scenarios

The ZENworks Endpoint Security Management components can be deployed in a consolidated (single server) configuration or a distributed (multiple server) configuration. In addition, a non-directory-service configuration is available that you can use if you do not have a supported directory system (Microsoft Active Directory or Novell® eDirectory™) or if you want to evaluate the product without installing all of the components.

- ♦ [Section 2.1.1, “Consolidated Configuration \(Single Server\),” on page 16](#)
- ♦ [Section 2.1.2, “Distributed Configuration \(Multiple Servers\),” on page 16](#)
- ♦ [Section 2.1.3, “Non-Directory Service Configuration,” on page 18](#)

2.1.1 Consolidated Configuration (Single Server)

In a consolidated configuration, you install both the Management Service and the Policy Distribution Service to the same server inside your corporate firewall. The Management Console can be installed on the server or on another machine that has access to the server. Likewise, the SQL database engine can be on the same server or on a dedicated SQL server.



Because the server is inside the firewall, users receive policy updates only when they are inside the firewall or connected via a VPN.

For functional, performance, and security reasons, this configuration is not supported on a Primary Domain Controller (PDC).

To create this configuration, complete the tasks in the following sections:

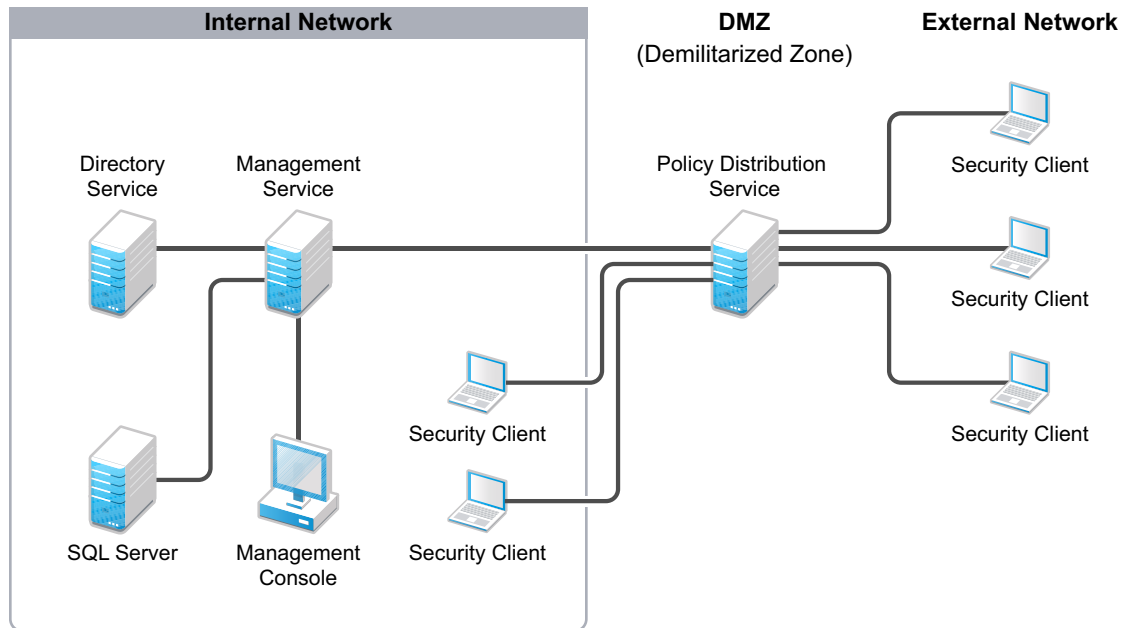
- ♦ [Chapter 4, “Installing the Services to a Single Server,” on page 29](#)
- ♦ [Chapter 6, “Installing the Management Console,” on page 45](#)
- ♦ [Chapter 7, “Installing the Security Client,” on page 57](#)

2.1.2 Distributed Configuration (Multiple Servers)

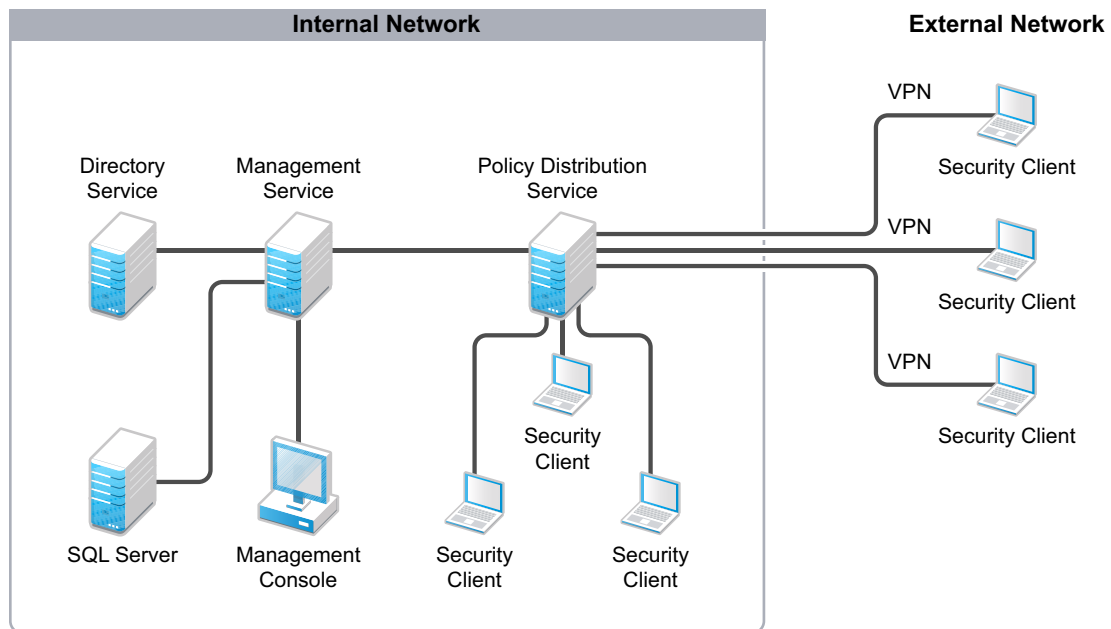
In a multi-server configuration, you install the Management Service and Policy Distribution Service to different servers. The benefits of this configuration include distributing workload between the servers and supporting external users without requiring a VPN.

You install the Management Service to a server on your internal network so that it is protected by your firewall. This enables it to securely communicate with the directory service and SQL database engine.

Where you install the Policy Distribution Service depends on the location of your users and the security requirements for your network. In the following scenario, the Policy Distribution Service is located outside of the internal network in the DMZ (demilitarized zone). This allows external users to access it without using a VPN. At the same time, internal users can still access it.



If you don't have external users, or if your external users frequently use VPN to connect to your internal network, you can place the Policy Distribution Service on a server inside your internal network, as shown in the following diagram:



To create this configuration, complete the tasks in the following sections:

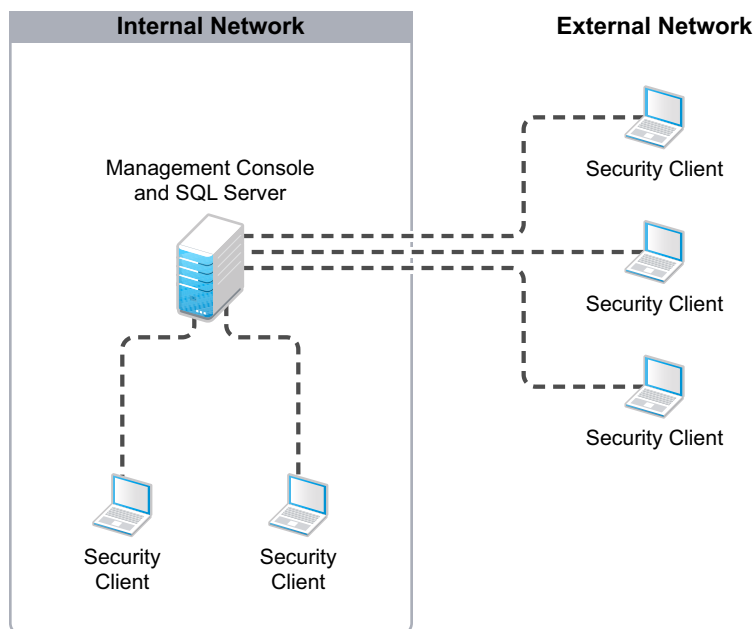
- ♦ [Chapter 5, "Installing the Services on Multiple Servers," on page 35](#)

- ♦ [Chapter 6, “Installing the Management Console,” on page 45](#)
- ♦ [Chapter 7, “Installing the Security Client,” on page 57](#)

2.1.3 Non-Directory Service Configuration

ZENworks Endpoint Security Management requires Microsoft Active Directory or Novell eDirectory as its directory service. If you don’t use one of these directory services, or if you want to evaluate the product without installing all of the ZENworks Endpoint Security Management components, you can use a non-directory service configuration.

The non-directory service configuration, as shown below, employs a standalone Management Console that writes security policies directly to the SQL databases. The SQL engine and databases must be located on the same machine as the Management Console.



The Management Service and Policy Distribution Service are not used in a non-directory service configuration. This means that:

- ♦ Automated distribution of security policies to devices is not possible. Instead, to distribute security policies, you export the policies from the Management Console and copy them to the device.
- ♦ Compliance reporting (reporting from the Security Client to the Management Console) is not available.

To create this configuration, complete the tasks in the following sections:

- ♦ [Chapter 6, “Installing the Management Console,” on page 45](#)
- ♦ [Chapter 7, “Installing the Security Client,” on page 57](#)

2.2 System Requirements

The following sections provide requirements for the ZENworks Endpoint Security Management components:

- ◆ [Section 2.2.1, “Server Requirements,” on page 19](#)
- ◆ [Section 2.2.2, “Client Requirements,” on page 20](#)
- ◆ [Section 2.2.3, “Management Console Requirements,” on page 20](#)
- ◆ [Section 2.2.4, “Directory Services Requirements,” on page 21](#)
- ◆ [Section 2.2.5, “SQL Server Requirements,” on page 22](#)

2.2.1 Server Requirements

The server (or servers) where you install the Management Service and Policy Distribution Service must meet the requirements listed in the following table:

Item	Requirement
Operating System	Microsoft Windows* Server 2003* (32-bit only).
Processor	Determined by the operating system.
Disk Space	500 MB if the Microsoft SQL database is not installed locally. If the Microsoft SQL database is local, follow the best practices outlined for SQL database disk space.
Web Server	Microsoft Internet Information Services (configured for SSL).
.NET Framework	Version 3.5,
Ports	If the Management Service and Policy Distribution Service are on different servers: <ul style="list-style-type: none">◆ The Management Service server must allow inbound and outbound traffic on the following ports: 80, 443, 53, 137-139 (if using NETBIOS to resolve names), 3091.◆ The Management Service server must allow inbound traffic on port 1433 if the Policy database is not located on the Policy Distribution Service server. This allows the Policy Distribution Service to contact the Management Service on port 1433 to access the Policy database.◆ The Policy Distribution Service server must allow inbound and outbound traffic on port 80. It must also allow outbound traffic on port 1433 if the Policy database is not on the Policy Distribution Service server; this allows the Policy Distribution Service to contact the Management Service on port 1433 to access the Policy database. <p>These ports assume that IIS is configured with the standard port assignments.</p>

In a single-server configuration (both the Management Service and the Policy Distribution Service on the same server), the server cannot be a Primary Domain Controller. See [Section 2.1.1, “Consolidated Configuration \(Single Server\),” on page 16](#).

2.2.2 Client Requirements

The endpoint devices where you install the Security Client must meet the requirements listed in the following table:

Item	Requirement
Security Client on Windows 2000 or Windows XP	<p>One of the following versions:</p> <ul style="list-style-type: none">◆ Windows 2000 SP4◆ Windows XP (32-bit) SP2 and SP3 <p>The operating system must have Windows Installer 3.1 installed and all operating system updates applied.</p> <p>Not all Security Client features are available on both operating systems. For a list of feature support based on operating system version, see “Security Client Differences Based on Windows Version” in the <i>ZENworks Endpoint Security Management 4.1 Administration Guide</i>.</p>
Security Client on Windows Vista* or Windows 7	<p>One of the following versions:</p> <ul style="list-style-type: none">◆ Windows Vista SP1 (32-bit)◆ Windows 7 (32-bit) <p>The device must have .NET 3.5 SP1 installed. Windows 7 comes with .NET 3.5 SP1, Windows Vista does not. You must update Windows Vista devices to .NET 3.5 SP1.</p> <p>Not all Security Client features are available on both operating systems. For a list of feature support based on operating system version, see “Security Client Differences Based on Windows Version” in the <i>ZENworks Endpoint Security Management 4.1 Administration Guide</i>.</p>
Processor	Determined by the operating system. The Security Client is supported only on 32-bit operating systems. However, those operating systems can be using 32-bit or 64-bit processors as supported by the operating system.
Disk Space	5 MB required, 5 additional MB recommended for reporting data.

2.2.3 Management Console Requirements

The machine where you install the Management Console must meet the requirements listed in the following table:

Item	Requirement
Operating System	Windows XP SP1 through SP3 Windows 2000 SP4 Windows Server 2003

Item	Requirement
SQL Server	If you use the standalone Management Console (meaning that you are using the non-directory service configuration), the Management Console machine must have a supported SQL server installed.
Active Directory Domain Membership	If you are using Active Directory as your directory service, the machine where you install the Management Console must be a member of the Active Directory domain to which you are connecting or have a trust relationship with the domain.

