ZENworks Endpoint Security Management

Version 3.2

Installation and Quick-Start Guide

June 14, 2007

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

PN: IG300MWE

Document Version 1.0 - supporting Novell ESM 3.2 and subsequent version 3 releases

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see the Novell Documentation Web page (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)

Third-Party Materials

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

Licenses

FIPS Certified AES Crypto

Compilation Copyright (c) 1995-2003 by Wei Dai. All rights reserved. This copyright applies only to this software distribution package as a compilation, and does not imply a copyright on any particular file in the package.
The following files are copyrighted by their respective original authors:
mars.cpp - Copyright 1998 Brian Gladman.
All other files in this compilation are placed in the public domain by Wei Dai and other contributors.
Permission to use, copy, modify, and distribute this compilation for any purpose, including commercial applications, is hereby granted without fee, subject to the following restrictions:

1. Any copy or modification of this compilation in any form, except in object code form as part of an application software, must include the above copyright notice and this license.
2. Users of this software agree that any modification or extension they provide to Wei Dai will be considered public domain and not copyrighted unless it includes an explicit copyright notice.
3. Wei Dai makes no warranty or representation that the operation of the software in this compilation will be error-free, and Wei Dai is under no obligation to provide any services, by way of maintenance, update, or otherwise. THE SOFTWARE AND ANY DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT EXPRESS OR IMPLIED WARRANTY INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL WEI DAI OR ANY OTHER CONTRIBUTOR BE LIABLE FOR DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
4. Users will not use Wei Dai or any other contributor's name in any publicity or advertising, without prior written consent in each case.
5. Export of this software from the United States may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.
6. Certain parts of this software may be protected by patents. It is the users' responsibility to obtain the appropriate licenses before using those parts.

If this compilation is used in object code form in an application software, acknowledgement of the author is not required but would be appreciated. The contribution of any useful modifications or extensions to Wei Dai is not required but would also be appreciated.

Contents

List of Figures

List of Tables

Introduction

ESM consists of five high-level functional components: Policy Distribution Service, Management Service, Management Console, Client Location Assurance Service, and the ZENworks Security Client. The figure below shows these components in the architecture:

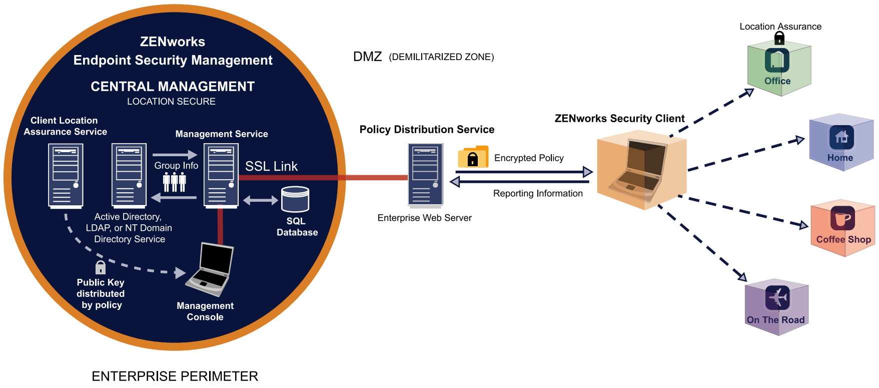


Figure 1: ESM Architecture

The **ZENworks Security Client** (ZSC) is responsible for enforcement of the distributed security policies on the endpoint system. When the ZSC is installed on all enterprise PCs, these endpoints may now travel outside the corporate perimeter and maintain their security, while endpoints inside the perimeter will receive additional security checks within the perimeter firewall.

Each Central Management component is installed separately (with the exception of a "single server" installation, see “ESM Single-Server Installation” on page 12 for details), the following components are installed on servers which are secured inside the corporate perimeter:

- **Policy Distribution Service** is responsible for the distribution of security policies to the ZSC, and retrieval of reporting data from the SSCs. The Policy Distribution Service can be deployed in the DMZ, outside the enterprise firewall, to ensure regular policy updates for mobile endpoints
- **Management Service** is responsible for user policy assignment and component authentication; reporting data retrieval, creation and dissemination of ESM reports; and security policy creation and storage
- **Management Console** is a visible user interface, which can run directly on the server hosting the Management Service or on a workstation residing inside the corporate firewall with connection to the Management Service server. The Management Console is used to both configure the Management Service and to create and manage user and group security policies. Policies can be created, copied, edited, disseminated, or deleted using the editor
- **Client Location Assurance Service** provides a cryptographic guarantee that ZENworks Security Client are actually in a defined location, as other existing network environment parameters indicate