2.2.4 Directory Services Requirements

The directory service used with ZENworks Endpoint Security Management must meet the requirements listed in the following table.

Item	Requirement
Directory Service	Microsoft Active Directory Novell eDirectory (Novell Directory Services for Windows is not supported)
Active Directory Domain Controller	The Active Directory Domain Controller (for any domains you plan to connect to for user and computer data) must reside on Windows Server 2000 with SP4, Windows Server 2003, or Windows Server 2008.
eDirectory Workstation objects	ZENworks Endpoint Security Management supports policy assignment to users or computers. Active Directory provides both User and Computer objects as base functionality. Novell eDirectory provides User objects as base functionality. Workstation objects are available only all of the following are true: <ul style="list-style-type: none"> ◆ Novell ZENworks 7 Desktop Management is installed with the eDirectory schema extended to support Workstation objects. ◆ The ZENworks 7 Desktop Management Agent is installed on the endpoint devices. Because The ZENworks 7 Desktop Management Agent is supported only on Windows 2000/XP devices, you cannot assign computer-based security policies to Windows Vista/7 devices ◆ The devices are registered as ZENworks workstations in eDirectory.

2.2.5 SQL Server Requirements

The SQL server used with ZENworks Endpoint Security Management must meet the requirements listed in the following table.

Item	Requirement
Version	<p>When integrating ZENworks Endpoint Security Management with a supported directory service (Active Directory or eDirectory), you must use one of the following versions:</p> <ul style="list-style-type: none">◆ Microsoft SQL Server 2000 SP4 (Standard or Enterprise Edition)◆ Microsoft SQL Server 2005 (Standard or Enterprise Edition)◆ Microsoft SQL Server 2008 (Standard or Enterprise Edition) <p>If you are not integrating with a supported directory service (meaning that you are using the non-directory service configuration), you must use one of the following versions and it must be installed on the same machine as the Management Console:</p> <ul style="list-style-type: none">◆ Microsoft SQL Server 2000 SP4 (Express, Standard, or Enterprise Edition)◆ Microsoft SQL Server 2005 (Express, Standard, or Enterprise Edition)◆ Microsoft SQL Server 2008 (Express, Standard, or Enterprise Edition)
Authentication Mode	Server authentication must be set to mixed mode to allow both SQL Server and Windows Authentication mode authentication

Preparing for Installation

3

Before you begin installing your ZENworks® Endpoint Security Management system, prepare your network environment by completing the tasks in the following sections:

- ♦ Section 3.1, “Configuring SQL Server 2005 or 2008,” on page 23
- ♦ Section 3.2, “Ensuring Server Name Resolution,” on page 26
- ♦ Section 3.3, “Configuring Secure (SSL) Communication,” on page 26
- ♦ Section 3.4, “Securing the Management and Policy Distribution Servers,” on page 27

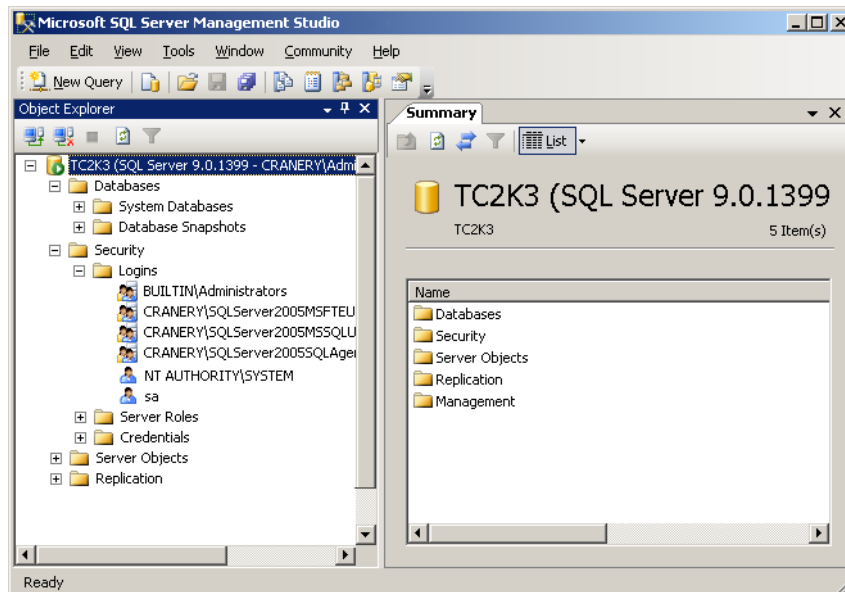
3.1 Configuring SQL Server 2005 or 2008

If you are using Microsoft SQL Server 2005 or Microsoft SQL Server 2008, you need to configure your SQL server to support ZENworks Endpoint Security Management. The graphics in the following procedure show SQL Server 2005, but the configuration steps are the same for SQL Server 2008.

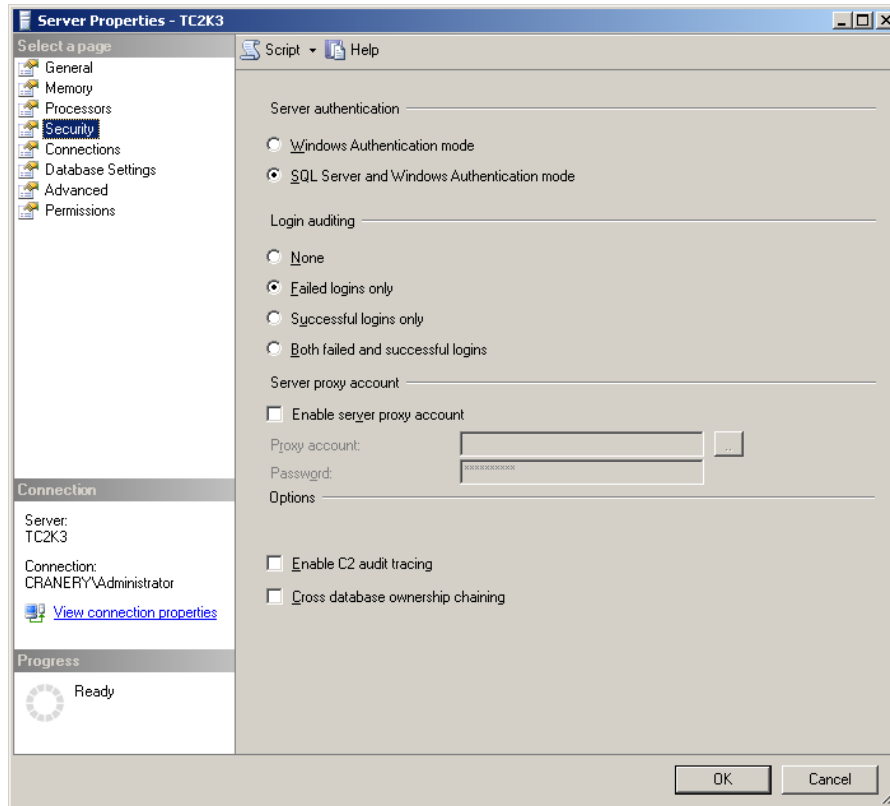
- 1 Make sure you have Microsoft SQL Server Management Studio.

Management Studio is included with the Standard and Enterprise editions. If you are using the Express edition, you can download Management Studio Express from the [Microsoft Download Center](http://www.microsoft.com/Downloads/details.aspx?FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796&displaylang=en) (<http://www.microsoft.com/Downloads/details.aspx?FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796&displaylang=en>).

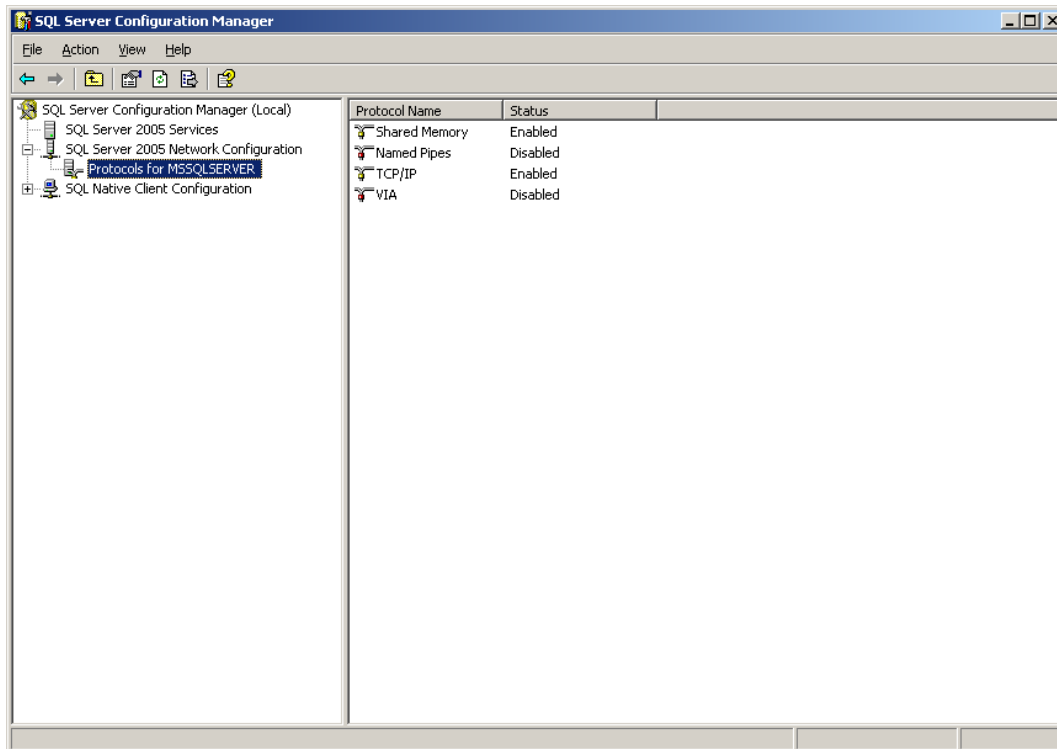
- 2 Launch Management Studio (*Start menu > All Programs > Microsoft SQL Server 2005 (or 2008) > SQL Server Management Studio*).



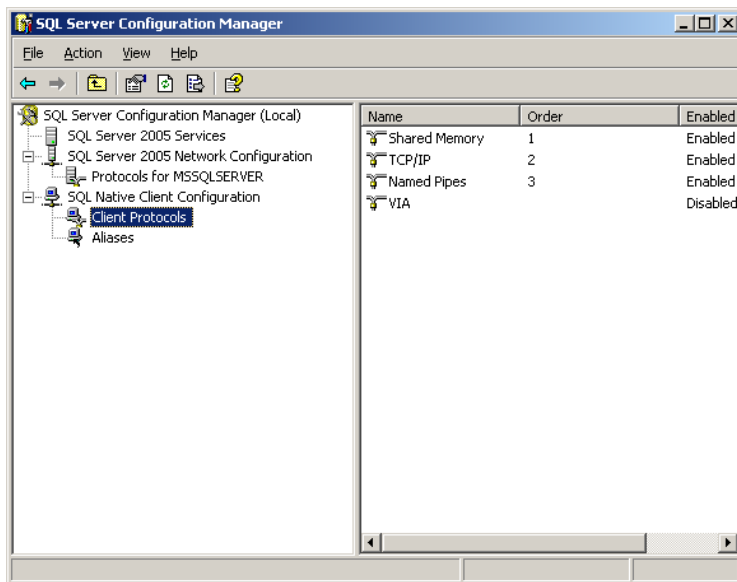
- 3 Right-click your SQL server (TC2K3 in the above graphic), then click *Properties*.



- 4 Select *Security*, then make sure that Server Authentication is set to *SQL Server and Windows Authentication mode*.
- 5 Click *OK*, then exit Management Studio.
- 6 Launch SQL Server Configuration Manager (*Start menu > All Programs > Microsoft SQL Server 2005 (or 2008) > Configuration Tools > SQL Server Configuration Manager*).
- 7 Expand the *SQL Server Network Configuration* section, select *Protocols for MSSQLSERVER* (where *MSSQLSERVER* is your server), then make sure that *TCP/IP* is enabled as shown below.



- 8 Expand the *SQL Native Client Configuration* section, select *Client Protocols*, then make sure that *TCP/IP* is enabled as shown below.



- 9 Exit SQL Server Configuration Manager.

3.2 Ensuring Server Name Resolution

You need to make sure that your network is configured to allow the Management Service, Policy Distribution Service, and Security Client to find and communicate with one another.

- ♦ **Management Service to Policy Distribution Service:** If the two services will be on different servers, make sure that Management server can successfully ping the Policy Distribution server. If the Policy Distribution server is inside the firewall, you can use the local (NETBIOS) server name or the server's Fully Qualified Domain Name (FQDN). If the Policy Distribution server is outside the firewall, use the server's FQDN.
- ♦ **Security Client to Policy Distribution Service:** Make sure that endpoint devices (where the Security Client will be installed) can successfully ping the Policy Distribution server.
- ♦ **Security Client to Management Service:** Make sure that endpoint devices (where the Security Client will be installed) can successfully ping the Management server.

3.3 Configuring Secure (SSL) Communication

Secure (SSL) communication is required between the Management Service and the Policy Distribution Service and between the Security Client and the Management Service. Make sure the following requirements are met:

- ♦ **Policy Distribution Service:** Configure Microsoft Internet Information Service (IIS) on the Policy Distribution server to accept (not require) SSL certificates. This enables the Policy Distribution Service to use SSL communication with the Management Service and non-SSL communication with the Security Client. Requiring (rather than just accepting) SSL certificates breaks communication to the Security Client.

To ensure that SSL certificates are accepted but not required, run the Microsoft Computer Management utility on the Policy Distribution server. In the utility, expand *Services and Applications* > expand *Internet Information Services (ISS) Manager* > expand *Web Sites* > right-click *Default Web Site* > click *Properties* > click the *Directory Security* tab > click the *Edit* button in the Secure communications group box. Make sure that the *Require secure channel (SSL)* check box is not selected.

- ♦ **Management Service:** Configure Microsoft Internet Information Service (IIS) on the Management server to require SSL certificates. Communication between the Management Service and the two other components (Policy Distribution Service and Security Client) is always SSL. If the Management Service and Policy Distribution Service are on the same server, do not require SSL certificates. Instead, configure IIS to accept SSL certificates as explained in the previous requirement for the Policy Distribution server.
- ♦ Set up SSL certificates for the Policy Distribution server and Management server using one of the following options:
 - ♦ Microsoft Certificate Services: Issue and manage your own certificates. For information, see the [Microsoft site \(http://technet.microsoft.com/en-us/library/cc736726\(WS.10\).aspx\)](http://technet.microsoft.com/en-us/library/cc736726(WS.10).aspx).
 - ♦ Certification Authority (CA): Obtain certificates from a trusted organization such as VeriSign*, GeoTrust*, or Thawte*.
 - ♦ Novell Self-Signed Certificate: Have the ZENworks Endpoint Security Management installation create self-signed certificates. This method is recommended only for small environments (100 users or less) or evaluation installations.

- ◆ Make sure that the SSL certificates use the same server names (Policy Distribution server name and Management server name) used to resolve server names in [Section 3.2, “Ensuring Server Name Resolution,” on page 26](#). If you use Novell self-signed certificates, the installation program ensures that the correct server names are included in the certificates.
- ◆ Validate the SSL connection from the Management server to the Policy Distribution server. To do so, open a Web browser on the Management server and enter `https://DSNAME` (where *DSNAME* is the server name of the Policy Distribution server). If you are not using Novell self-signed certificates, the browser should display valid data with no certificate warnings (valid data might be `Page under Construction`); any certificate warnings must be resolved before installation. If you are using Novell self-signed certificates, the certificate warnings are acceptable.
- ◆ Validate the SSL connection from an endpoint device (a device where the Security Client will be installed) to the Management server. The first time the Security Client connects to the ZENworks Endpoint Security Management system, it connects to the Management server. All subsequent connections are non-SSL connections to the Policy Distribution server.

3.4 Securing the Management and Policy Distribution Servers

You should secure the server (or servers) where you plan to install the Management Service and the Policy Distribution Service.

In addition to any standard security practices required by your organization, we recommend that you consider the following security measures. These measures do not need to be completed prior to installation, but delaying might leave undesirable openings in your corporate security.

- ◆ Configure (harden) the server to deactivate all applications, services, accounts, and other options not necessary to the intended functionality of the server. The steps involved in doing so depend upon the specifics of the local environment. You should consult the appropriate section of the [Microsoft Technet security Web page \(http://www.microsoft.com/technet/security/default.mspx\)](http://www.microsoft.com/technet/security/default.mspx).
- ◆ Limit access to trusted machines by setting up the directory and Internet Information Service (IIS) to use ACLs. The following articles provide information:
 - ◆ [Granting and Denying Access to Computers \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
 - ◆ [Restrict Site Access by IP Address or Domain Name \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
 - ◆ [IIS FAQ: 2000 IP address and domain name restrictions \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
 - ◆ [Working With IIS Packet Filtering \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)
- ◆ Remove the following default folders from the IIS installation:
 - ◆ IISHelp
 - ◆ IISAdmin
 - ◆ Scripts
 - ◆ Printers

- ◆ Use IIS Lockdown Tool 2.1 to further secure your IIS installation. The tool is available at [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx). Version 2.1 includes lockdown templates for the major IIS-dependent Microsoft products. Select the template that most closely matches the role of this server. If you are in doubt, the Dynamic Web server template is recommended.
- ◆ Physically secure the server to prevent access by unauthorized individuals. You should take measures appropriate to the risks involved and your organization's requirements. There are multiple available standards and guidelines available, including NIST recommendations, HIPAA requirements, ISO/IEC 17799, and less formal collections of recommendations such as CISSP or SANS guidelines. Even when a given regulatory framework is not applicable, it can still act as a valuable resource and planning guide.
- ◆ Restrict network access to the server. You might consider using your firewall technology to 1) restrict incoming connection attempts to the ports and protocols from which a valid access attempt might be expected and 2) restrict outgoing connection attempts to the IP addresses, ports, and protocols to which a valid access attempt might be expected.

Installing the Services to a Single Server

4

In a single-server installation, you install the Management Service and the Policy Distribution Service to a single server inside your firewall (see [Section 2.1.1, “Consolidated Configuration \(Single Server\),”](#) on page 16). Users receive policy updates only when they are inside the firewall or connected via VPN.

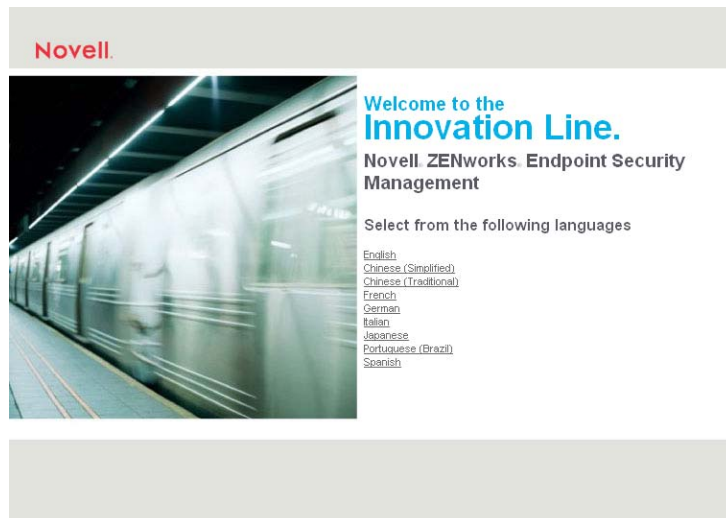
After you complete the following instructions to install the two ZENworks® services, continue with [Chapter 6, “Installing the Management Console,”](#) on page 45 and [Chapter 7, “Installing the Security Client,”](#) on page 57.

To perform a single-server installation:

- 1 Make sure the server meets the system requirements (see [Section 2.2.1, “Server Requirements,”](#) on page 19).
- 2 Make sure that you have completed all installation preparation tasks (see [Chapter 3, “Preparing for Installation,”](#) on page 23).
- 3 At the server, insert the ZENworks Endpoint Security Management disk to run the Master Installer.

The Master Installer is a set of browser-based screens that helps you launch the setup programs for the various ZENworks Endpoint Security Management components.

If the Master Installer does not auto-run, double-click `default.htm` at the root of the disk.



- 4 Click the language you want to use for the text displayed on the Master Installer pages.

Novell.



Welcome to the Innovation Line.
Novell ZENworks Endpoint Security Management


Product Installation Media

Novell ZENworks Endpoint Security Management lets you implement tightly controlled, highly adaptive security policies without placing any configuration or enforcement burden at all upon the end user. Only you can estimate how valuable your data is to the organization's mission and profitability. But as we've seen, stolen or corrupted data typically results in costs that are unacceptable for almost any enterprise. That's why the business case is clear, even in the absence of a precise ROI calculation: no company that's vulnerable to careless or malicious handling of data can afford to be caught without a complete, centrally controlled endpoint security solution. Novell ZENworks Endpoint Security Management is that solution.

- [+ Evaluation Setup](#)
- [+ Consolidated Setup](#)
- [+ Distributed Setup](#)
- [+ Documentation and Manuals](#)

5 Click *Consolidated Setup*.

Novell. [Home](#)



ZENworks Endpoint Security Management Consolidated Setup

Software (listed in the required install order)
 ZENworks Single Server
 ZENworks Management Console
 ZENworks Endpoint Security Client
 Check online for updated software

Documentation
 Installation Guide
 Administrator Manual
 User Guide

Tools
 The folder below contains a tool that can be run on computers not running ZESM to decrypt files encrypted by the ZESM Security Client.
 Decryption Tool

Description

The ZENworks® Consolidated Setup configures both the Policy Distribution Service and Management Service onto a "single server". Like the Management Service, the single server should be installed inside the enterprise firewall. Security Clients will have to have access to the single server Policy Distribution Service to receive policy updates and upload reporting information. The Management Console will be configured to synchronize with a Directory Service to allow for publishing policies to your organization. The Security client can be installed by distributing the default installation package (setup.exe), or preferably through a MSI package customized for your enterprise setup. (see the Administrator Manual for more details).

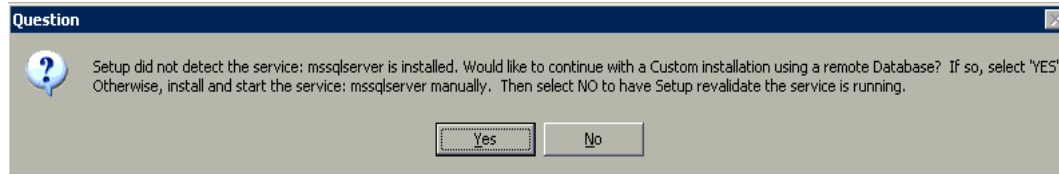
[Return to Main Page](#)

6 Click *ZENworks Single Server* to launch the Single Server installation program.

7 Select the language you want to use for the installation program, then click *OK*.

With MS SQL Server 2005 or 2008, you must perform a Custom installation. Typical installation is not supported.

8 The installation program attempts to detect a local SQL Server. If the installation program does not detect a local SQL Server, the following dialog box is displayed:



Take one of the following actions:

- ◆ If MS SQL Server 2000 is installed locally on the server, make sure that the SQL Server is running, then click *No*.
 - ◆ If you are using remote MS SQL Server 2000, click *Yes*.
 - ◆ If you are using MS SQL Server 2005 or 2008, either locally or remotely, click *Yes*.
- 9 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Setup type	<p>Select <i>Typical</i> only for the following installation scenario: 1) MS SQL Server 2000 is installed locally on the server, and 2) you intend to use Novell® self-signed certificates (no Microsoft or third-party CA certificates).</p> <p>For all other installation scenarios, select <i>Custom</i>.</p>
SSL certificate	<p>This option is available only with a Custom installation. A Typical installation automatically uses Novell self-signed certificates.</p> <p>An SSL certificate is required for secure communication between the Management Service and the Management Console and between the Management Service and the Security Client.</p> <p>If you already have a certificate authority, select <i>Use the existing certificate IIS is configured with</i>.</p> <p>If you need a certificate, click <i>Allow Novell to create, install, and use its own self-signed root certificate</i>. The installing program creates the certificate and the signing authority.</p>

Installation Prompt	Explanation
SQL Server hosting the Policy Distribution Service database	<p>The installation program attempts to detect and list any physical servers on the network that have SQL Servers installed. Only the physical server name is listed. However, you need to provide both the physical server name and the SQL Server name (default instance or named instance). For example, if the physical server name is SERVER1 and the named instance of the SQL Server is SQL2008, you would enter:</p> <pre data-bbox="630 485 846 512">SERVER1\SQL2008</pre> <p>If the SQL Server is using the default instance, you would enter:</p> <pre data-bbox="630 590 906 617">SERVER1\MSSQLSERVER</pre> <p>In addition, you need to provide the username and password for a database account that has SysAdmin rights. The default is the sa account.</p> <p>After you enter the information and click OK, you might receive a message stating that the administrator password cannot be verified because OSQL is not installed. Click <i>OK</i> to dismiss the message. The password is verified later after the installation program installs OSQL.</p>
Policy Distribution Service database name	<p>If you do not want to use the default name (STDSDB) assigned to the Policy Distribution database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.</p>
Policy Distribution Service account username and password	<p>The installation program creates an SQL user account (DS_STDSDB_USER) that the Policy Distribution Service uses to access the database. You cannot change the account name.</p> <p>Specify a password for the account. Make sure that the password meets the password requirements for your SQL Server (for example, if you require strong passwords, make sure to specify a strong password).</p> <p>We recommend that you do not use special characters in the password. However, if you do, the special characters are changed in the configuration files. For example, an @ is changed to an A. The communication between the service and the database works as expected. However, when you troubleshoot with OSQL, you must use the configuration file password, not the one you specified with special characters.</p>
SQL Server hosting the Management Service database	<p>This information should be identical to the information you entered for the SQL Server hosting the Policy Distribution Service database.</p>
Management Service database name	<p>If you do not want to use the default name (STMSDB) assigned to the Management database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.</p>
Server name	<p>Specify either the local name or fully qualified domain name of the physical server. The name you enter must match the name used in the server's SSL certificate.</p>

Installation Prompt	Explanation
SQL Server hosting the Management Service database	This information should be identical to the information you entered for the SQL Server hosting the Policy Distribution Service database .
Reporting Service database name	If you do not want to use the default name (STRSDB) assigned to the Reporting database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.
License installation	<p>If you have purchased a ZENworks Endpoint Security Management license, select <i>Browse for the file containing the ESM license that I have purchased</i>, then click <i>Next</i> to display a Browse dialog box. Otherwise, select <i>Install a 60-day evaluation license</i>.</p> <p>If you select the 60-day evaluation, you can license the product after installation. For instructions, see “Applying a License Key” in ZENworks Endpoint Security Management 4.1 Administration Guide.</p>
Data File Group Folder	Each database (Policy Distribution, Management, and Reporting) has a set of data files associated with it. By default, the data files are installed to the SQL Server’s DATA directory. If you have another location where you keep your data files, select that location instead.
Index File Group Folder	Each database (Policy Distribution, Management, and Reporting) has a set of index files associated with it. By default, the index files are installed to the SQL Server’s DATA directory. If you have another location where you keep your index files, select that location instead.
Log File Group Folder	Each database (Policy Distribution, Management, and Reporting) has a set of log files associated with it. By default, the log files are installed to the SQL Server’s DATA directory. If you have another location where you keep your log files, select that location instead.
ESM Setup Files Folder	The installation program creates an <code>ESM Setup Files</code> folder that contains files (<code>Setup.id</code> , <code>ESM-MS.cer</code> , <code>ESM-DS.cer</code> , <code>STInstParam.id</code> , and so forth) that are required by the Management Console and Security Client. By default, the folder is created on the server desktop. We recommend that you keep the default location.

When the installation is complete, the installation program runs a set of tests to verify that the system is configured properly.

- 10** If a test fails, mouse over the configuration test to display the possible causes. You must resolve any failures before continuing.

If no configuration issues are encountered, the Policy Distribution Service and Management Service launch immediately following installation. You do not need to reboot the server.

Installing the Services on Multiple Servers

5

In a multi-server installation, you install the Management Service and the Policy Distribution Service to different servers. The Management Service must be installed to a server inside your firewall. The Policy Distribution Service can be installed to a server inside or outside your firewall, depending on the location of the users who connect through the Security Client. For configuration options, see [Section 2.1.2, “Distributed Configuration \(Multiple Servers\),” on page 16](#).

You must install the Policy Distribution Service before you install the Management Service. The following sections provide instructions.

- ♦ [Section 5.1, “Installing the Policy Distribution Service,” on page 35](#)
- ♦ [Section 5.2, “Installing the Management Service,” on page 39](#)

After you complete the installation of the two services, continue with [Chapter 6, “Installing the Management Console,” on page 45](#) and [Chapter 7, “Installing the Security Client,” on page 57](#).

5.1 Installing the Policy Distribution Service

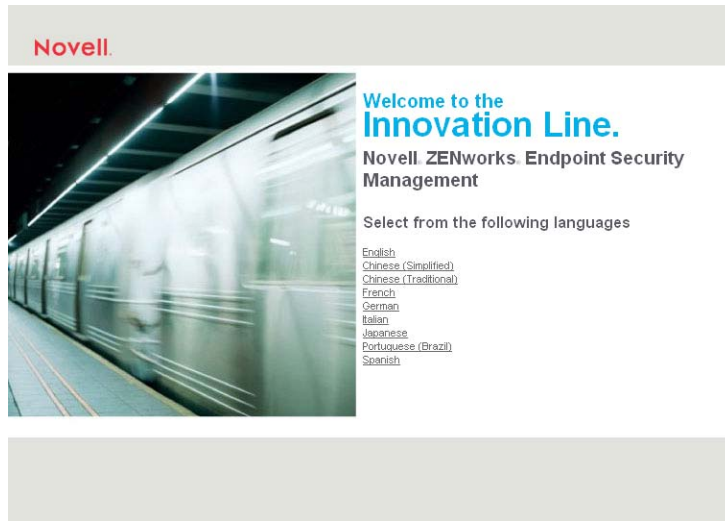
You can install the Policy Distribution Service to a server that is inside of or outside of your firewall. In general, if you have users outside the firewall who require access to policy updates, you should install the service outside the firewall; otherwise, users need to use a VPN connection to access the service inside the firewall.

To install the Policy Distribution Service:

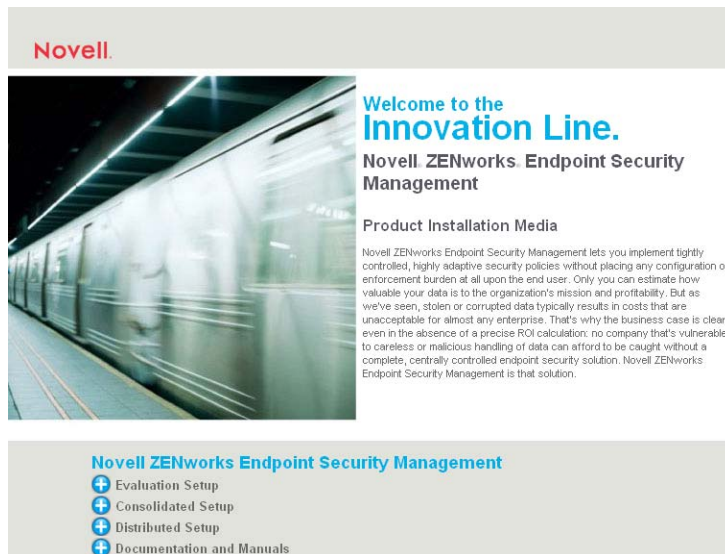
- 1** Make sure the server meets the system requirements (see [Section 2.2.1, “Server Requirements,” on page 19](#)).
- 2** Make sure that you have completed all installation preparation tasks (see [Chapter 3, “Preparing for Installation,” on page 23](#)).
- 3** At the server, insert the ZENworks[®] Endpoint Security Management disk to run the Master Installer.

The Master Installer is a set of browser-based screens that helps you launch the setup programs for the various ZENworks Endpoint Security Management components.

If the Master Installer does not auto-run, double-click `default.htm` at the root of the disk.



4 Click the language you want to use for the text displayed on the Master Installer pages.



5 Click *Distributed Setup*.

Novell Home

ZENworks. Endpoint Security Management Distributed Setup

Software (listed in the required install order)
 ZENworks Policy Distribution Service
 ZENworks Management Service
 ZENworks Management Console
 ZENworks Endpoint Security Client
 Check online for updated software

Documentation
 Installation Guide
 Administrator Manual
 User Guide

Tools
 The folder below contains a tool that can be run on computers not running ZESM to decrypt files encrypted by the ZESM Security Client.
 Decryption Tool

Description
 The ZENworks® Distributed Setup is designed for the greatest amount of flexibility, in terms of installation. To maximize and optimize the configuration, it is recommended that the Policy Distribution Service and Management Service be installed on separate servers. The SQL Databases for each of the services (policy distribution, management, and reporting) should be distributed as well. The Policy Distribution Service can be installed outside the enterprise firewall to all clients to download policy updates and upload reporting data over standard internet access. The Management Service should be installed inside the enterprise firewall. The Management Console will be configured to synchronize with a Directory Service to allow for publishing policies to your organization. The Security client can be installed by distributing the default installation package (setup.exe), or preferably through a MSI package customized for your enterprise setup. (see the Administrator Manual for more details).

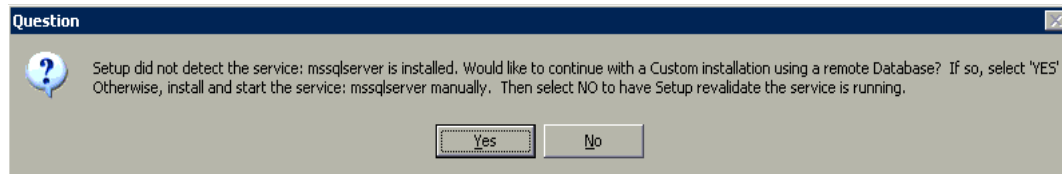
[Return to Main Page](#)

- 6 Click *ZENworks Policy Distribution Service* to launch the installation program.

The installation program verifies that all required software is installed on the server. If any software is absent, it is installed automatically before the installation continues. During this process, you might need to accept the license agreements for the additional software.

If Microsoft Data Access Components (MDAC) 2.8 is installed, the server must reboot. You will need to restart the installation program after the reboot.

- 7 Select the language you want to use for the installation program, then click *OK*.
- 8 The installation program attempts to detect a local SQL Server. If the installation program does not detect a local SQL Server, the following dialog box is displayed:



Take one of the following actions:

- ♦ If MS SQL Server 2000 is installed locally on the server, make sure that the SQL Server is running, then click *No*.
 - ♦ If you are using remote MS SQL Server 2000, click *Yes*.
 - ♦ If you are using MS SQL Server 2005 or 2008, either locally or remotely, click *Yes*.
- 9 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Setup type	<p>Select <i>Typical</i> only for the following installation scenario: 1) MS SQL Server 2000 is installed locally on the server, and 2) you intend to use Novell self-signed certificates (no Microsoft or third-party CA certificates).</p> <p>For all other installation scenarios, select <i>Custom</i>.</p>
SSL certificate	<p>This option is available only with a Custom installation. A Typical installation automatically uses Novell self-signed certificates.</p> <p>An SSL certificate is required for secure communication between the Policy Distribution Service and the Management Service</p> <p>If you already have a certificate authority, select <i>Use the existing certificate IIS is configured for</i>. Throughout the rest of the installation instructions, this certificate is referred to as the enterprise certificate.</p> <p>If you need a certificate, click <i>Allow Novell to create, install, and use its own self-signed root certificate</i>. The installing program creates the certificate and the signing authority. Throughout the rest of the installation instructions, this certificate is referred to as the Novell self-signed certificate.</p>
SQL Server hosting the Policy Distribution Service database	<p>The installation program attempts to detect and list any physical servers on the network that have SQL Servers installed. Only the physical server name is listed. However, you need to provide both the physical server name and the SQL Server name (default instance or named instance). For example, if the physical server name is SERVER1 and the named instance of the SQL Server is SQL2008, you would enter:</p> <pre>SERVER1\SQL2008</pre> <p>If the SQL Server is using the default instance, you would enter:</p> <pre>SERVER1\MSSQLSERVER</pre> <p>In addition, you need to provide the username and password for a database account that has SysAdmin rights. The default is the sa account. The installation program uses the account to create the database and a user account for the Policy Distribution Service.</p> <p>After you enter the information and click <i>OK</i>, you might receive a message stating that the administrator password cannot be verified because OSQL is not installed. Click <i>OK</i> to dismiss the message. The password is verified later after the installation program installs OSQL.</p>
Policy Distribution Service database name	<p>If you do not want to use the default name (STDSDB) assigned to the Policy Distribution database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.</p>

Installation Prompt	Explanation
Policy Distribution Service account username and password	<p>The installation program creates an SQL user account (DS_STDSDB_USER) that the Policy Distribution Service uses to access the database. You cannot change the account name.</p> <p>Specify a password for the account. Make sure that the password meets the password requirements for your SQL Server (for example, if you require strong passwords, make sure to specify a strong password).</p> <p>We recommend that you do not use special characters in the password. However, if you do, the special characters are changed in the configuration files. For example, an @ is changed to an A. The communication between the service and the database works as expected. However, when you troubleshoot with OSQL, you must use the configuration file password, not the one you specified with special characters.</p>
Server name	Specify either the local name or fully qualified domain name of the physical server. The name you enter must match the name used in the server's SSL certificate.
Data File Group Folder	The Policy Distribution database has a set of data files associated with it. By default, the data files are installed to the SQL Server's DATA directory. If you have another location where you keep your data files, select that location instead.
Index File Group Folder	The Policy Distribution database has a set of index files associated with it. By default, the index files are installed to the SQL Server's DATA directory. If you have another location where you keep your index files, select that location instead.
Log File Group Folder	The Policy Distribution database has a set of log files associated with it. By default, the log files are installed to the SQL Server's DATA directory. If you have another location where you keep your log files, select that location instead.
ESM Setup Files Folder	<p>The installation program creates a Setup.ID file required by the Management Service installation program. If you are using a Novell self-signed certificate, it also creates the ESM-DS.cer file.</p> <p>By default, these files are saved to an ESM Setup Files folder on the server desktop. If desired, you can specify a different folder.</p> <p>Before installing the Management Service, you need to manually copy the ESM Setup Files folder to its server. If you used an enterprise certificate (rather than a Novell self-signed certificate), you need to place a copy of that certificate in the folder.</p>

- 10** When the installation is complete, the Policy Distribution Service starts. Continue with the next section, [Installing the Management Service](#).

5.2 Installing the Management Service

You install the Management Service to a server inside the firewall. This enables it to access the SQL Server and directory service (Microsoft Active Directory or Novell eDirectory).

To install the Management Service:

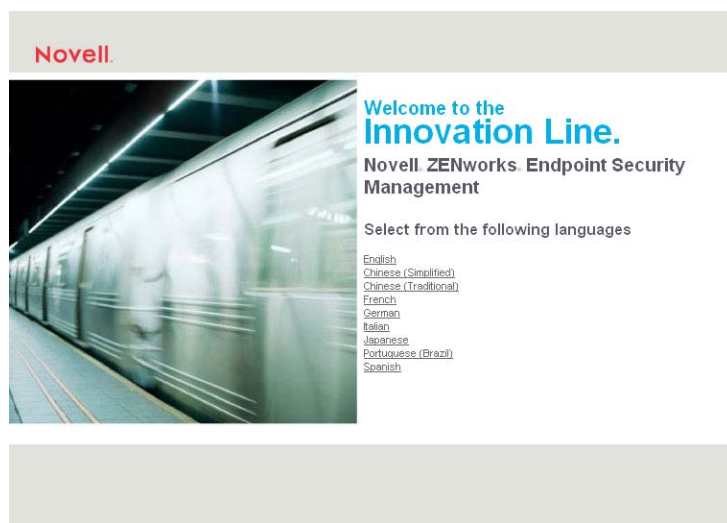
- 1 Make sure the server meets the system requirements (see [Section 2.2.1, “Server Requirements,”](#) on page 19).
- 2 Make sure that you have completed all installation preparation tasks (see [Chapter 3, “Preparing for Installation,”](#) on page 23).
- 3 Copy the `ESM Setup Files` folder from the Policy Distribution server to the target Management server.

The `ESM Setup Files` folder contains files required by the Management Service installation program. If you used an enterprise certificate (rather than a Novell self-signed certificate) when you installed the Policy Distribution Service, you need to place a copy of that certificate in the folder before copying it to the Management server.

- 4 At the server, insert the ZENworks Endpoint Security Management disk to run the Master Installer.

The Master Installer is a set of browser-based screens that helps you launch the setup programs for the various ZENworks Endpoint Security Management components.

If the Master Installer does not auto-run, double-click `default.htm` on the root of the disk.



- 5 Click the language you want to use for the text displayed on the Master Installer pages.

Novell.



Welcome to the Innovation Line.
Novell ZENworks Endpoint Security Management


Product Installation Media

Novell ZENworks Endpoint Security Management lets you implement tightly controlled, highly adaptive security policies without placing any configuration or enforcement burden at all upon the end user. Only you can estimate how valuable your data is to the organization's mission and profitability. But as we've seen, stolen or corrupted data typically results in costs that are unacceptable for almost any enterprise. That's why the business case is clear, even in the absence of a precise ROI calculation: no company that's vulnerable to careless or malicious handling of data can afford to be caught without a complete, centrally controlled endpoint security solution. Novell ZENworks Endpoint Security Management is that solution.

- [+ Evaluation Setup](#)
- [+ Consolidated Setup](#)
- [+ Distributed Setup](#)
- [+ Documentation and Manuals](#)

6 Click *Distributed Setup*.

Novell. [Home](#)



ZENworks Endpoint Security Management
[Distributed Setup](#)

Software (listed in the required install order)
 ZENworks Policy Distribution Service
 ZENworks Management Service
 ZENworks Management Console
 ZENworks Endpoint Security Client
 Check online for updated software

Documentation
 Installation Guide
 Administrator Manual
 User Guide

Tools
 The folder below contains a tool that can be run on computers not running ZESM to decrypt files encrypted by the ZESM Security Client.
 Decryption Tool

Description

The ZENworks® Distributed Setup is designed for the greatest amount of flexibility, in terms of installation. To maximize and optimize the configuration, it is recommended that the Policy Distribution Service and Management Service be installed on separate servers. The SQL Databases for each of the services (policy distribution, management, and reporting) should be distributed as well. The Policy Distribution Service can be installed outside the enterprise firewall to all clients to download policy updates and upload reporting data over standard internet access. The Management Service should be installed inside the enterprise firewall. The Management Console will be configured to synchronize with a Directory Service to allow for publishing policies to your organization. The Security client can be installed by distributing the default installation package (Setup.exe), or preferably through a MSI package customized for your enterprise setup. (See the Administrator Manual for more details).

[Return to Main Page](#)

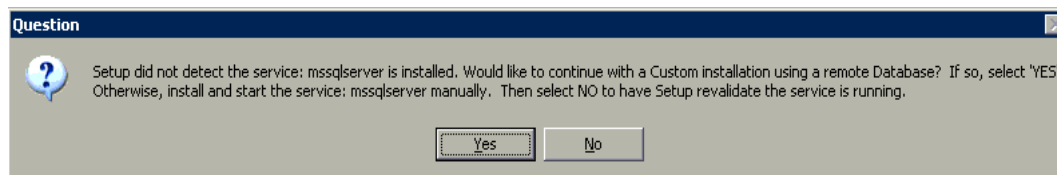
7 Click *ZENworks Management Service* to launch the installation program.

The installation program verifies that all required software is installed on the server. If any software is absent, it is installed automatically before the installation continues. During this process, you might need to accept the license agreements for the additional software.

If Microsoft Data Access Components (MDAC) 2.8 is installed, the server must reboot. You will need to restart the installation program after the reboot.

8 Select the language you want to use for the installation program, then click *OK*.

9 The installation program attempts to detect a local SQL Server. If the installation program does not detect a local SQL Server, the following dialog box is displayed:



Take one of the following actions:

- ◆ If MS SQL Server 2000 is installed locally on the server, make sure that the SQL Server is running, then click *No*.
- ◆ If you are using remote MS SQL Server 2000, click *Yes*.
- ◆ If you are using MS SQL Server 2005 or 2008, either locally or remotely, click *Yes*.

10 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Setup type	<p>Select <i>Typical</i> only for the following installation scenario: 1) MS SQL Server 2000 is installed locally on the server, and 2) you intend to use Novell self-signed certificates (no Microsoft or third-party CA certificates).</p> <p>For all other installation scenarios, select <i>Custom</i>. After you click <i>Next</i>, you are prompted for the Setup.ID file created by the Policy Distribution Service installation program. Browse to the ESM Setup Files folder you copied to the server, then select the file.</p>
Policy Distribution Service account username and password	Specify the password for the SQL user account you created for the Policy Distribution Service when installing it.!
Policy Distribution Service SSL certificate	During installation of the Policy Distribution Service, you specified whether to use an existing enterprise certificate or have the installation program create a Novell self-signed certificate. Select the corresponding option (that is, if the Policy Distribution Service used an existing enterprise certificate, select <i>The Novell Distribution Service used a certificate IIS was already configured with</i>).
Server name	Specify either the local name or fully qualified domain name of the physical server. The name you enter must match the name used in the server's SSL certificate.
Management Service SSL certificate	<p>This option is available only with a Custom installation. A Typical installation automatically uses Novell self-signed certificates.</p> <p>An SSL certificate is required for secure communication between the Policy Distribution Service and the Management Service</p> <p>If you already have a certificate authority, select <i>Use the existing certificate IIS is configured for</i>.</p> <p>If you need a certificate, click <i>Allow Novell to create, install, and use its own self-signed root certificate</i>. The installing program creates the certificate and the signing authority.</p>
ESM Setup Files Folder	Specify the ESM Setup Files folder that you copied from the Policy Distribution server to this server.

Installation Prompt	Explanation
SQL Server hosting the Management Service database	<p>The installation program attempts to detect and list any physical servers on the network that have SQL Servers installed. Only the physical server name is listed. However, you need to provide both the physical server name and the SQL Server name (default instance or named instance). For example, if the physical server name is SERVER1 and the named instance of the SQL Server is SQL2008, you would enter:</p> <pre>SERVER1\SQL2008</pre> <p>If the SQL Server is using the default instance, you would enter:</p> <pre>SERVER1\MSSQLSERVER</pre> <p>In addition, you need to provide the username and password for a database account that has SysAdmin rights. The default is the sa account. The installation program uses the account to create the database.</p> <p>After you enter the information and click <i>OK</i>, you might receive a message stating that the administrator password cannot be verified because OSQL is not installed. Click <i>OK</i> to dismiss the message. The password is verified later after the installation program installs OSQL.</p>
Management Service database name	<p>If you do not want to use the default name (STMSDB) assigned to the Management database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.</p>
SQL Server hosting the Reporting Service database	<p>This information should be identical to the information you entered for the SQL Server hosting the Management Service database.</p>
Reporting Service database name	<p>If you do not want to use the default name (STRSDB) assigned to the Reporting database, specify a new name that contains only letters and numbers and conforms to your SQL Server database naming conventions.</p>
License installation	<p>If you have purchased a ZENworks Endpoint Security Management license, select <i>Browse for the file containing the ESM license that I have purchased</i>, then click <i>Next</i> to display a Browse dialog box. Otherwise, select <i>Install a 60-day evaluation license</i>.</p> <p>If you select the 60-day evaluation, you can license the product after installation. For instructions, see “Applying a License Key” in ZENworks Endpoint Security Management 4.1 Administration Guide.</p>
Data File Group Folder	<p>Each database (Management and Reporting) has a set of data files associated with it. By default, the data files are installed to the SQL Server’s <code>DATA</code> directory. If you have another location where you keep your data files, select that location instead.</p>
Index File Group Folder	<p>Each database (Management and Reporting) has a set of index files associated with it. By default, the index files are installed to the SQL Server’s <code>DATA</code> directory. If you have another location where you keep your index files, select that location instead.</p>

Installation Prompt	Explanation
Log File Group Folder	Each database (Management and Reporting) has a set of log files associated with it. By default, the log files are installed to the SQL Server's <code>DATA</code> directory. If you have another location where you keep your log files, select that location instead.

When the installation is complete, the installation program runs a set of tests to verify that the system is configured properly.

- 11** If a test fails, mouse over the configuration test to display the possible causes. You must resolve any failures before continuing.

If no configuration issues are encountered, the Management Service launches immediately following installation. You do not need to reboot the server.

- 12** If you used an existing IIS certificate (rather than having the installation program create a Novell self-signed certificate), copy the certificate to the `ESM Setup Files` folder.

The Management Console installation program requires the certificate. Copying the certificate to the `ESM Setup Files` folder at this time ensures that it is in the folder when you install the Management Console.

Installing the Management Console

The Management Console is used to create and manage the security policies that are applied by the Security Client to devices. Complete the tasks appropriate to your deployment scenario:

- ♦ [Section 6.1, “Installing the Management Console for Use with the Management and Policy Distribution Services,” on page 45](#)
- ♦ [Section 6.2, “Installing the Standalone Management Console,” on page 54](#)

After you install the Management Console, you can use it to create security policies. See “[Security Policies](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

6.1 Installing the Management Console for Use with the Management and Policy Distribution Services

If you have installed the Management Service and Policy Distribution Service, complete the tasks in the following sections to install the Management Console and configure a connection to your directory service.

- ♦ [Section 6.1.1, “Installing the Software,” on page 45](#)
- ♦ [Section 6.1.2, “Creating a Directory Service Configuration,” on page 48](#)

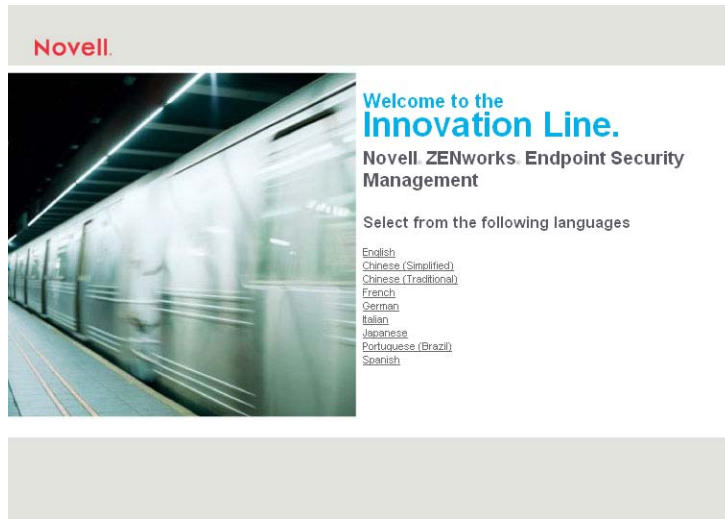
6.1.1 Installing the Software

You can install the Management Console on the server where the Management Service resides, or you can install it on another computer that has direct communication with the Management Service.

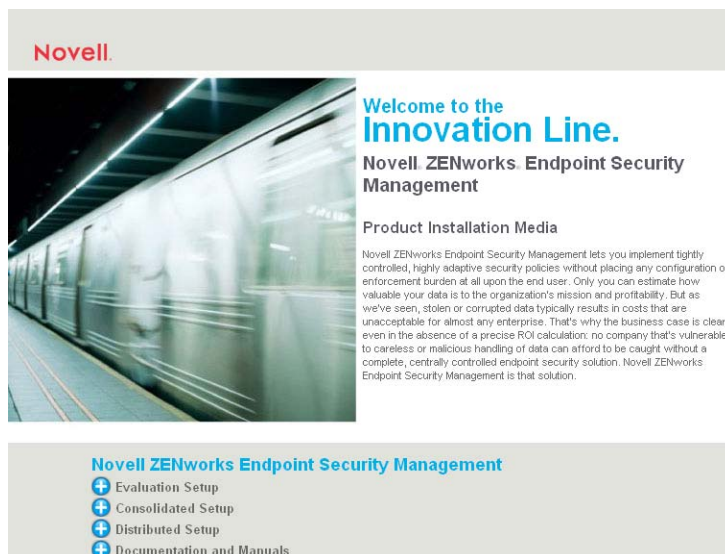
- 1 If you are not installing the Management Console on the same server as the Management Service:
 - ♦ Make sure the target computer meets the system requirements (see [Section 2.2.3, “Management Console Requirements,” on page 20](#))
 - ♦ Copy the `ESM Setup Files` folder from the Management server to the target computer’s desktop. Verify that the `ESM Setup Files` folder contains the following files before you copy it to the computer’s desktop: the Policy Distribution server’s SSL certificate, the Management server’s SSL certificate, and the `STInstParam.id` file.
- 2 If you are using Microsoft Active Directory as your directory service, make sure that the computer is logged in to the Active Directory domain.
- 3 At the target computer, insert the ZENworks Endpoint Security Management disk to run the Master Installer.

The Master Installer is a set of browser-based screens that helps you launch the setup programs for the various ZENworks® Endpoint Security Management components.

If the Master Installer does not auto-run, double-click `default.htm` at the root of the disk.



- 4 Click the language you want to use for the text displayed on the Master Installer pages.



- 5 Click *Consolidated Setup* or *Distributed Setup*.

Both options enable you to install the Management Console.

- 6 Click *ZENworks Management Console* to launch the Management Console installation program.

You can also launch the installation program directly from the installation media:

`\Installs\MC\setup.exe`

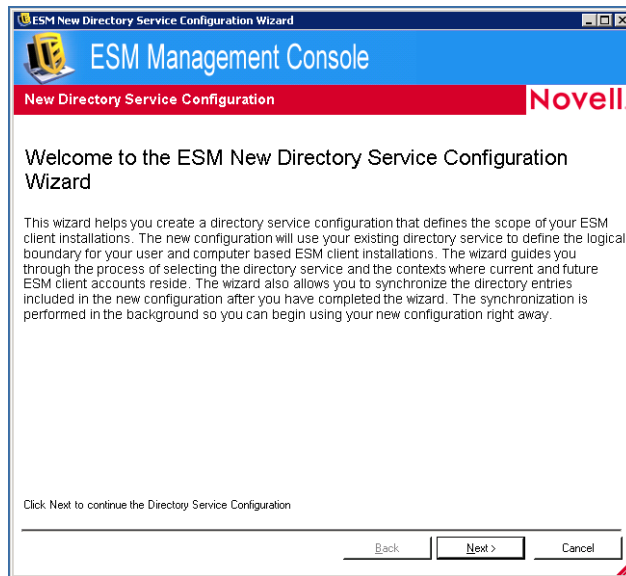
- 7 Select the display language for the installation program, then click *OK*.
- 8 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Setup type	<p>A Typical installation uses the server and SSL information contained in the <code>STInstParam.id</code> file located in the <code>ESM Setup Files</code> folder, if the folder is located on the computer's desktop. If the folder is not located on the desktop, the Typical installation displays the same prompts as a Custom installation.</p> <p>A Custom installation displays all of the information prompts. If the <code>ESM Setup Files</code> folder is located on the desktop, the information from the <code>STInstParam.id</code> is used for the defaults. You can change the defaults if necessary.</p>
Policy Distribution Service host name	Specify the hostname of the server where the Policy Distribution Service is installed. The hostname you use (local name or fully qualified domain name) depends on the location of the server and must match the hostname as defined in the server's SSL certificate.
Management Service host name	Specify the hostname of the server where the Management Service is installed. The hostname you use (local name or fully qualified domain name) depends on the location of the server and must match the hostname as defined in the server's SSL certificate.
SQL Server used by the Management Service	<p>Provide both the physical server name and the SQL Server name (default instance or named instance) where the Management database resides. For example, if the physical server name is <code>SERVER1</code> and the named instance of the SQL Server is <code>SQL2008</code>, you would enter:</p> <pre>SERVER1\SQL2008</pre> <p>If the SQL Server is using the default instance, you would enter:</p> <pre>SERVER1\MSSQLSERVER</pre>
SQL Server used by the Reporting Service	<p>Provide both the physical server name and the SQL Server name (default instance or named instance) where the Reporting database resides. For example, if the physical server name is <code>SERVER1</code> and the named instance of the SQL Server is <code>SQL2008</code>, you would enter:</p> <pre>SERVER1\SQL2008</pre> <p>If the SQL Server is using the default instance, you would enter:</p> <pre>SERVER1\MSSQLSERVER</pre>
Management database name	Specify the name of the database created for the Management Service. If you used the default, the name is <code>STMSDB</code> .
Reporting database name	Specify the name of the database created for the Reporting Service. If you used the default, the name is <code>STRSDB</code> .
SSL certificates	Specify if existing certificates were used when installing the Policy Distribution Service and Management Service, or if the installation program created Novell® self-signed certificates.
Log File Group Folder	Each database (Management and Reporting) has a set of log files associated with it. By default, the log files are installed to the SQL Server's <code>DATA</code> directory. If you have another location where you keep your log files, select that location instead.

- 9 When the installation is complete, select the *Launch the ESM Management Console now* option, then click *Finish*.

You can also launch the Management Console by double-clicking the *ESM Management Console* icon on the desktop or by selecting the *Start* menu > *All Programs* > *Novell* > *ESM Management Console* > *Management Console*.

The Management Console starts with the New Directory Service Configuration Wizard displayed. The wizard lets you set up the connection to your directory service and specify the users and computers you want to manage with ZENworks Endpoint Security Management.



- 10 Continue with the next section, [Creating a Directory Service Configuration](#).

6.1.2 Creating a Directory Service Configuration

ZENworks Endpoint Security Management integrates with Microsoft Active Directory and Novell eDirectory™ to enable security policies to be published to the users and computers in the directory. When the Security Client authenticates through a user or computer account, any policies associated with the account are applied to the computer.

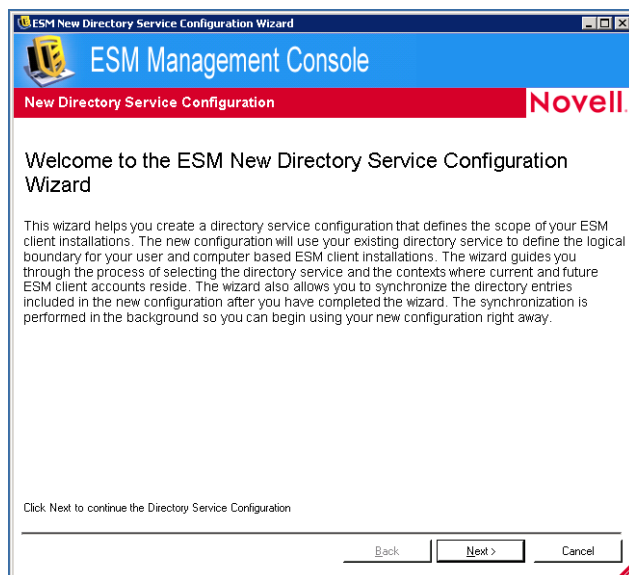
When you create a directory service configuration for one of these directories, you define the connection information for the directory and identify the users or computers to whom policies can be published. The following sections provide instructions for creating configurations for the two directory services:

- ♦ [“Defining eDirectory as the Directory Service” on page 48](#)
- ♦ [“Defining Active Directory as the Directory Service” on page 51](#)

Defining eDirectory as the Directory Service

- 1 Make sure the New Directory Service Configuration Wizard is displayed.

If the wizard is not displayed, launch the Management Console by double-clicking the *ESM Management Console* icon on the desktop or by selecting the *Start* menu > *All Programs* > *Novell* > *ESM Management Console* > *Management Console*.




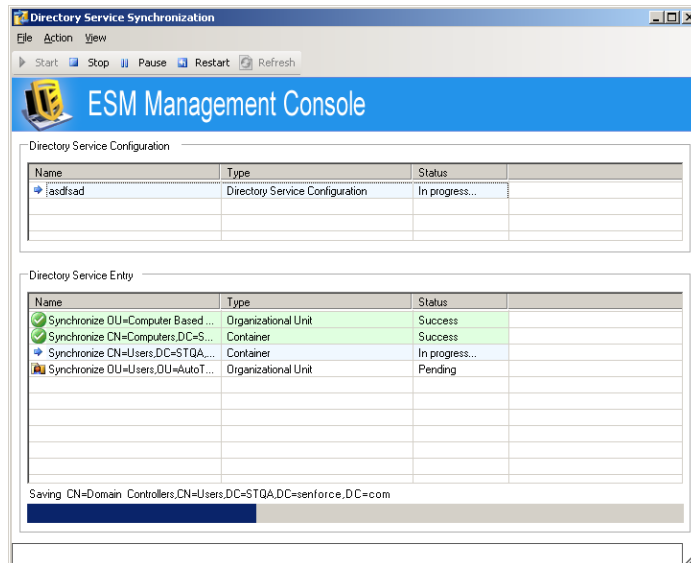
2 Complete the wizard. The following table provides information for each of the pages.

IMPORTANT: Do not use the wizard's Back button. Doing so can result in lost settings and incorrect data synchronization from the directory service to the Management database. If you make a mistake, cancel the wizard and begin again.

Wizard Page	Explanation
Configure Server	<p>Select <i>Novell eDirectory</i>.</p> <p>In the <i>Name</i> field, specify a name that identifies this configuration in the Management Console. When users log in through the Security Client, they must select the directory service configuration that represents the directory service in which their user account exists. If you will have multiple directory service configurations, we recommend that the names you provide for the configurations are the same as or similar to the eDirectory tree names so that users recognize which configuration to select.</p>
Connect to Server	<p>Host Name: Specify the DNS name or IP address of an eDirectory server.</p> <p>Port: Specify the eDirectory server port. The default is 389 (non-secure) or 636 (secure).</p> <p>Enable Encryption for this session using TLS/SSL: Select this option if you want to use either TLS or SSL to encrypt the current session. Encrypting the session ensures that the eDirectory data imported by the Management Console is secure during transmission. If you enable this option, you must use port 389 or 636.</p>

Wizard Page	Explanation
Provide Credentials	<p>The Management Console requires a user account for authentication to eDirectory.</p> <p>User Name: Specify the login name of a user who has permission to view the entire directory.</p> <p>Password: Specify the password for the user account.</p> <p>Context: Specify the user's context.</p>
Select Directory Partition(s)	To receive security policies, the Security Client must authenticate to eDirectory through a user or workstation account. You must identify the location of the users or workstations that you want to be able to authenticate. The first step is to select the partitions that contain the users or workstations.
Select Client Context(s)	The second step in identifying the location of the users or workstations that you want to be able to authenticate is to select the containers in which the users or workstations reside.
Select Context(s) for Synchronization	<p>To publish a security policy to a user or workstation, the user or workstation must be available in the Management Console. There are two ways a user or workstation becomes available in the console:</p> <ul style="list-style-type: none"> ◆ You use this page to synchronize the Management Console with eDirectory. To do so, select the eDirectory containers with users or workstations you want to populate into the Management Console. You can synchronize only the containers you selected as Client contexts (the previous page). ◆ Wait for the user or workstation to authenticate through the Security Client. When the user or workstation checks in, it is automatically added to the Management Console. <p>Synchronizing containers prepopulates the Management Console so that you can immediately publish security policies to individual users or workstations. If you don't synchronize containers, you must publish security policies at the container level (which means all users or workstations in the container receive the policies) or wait for individual users or workstations to authenticate and be added to the Management Console.</p>

- 3** If you have not already done so, click *Finish* to complete the directory service configuration. The directory is added to the *Directory Service Configurations* list.
- If you selected containers to synchronize, the Management Console begins the synchronization. You can double-click  in the Windows notification area to display the Directory Services Synchronization dialog box.



The synchronization occurs in the background. If you exit the Management Console, the synchronization stops. When you open the Management Console again, the synchronization resumes where it left off.

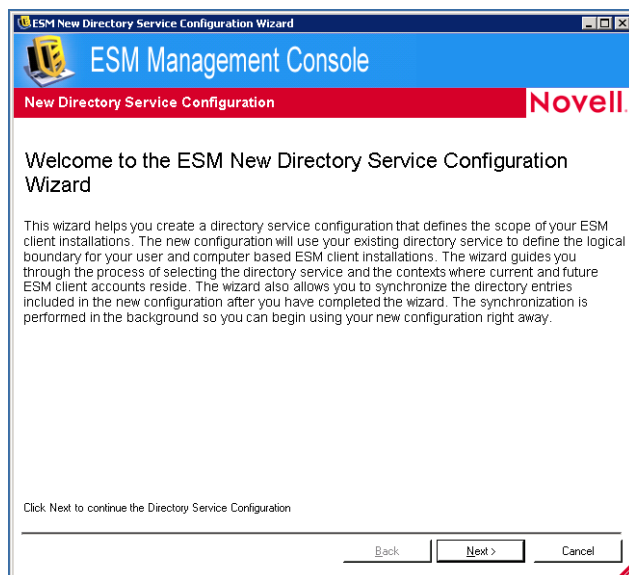
Defining Active Directory as the Directory Service

For the Active Directory domain you are connecting to, the Domain Controller must reside on Windows Server 2000 with SP4, Windows Server 2003, or Windows Server 2008.

If a Windows Server 2008 Domain Controller is down when you run the New Directory Service Configuration Wizard, the wizard might error out. If this occurs, set the port to 389 when running the wizard.

- 1 Make sure the computer is logged in to the Active Directory domain.
- 2 Make sure the New Directory Service Configuration Wizard is displayed.

If the wizard is not displayed, launch the Management Console by double-clicking the *ESM Management Console* icon on the desktop or by selecting the *Start* menu > *All Programs* > *Novell* > *ESM Management Console* > *Management Console*.




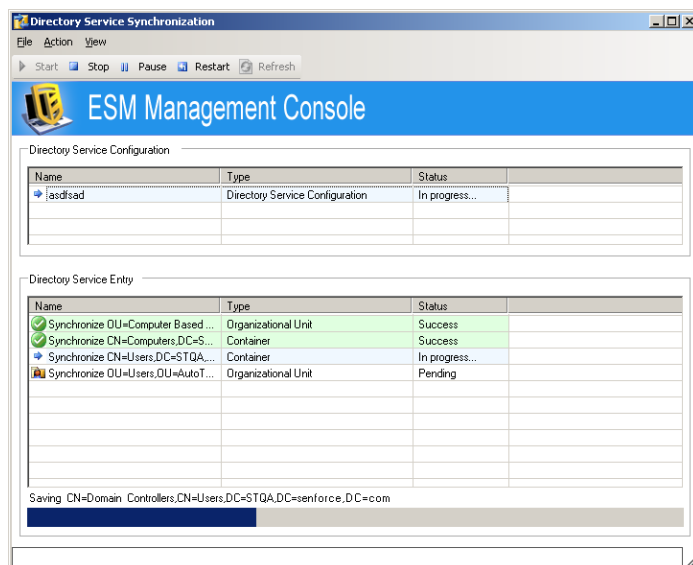
3 Complete the wizard. The following table provides information for each of the pages.

IMPORTANT: Do not use the wizard's Back button. Doing so can result in lost settings and incorrect data synchronization from the directory service to the Management database. If you make a mistake, cancel the wizard and begin again.

Wizard Page	Explanation
Configure Server	<p>Select <i>Microsoft Active Directory</i>.</p> <p>In the <i>Name</i> field, specify a name that identifies this configuration in the Management Console. When users log in through the Security Client, they must select the directory service configuration that represents the directory service in which their user account exists. If you will have multiple directory service configurations, we recommend that the names you provide for the configurations are the same as or similar to the domain names so that users recognize which configuration to select.</p>
Connect to Server	<p>Host Name: Specify the DNS name or IP address of an Active Directory server. By default, the field is populated with the address of an Active Directory server in the Management Console's domain. To select a different Active Directory server, click <i>Browse</i>.</p> <p>Port: 3268 (the default) is the Active Directory Global Catalog server port. If the specified Active Directory server is not a Global Catalog server, specify a different port (for example, 389).</p> <p>Enable Encryption: Select this option if you want to use either Kerberos* or NTLM to encrypt the current session. Encrypting the session ensures that the Active Directory data imported by the Management Console is secure during transmission.</p>

Wizard Page	Explanation
Provide Credentials	<p>The Management Console requires a user account for authentication to Active Directory.</p> <p>User Name: Specify the login name of a user who has permission to view the entire directory. We recommend that you use the domain administrator.</p> <p>Password: Specify the password for the user account.</p> <p>Domain: Select the user's domain.</p> <p>Authentication Method: Select the authentication method required by the Active Directory server (<i>Basic, Kerberos, NTLM, Negotiate</i>).</p>
Locate Account Entry	<p>This page is displayed only if the administrator account you specified is not in a standard Active Directory user container. Expand the directory tree to locate and select the administrator's container.</p>
Select Authenticating Domain(s)	<p>To receive security policies, the Security Client must authenticate to Active Directory through a user or computer account. You must identify the location of the users or computers that you want to be able to authenticate. The first step is to select the domains that contain the users or computers.</p>
Select Client Container(s)	<p>The second step in identifying the location of the users or computers that you want to be able to authenticate is to select the containers in which the users or computers reside.</p>
Select Container(s) for Synchronization	<p>To publish a security policy to a user or computer, the user or computer must be available in the Management Console. There are two ways a user or computer becomes available in the console:</p> <ul style="list-style-type: none"> ◆ You use this page to synchronize the Management Console with Active Directory. To do so, select the Active Directory containers with users or computers you want to populate into the Management Console. You can synchronize only the containers you selected as Client containers (the previous page). ◆ Wait for the user or computer to authenticate through the Security Client. When the user or computer checks in, it is automatically added to the Management Console. <p>Synchronizing containers prepopulates the Management Console so that you can immediately publish security policies to individual users or computers. If you don't synchronize containers, you must publish security policies at the container level (which means all users or computers in the container receive the policies) or wait for individual users or computers to authenticate and be added to the Management Console.</p>

- 4** If you have not already done so, click *Finish* to complete the directory service configuration. The directory is added to the Directory Services Configuration list.
- If you selected containers to synchronize, the Management Console begins the synchronization. You can double-click  in the Windows notification area to display the Directory Services Synchronization dialog box.



The synchronization occurs in the background. If you exit the Management Console, the synchronization stops. When you open the Management Console again, the synchronization resumes where it left off.

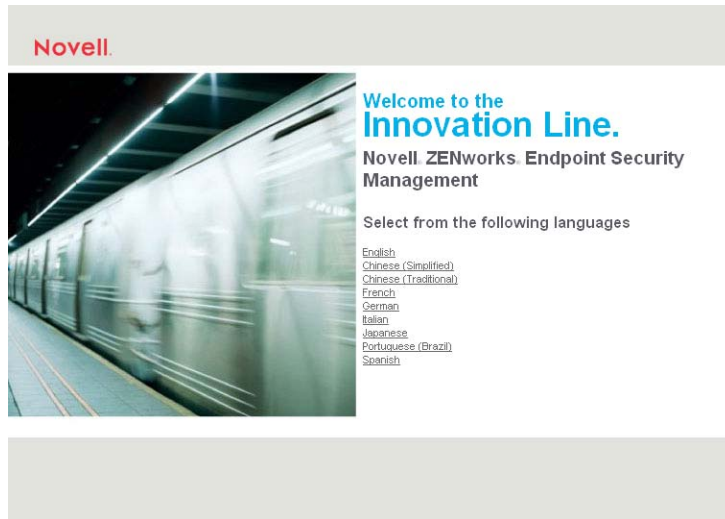
6.2 Installing the Standalone Management Console

If you are not using the Management and Policy Distribution Services (see [Section 2.1, “Deployment Scenarios,”](#) on page 15), you must install the standalone version of the Management Console. The standalone Management Console enables you to create security policies and manually distribute them to endpoint machines.

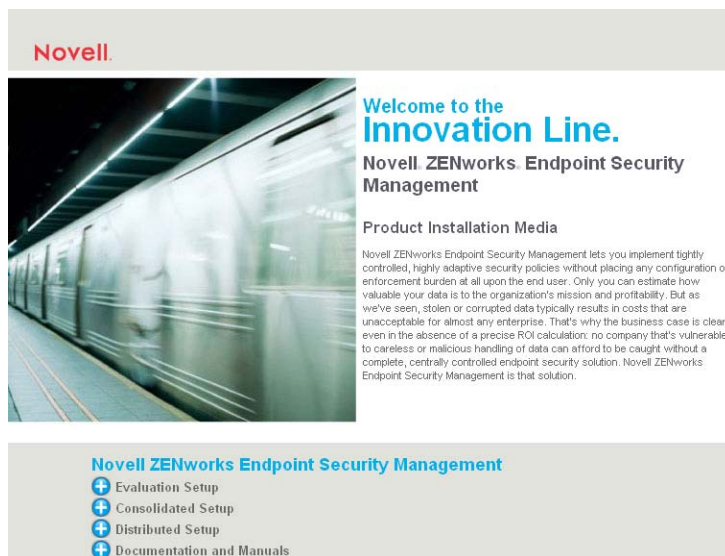
- 1 Make sure that the computer where you plan to install the Management Console has a supported SQL server installed. For information about supported SQL servers, see [Section 2.2.5, “SQL Server Requirements,”](#) on page 22.
- 2 At the target computer, insert the ZENworks Endpoint Security Management disk to run the Master Installer.

The Master Installer is a set of browser-based screens that helps you launch the setup programs for the various ZENworks Endpoint Security Management components.

If the Master Installer does not auto-run, double-click `default.htm` on the root of the disk.



- 3 Click the language you want to use for the text displayed on the Master Installer pages.



- 4 Click *Evaluation Setup*.
- 5 Click *ZENworks Management Console (stand-alone)* to launch the Management Console installation program.

You can also launch the installation program directly from the installation media:

```
\Installs\SAMC\setup.exe
```

- 6 Select the display language for the installation program, then click *OK*.
- 7 If .NET 3.5 is not already installed on the server, you are prompted to install it. Follow the prompts to complete the .NET 3.5 installation.
- 8 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Destination Location	Accept the default location or specify a different directory in which to install the Management Console.
Management Database Name	Specify a name for the database that the Management Console will use to store policy data. The default name is STMSDB.

9 After the configuration is validated, click *Done* to close the validation dialog box.

10 Select the *Launch the ESM Management Console now* option, then click *Finish*.

You can also launch the Management Console by double-clicking the *ESM Management Console* icon on the desktop or by selecting the *Start* menu > *All Programs* > *Novell* > *ESM Management Console* > *Management Console*.

Installing the Security Client

7

The ZENworks® Endpoint Security Management Client (referred to as the *Security Client*) must be installed on any machines on which you want to enforce security policies.

There are two Security Clients:

- ♦ **Security Client for Windows 2000/XP:** Supports Windows XP 32-bit (SP1 and SP2) and Windows 2000 (SP4) machines. The installation program (`setup.exe`) for this client is located in the `\Installs\CL` directory on the installation media.
- ♦ **Security Client for Windows Vista/7:** Supports Windows Vista 32-bit (SP1) and Windows 7 32-bit machines. The installation program (`setup.exe`) for this client is located in the `\Installs\CL_VISTA` directory on the installation media.

You can use the installation program (`setup.exe`) to install the client directly to a machine, or you can use the installation program to create an MSI package that Windows Installer can use to install the client on a machine.

- ♦ [Section 7.1, “Using the Installation Program \(SETUP.EXE\),” on page 57](#)
- ♦ [Section 7.2, “Using an MSI Package,” on page 60](#)
- ♦ [Section 7.3, “Logging In,” on page 64](#)

7.1 Using the Installation Program (SETUP.EXE)

1 (Recommended) Do the following to the target machine:

- ♦ Update all Microsoft security patches and antivirus/spyware software patches.
- ♦ Shut down any antivirus/spyware software that might interact with valid registry functions.

2 Copy the installation program, SSL certificate, and product license file to the target machine:

2a Copy one of the following directories from the installation media to the target machine:

- ♦ Windows 2000/XP Security Client: `\Installs\CL`
- ♦ Windows Vista/7 Security Client: `\Installs\CL_VISTA`

2b Copy the Management Service SSL certificate (`ESM-MS.cer` or the enterprise certificate) to the `CL` or `CL_VISTA` directory.

If you are not using the Management Service (a [non-directory service configuration](#)), you can skip this step. In a non-directory service configuration, there is no Management Service for the Security Client to connect to and therefore no certificate.

2c Copy the Novell® license file (`license.dat`) to the `CL` or `CL_VISTA` directory.

Without the license file, the Security Client is installed in 60-day evaluation mode. If the Security Client connects to a Management Service, you do not need to include the file; when it connects, it receives the license information from the Management Service. If you are not using the Management Service (a [non-directory service configuration](#)) or the Security Client does not connect to the Management Service within 60 days of installation, you need to include the license file with the installation program.

3 Launch the installation program (`setup.exe`).

- 4** Select the language for the installation program, then click *OK*.
- 5** On the Welcome screen, click *Next*.
- 6** Accept the License Agreement, then click *Next*.
- 7** (Conditional) If the computer does not have Microsoft Web Services Enhancements (WSE) 2.0 with Service Pack 3 and Microsoft Visual C++ 2008 installed, you are prompted to install them. Click *Install*.

- 8 Complete the installation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Uninstall Password	<p>If you want to require an uninstall password, select <i>Require an uninstall password</i> and then enter the password. Otherwise, select <i>Do not require an uninstall password</i>.</p> <p>We recommend that you require an uninstall password and only distribute the password if necessary. This ensures that the machine's user does not uninstall the Security Client to bypass security enforcement.</p>
Centrally Managed or Unmanaged	<p>A centrally managed Security Client is one that connects to the Management Service and Policy Distribution Service to receive its security policies. If this Security Client installation is centrally managed, select <i>Managed through ESM servers</i>.</p> <p>An unmanaged Security Client is one that receives its policies as export files from the standalone Management Console (no Management Service and Policy Distribution Service). If this Security Client installation is unmanaged, select <i>Not connected to ESM servers (policies received as files)</i>.</p>
ESM Management Server	<p>This page is displayed only if the Security Client is centrally managed.</p> <p>Specify the Management Service server name as defined in the SSL certificate. This might be the server's fully qualified domain name (FQDN) or the server's local name.</p>
Directory Service Configuration	<p>This page is displayed only if the Security Client is centrally managed and you are installing on Windows 2000 or Windows XP.</p> <p>Select the directory service (Microsoft Active Directory or Novell eDirectory) in which your user or computer account resides. This directory service will be used to assign security policies to you through the user or computer account.</p>
Policy Type (User or Computer/Workstation)	<p>This page is displayed only if the Security Client is centrally managed.</p> <p>Security policies can be published to users or computers. The Security Client needs to know which method you are using. Select the appropriate option (<i>User Based Policy</i> or <i>Computer/Workstation Based Policy</i>).</p> <p>If you selected Novell eDirectory as your directory service, you should only use Computer/Workstation based policies if the following conditions exist:</p> <ul style="list-style-type: none"> ◆ Your organization has Novell ZENworks 7 Desktop Management installed so that the eDirectory schema is extended to support Workstation objects. ◆ Your computer has the ZENworks 7 Desktop Management Agent installed and is registered as a workstation in Novell eDirectory.

- 9 Restart the machine when prompted.

7.2 Using an MSI Package

You can run the installation program (`setup.exe`) in administrative mode to create a Windows Installer MSI package. The following sections explain how to create and distribute the MSI package.

- ◆ [Section 7.2.1, “Creating the MSI Package,” on page 60](#)
- ◆ [Section 7.2.2, “Adding a Policy to the MSI Package,” on page 63](#)
- ◆ [Section 7.2.3, “Distributing the MSI Package,” on page 63](#)

7.2.1 Creating the MSI Package

1 Copy the installation program, SSL certificate, and product license file to the machine you want to use to create the MSI package:

1a Copy one of the following directories from the installation media to the target machine:

- ◆ Windows 2000/XP Security Client: `\Installs\CL`
- ◆ Windows Vista/7 Security Client: `\Installs\CL_VISTA`

1b Copy the Management Service SSL certificate (`ESM-MS.cer` or the enterprise certificate) to the `CL` or `CL_VISTA` directory.

If you are not using the Management Service (a [non-directory service configuration](#)), you can skip this step. In a non-directory service configuration, there is no Management Service for the Security Client to connect to and therefore no certificate.

1c Copy the Novell license file (`license.dat`) to the `CL` or `CL_VISTA` directory.

Without the license file, the Security Client is installed in 60-day evaluation mode. If the Security Client connects to a Management Service, you do not need to include the file; when it connects, it receives the license information from the Management Service. If you are not using the Management Service (a [non-directory service configuration](#)) or the Security Client does not connect to the Management Service within 60 days of installation, you need to include the license file with the installation program.

2 Launch `setup.exe` using the following syntax:

```
setup.exe /a /V"variables"
```

For example:

```
setup.exe /a /V"/qn /L*v c:\log.txt"
```

The following table explains the available command line variables:

Command Line Variable	Description
<code>STDRV=stateful</code>	Applies only to the Windows 2000/XP Security Client. This option changes the default state of the NDIS driver from All Open to All Stateful. This permits all network traffic from boot time until the Security Client determines its location and applies the appropriate location policies.
<code>/qn</code>	Suppresses the typical MSI Installation process to perform a quiet installation. Forces an immediate reboot upon completion without user notification. Use the STRBR variable to stop a reboot.

Command Line Variable	Description
STRBR=ReallySuppress	Does not reboot the machine after installation. The Security Client is not activated until the user (or another method) reboots the machine.
STNMS="MS Name"	Changes the Management Service to which the Security Client connects.
POLICYTYPE=0	<p>Instructs the Security Client to attempt to authenticate through the endpoint device's Active Directory computer account to receive computer-based policies,</p> <p>The Security Client attempts to authenticate using the computer's Active Directory domain credentials. If authentication fails, the Security Client displays a login prompt that allows the user to select a directory service (Active Directory or eDirectory) and specify credentials.</p>
POLICYTYPE=1	<p>Instructs the Security Client to attempt to authenticate through the user's Windows login account to receive user-based policies.</p> <p>The Security Client attempts to authenticate to Active Directory using the user's Windows login credentials. If authentication fails, the Security Client displays a login prompt that allows the user to select a directory service (Active Directory or eDirectory) and specify credentials.</p>
POLICYTYPE=3	<p>Applies only to the Windows 2000/XP Security Client.</p> <p>Instructs the Security Client to attempt to authenticate through the user's eDirectory user account (as supplied in the Novell Client) to receive user-based policies in Novell eDirectory. The Security Client receives its credentials from the Novell Client without prompting the user.</p> <p>In order for the Security Client to receive the user credentials from the Novell Client, the Novell Client must be a specific version. For details, see Novell TID 7005278 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005278&sliceId=1&docTypeID=DT_TID_1_1&dialogID=119482435&stateId=0%20%2019478813).</p>
POLICYTYPE=4	<p>Applies only to the Windows 2000/XP Security Client.</p> <p>Instructs the Security Client to attempt to authenticate through the endpoint device's eDirectory workstation account to receive computer-based policies. To use this option, Novell ZENworks 7 Desktop Management must be installed. For more information, see Section 2.2.4, "Directory Services Requirements," on page 21.</p>
STVA="Adapter name"	<p>Adds a Virtual Adapter.</p> <p>Use this option to activate policy control over a virtual adapter</p>
STSESCANCEL=1	Removes the <code>Cancel</code> button from the Enter Decryption Password dialog box. Removing the <code>Cancel</code> button forces the user to enter the decryption password.
/L*v c:\log.txt	<p>Turns on logging.</p> <p>Use to activate logging at installation. If it is not done now, you must do it through the Security Client's Diagnostics tools. See "Using the Security Client Diagnostic Tools" in the ZENworks Endpoint Security Management 4.1 Administration Guide.</p>

3 Complete the MSI package creation, using information from the following table. Each row of the table corresponds to one of the installation program screens that requires input.

Installation Prompt	Explanation
Uninstall Password	<p>You can require a password to be entered when attempting to uninstall the Security Client. We recommend that you require an uninstall password and only distribute the password if necessary. This ensures that the machine's user does not uninstall the Security Client to bypass security enforcement.</p> <p>If you want an uninstall password, select <i>Require an uninstall password</i> and then enter the password. Otherwise, select <i>Do not require an uninstall password</i>.</p>
Centrally Managed or Unmanaged	<p>A centrally managed Security Client is one that connects to the Management Service and Policy Distribution Service to receive its security policies. If this Security Client installation is centrally managed, select <i>Managed through ESM servers</i>.</p> <p>An unmanaged Security Client is one that receives its policies as export files from the standalone Management Console (no Management Service and Policy Distribution Service). If this Security Client installation is unmanaged, select <i>Not connected to ESM servers (policies received as files)</i>.</p>
ESM Management Server	<p>This page is displayed only if the Security Client is centrally managed.</p> <p>Specify the fully qualified domain name (FQDN) for the server running the Management Service:</p>
Directory Service Configuration	<p>This page is displayed only if the Security Client is centrally managed and you are installing on Windows 2000 or Windows XP.</p> <p>Select the directory service (Microsoft Active Directory or Novell eDirectory) in which your user or computer account resides. This directory service will be used to assign security policies to you through the user or computer account.</p>
Policy Type (User or Computer/Workstation)	<p>This page is displayed only if the Security Client is centrally managed.</p> <p>Security policies can be published to users or computers. The Security Client needs to know which method you are using. Select the appropriate option (<i>User Based Policy</i> or <i>Computer/Workstation Based Policy</i>).</p> <p>If you selected Novell eDirectory as your directory service, you should only use Computer/Workstation based policies if the following conditions exist:</p> <ul style="list-style-type: none"> ◆ Your organization has Novell ZENworks 7 Desktop Management installed so that the eDirectory schema is extended to support Workstation objects. ◆ Your computer has the ZENworks 7 Desktop Management Agent installed and is registered as a workstation in Novell eDirectory.
Email/Web Notification	<p>If you want to receive e-mail notification if the installation fails on a machine, specify an e-mail address.</p> <p>If you want to want to post installation status (failed and successful) to a Web server, specify the Web server name.</p>

Installation Prompt	Explanation
Network Location	Specify the location for the created MSI package. Typically, this is a network location that users have access to. If necessary, you can specify a local directory and then move the MSI package to whatever location you plan to use for distribution of the package.

4 If you haven't done so already, click *Install* to create the MSI package.

The MSI package, which is created in the location you specified, includes two components:

- ♦ The `ZENworks Security Client.msi` file, which includes the installation settings and information.
- ♦ The resource folders (`Binaries`, `MSSoap`, `program files`, `System`, and `System32`) that contain the installation files.

If you move the MSI package, you need to move both components.

7.2.2 Adding a Policy to the MSI Package

The Security Client is installed with a default policy, referred to as the *resource* policy. The resource policy is in effect until the Security Client receives a *distributed* policy. This occurs when the client connects to the ZENworks services or when you export a policy file from the standalone Management Console and manually distribute it to the client.

If you want to apply a distributed policy immediately, you can include it in the MSI package. As soon as the Security Client starts after installation, the distributed policy is applied.

1 In the Management Console, create the policy you want to distribute with the MSI package (see “Security Policies” in the *ZENworks Endpoint Security Management 4.1 Administration Guide* for details).

2 Export the policy, then rename the policy to `policy.sen`.

The policy must be named `policy.sen` in order for the Security Client to accept it.

3 Copy the `policy.sen` and the `setup.sen` files to the MSI package's `program files\Novell\ZENworks Security Client` folder.

The two new policy files replace the existing `policy.sen` and `setup.sen` files.

7.2.3 Distributing the MSI Package

If you don't already have a method for distributing software to machines, here are some possibilities:

- ♦ If you own ZENworks 10 Configuration Management, distribute the MSI package as a bundle. See the *ZENworks 10 Configuration Management Software Distribution Reference* (http://www.novell.com/documentation/zcm10/zcm10_software_distribution/data/bookinfo.html).
- ♦ If you own ZENworks 7 Desktop Management, distribute the MSI package as an application object. See the *ZENworks 7 Desktop Management Administration Guide* (<http://www.novell.com/documentation/zenworks7/dm7admin/data/br3q8ai.html>).

- ♦ If you use Active Directory, use a Group policy's Computer Configuration to distribute the MSI package.
- ♦ Place the MSI package on a network share or Web server from which users can launch the `ZENworks Security Client.msi` file.

7.3 Logging In

The Security Client runs automatically at system startup. Security Clients that are installed in managed mode must authenticate to the Management Service the first time they start. During this initial authentication, the Management Service informs the Security Client of the Policy Distribution Service's address. Subsequent Security Client authentication goes through the Policy Distribution Service.

Depending on the policy type (machine-based or user-based) and the directory service, users might receive a Security Client login prompt:

- ♦ **Computer-based policies:** If the Security Client is configured to accept computer-based policies from Active Directory or eDirectory, the Security Client authentication occurs when the endpoint device authenticates to the directory service. No user intervention is required.
- ♦ **User-based policies in Active Directory:** If the Security Client is configured to accept user-based policies from Active Directory, the Security Client authentication occurs when the user logs in to the Active Directory domain. No user intervention is required unless the user does not log in to the domain.
- ♦ **User-based policies in eDirectory:** If the Security Client is configured to accept user-based policies from eDirectory, the Security Client prompts users for login credentials at startup. If you do not want Windows XP users to be prompted, you can implement single-sign on through the Novell Client; this is not available for Windows 2000/Vista/7 users. Single-sign on simply requires the use of a specific version of the Novell Client. For information, see [Novell TID 7005278](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005278&sliceId=1&docTypeID=DT_TID_1_1&dialogID=119482435&stateId=0%200%20119478813) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005278&sliceId=1&docTypeID=DT_TID_1_1&dialogID=119482435&stateId=0%200%20119478813).

The following sections provide instructions for logging in when the Security Client Login dialog box is displayed:

- ♦ [Section 7.3.1, “Windows 2000/XP,” on page 64](#)
- ♦ [Section 7.3.2, “Windows Vista/7,” on page 65](#)

7.3.1 Windows 2000/XP

The Security Client login prompt on Windows 2000/XP looks like the following:



To log in:

1 Fill in the following fields:

User Name: Specify the username you enter to log in to your Active Directory domain or eDirectory tree. Specify the username only (without the domain or tree context).

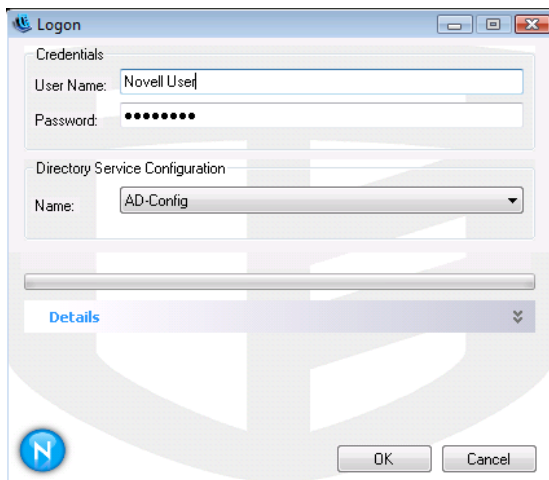
User Password: Specify the password associated with the username you entered.

User Domain/Directory: Select your Active Directory domain or eDirectory tree.

2 Click *OK*.

7.3.2 Windows Vista/7

The Security Client login prompt on Windows Vista/7 looks like the following:



If you receive the Security Client login prompt:

1 Fill in the following fields:

User Name: Specify the username you enter to log in to your Active Directory domain or eDirectory tree. Specify the username only (without the domain or tree context).

Password: Specify the password associated with the username you entered.

Directory Service Configuration Name: Select the configuration name that represents your Active Directory domain or eDirectory tree.

2 Click *OK*.

ZENworks® Endpoint Security Management 4.1 does not provide an automated upgrade process from one release to another. The following steps explain how to manually export policies and keys, remove the existing software, install the new software, and import the policies and keys into the new system.

- 1 Export all policies. For instructions, see “[Exporting a Policy](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.
- 2 Export all encryption keys. For instructions, see “[Exporting Encryption Keys](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

You do not need to export the encryption keys if you exported your encryption policies. Each encryption policy includes all encryption keys. However, it is best practice to export the keys regularly to back up the keys, so we recommend that you do it at this time.

- 3 Uninstall the Management Service, Policy Distribution Service, and Management Console. To do so, use the Windows Add/Remove Programs feature.

You can uninstall the components in any order. Make sure you also remove the databases.

- 4 Reinstall the components in the following order:

- ♦ Policy Distribution Service
- ♦ Management Service
- ♦ Management Console

If you are installing the Policy Distribution Service and Management Service on the same machine, see [Chapter 4, “Installing the Services to a Single Server,”](#) on page 29 for instructions. If you are installing them on separate machines, see [Chapter 5, “Installing the Services on Multiple Servers,”](#) on page 35.

For Management Console installation instructions, see [Chapter 6, “Installing the Management Console,”](#) on page 45.

- 5 Using the Management Console, import the policies. For instructions, see “[Importing Policies](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.
- 6 Import the encryption keys. For instructions, see “[Importing Encryption Keys](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

If you have already imported your encryption policies, this step is not necessary. However, it doesn’t harm your system and ensures that your system contains all of the encryption keys.

- 7 Upgrade the Security Clients. For instructions, see “[Updating the Security Client](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

Typically, the new certificates for the Management Service and Policy Distribution Service work with the Security Client’s existing certificates. If you encounter problems with Security Clients communicating with the services, redistribute the new certificates as part of the client upgrade.

- 8 Republish the policies. For instructions, see “[Distributing a Policy](#)” in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