System Requirements

Table 3: ESM System Requirements

Server System Requirements	Endpoint System Requirements
Operating Systems: Microsoft Windows 2000 Server SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server	**Operating Systems:** Windows XP SP1 Windows XP SP2 Windows 2000 SP4
Processor: 3.0 GHz Pentium 4 HT (or greater) 756 MB RAM minimum (1 GB+ Recommended)	**Processor:** 600MHz Pentium 3 (or greater) Minimum 128 MB RAM (256 MB or greater recommended
Disk Space: 500 MB - Without local Microsoft SQL database 5 GB - With local MS SQL database (SCSI recommended)	**Disk Space:** 5 MB required, 5 additional MB recommended for reporting data
Required Software: Supported RDBMS (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005) Microsoft Internet Information Services (configured for SSL) Supported Directory Services (eDirectory, Active Directory or NT Domains*) * = NT Domains is only supported when the Management Service is installed on a Windows 2000, or 2000 advanced server (SP4).	**Required Software:** Windows 3.1 Installer All Windows updates should be current

The Policy Distribution, Management, and Client Location Assurance services require a LOCAL account of ASP.NET to be enabled. If this is disabled, the services will NOT work correctly.

About the ESM Manuals

The ZENworks Endpoint Security Management manuals provide three levels of guidance for the users of the product.

ESM Administrator's Manual - This guide is written for the ESM Administrators who are required to manage the ESM services, create security policies for the enterprise, generate and analyze reporting data, and provide troubleshooting for end-users. Instructions for completing these tasks are provided in this manual

ESM Installation and Quick-Start Guide - This guide provides complete installation instructions for the ESM components and assists the user in getting those components up and running

ZENworks Security Client User's Manual - This manual is written to instruct the end-user on the operation of the ZENworks Security Client (ZSC). This guide may be sent to all employees in the enterprise to help them understand how to use the ZSC.

ESM Installation

The installation software should be physically protected to prevent any tampering or unauthorized use. Likewise, administrators should review the guidelines for pre-installation and installation to ensure the ESM system can function without interruption, or be made vulnerable by inadequate hardware protection.

The administrator installing this software MUST be the primary administrator for the servers and the domain. If using enterprise SSL certificates, this must also be the same username used to create the SSL Root Security certificate.

Installation Packages

If you have downloaded the individual installation packages from the Novell Download site, review the installation instructions below and on the following pages, and place each component (i.e., DS-Release-3.2.zip and MS-Release-3.2.zip) on their designated servers prior to unzipping and installing.

If installing from a CD, a Master Installer is launched, which utilizes simple user interface which guides the ESM Administrator through the installation process. Simply load the installation CD on each machine to access the Master Installer and install the desired component.

About the Master Installer

At launch, the Master Installer displays two menu options: Products and Documentation.

The Products link opens the installation menu. The menu items on this screen will launch the designated installer for each component. In the case of the ZENworks Security Client, an additional option is available to launch the installation in Administrator Mode, which will help the ESM Administrator to create an MSI package for easy distribution (see “MSI Installation” on page 55).

For information on the complete operation of the ESM components, please refer to the ESM Administrator's Manual, available through the Documentation link.

Installation Options

ESM back-end components can be installed as either Single Server, or Multi-Server installations. Single Server installations are ideal for small deployments that do not require regular policy updates. Multi-Server installations are provided for large deployments, and/or for regular policy updates. Please consult with Novell Professional Services to determine which installation type is right for you.

ZENworks Security Client can operate (when needed) without connectivity to the Policy Distribution Service. Likewise, a Stand-Alone Management Console can be optionally installed for evaluation purposes. The installation for this Unmanaged mode of operation is described on page 61 of this guide.

Installation Order

ESM should be installed in the following order:

1. Single Server Installation or Multi-Server Installation
    - Policy Distribution Service
    - Management Service
2. Management Console
3. Client Location Assurance Service
4. ZENworks Security Client

Before Installing ESM

There are a few questions the ESM administrator needs to consider prior to beginning installation:

How will your users receive their ESM security policies?

The options for policy distribution center around whether users should be able to receive a policy update anywhere, including outside the central network, or if they should receive them ONLY when they are in (or connected via VPN) a secured network. For organizations planning to frequently update their ESM security policies, it is recommended a multi-server installation be used that places the Policy Distribution Service on a web server outside the DMZ.

What type of server deployments are available to you?

If your organization only has a few servers available, then a Single-Server installation deployment may be necessary. If server availability isn't an issue, then the size of your client deployment, and the number of users operating outside the firewall should be taken into consideration.

What is your available SQL Server deployment?

ESM creates three SQL databases at installation. If your deployment is small, a single SQL database, or a server-side DB could be installed on the Policy Distribution and Management Service's server(s). For larger deployments, a separate SQL database server should be employed to receive the data from the Policy Distribution and Management Services. Only the following RDBMS types are allowed: SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4.

If a named instance, the configuration of the server(s) should be as follows:

Provider=sqloledb

Data Source=ServerName\InstanceName (this definition type is REQUIRED for ESM to install)

Initial Catalog=DatabaseName

User Id=Username

Password=Password

Set SQL to mixed mode.

The username and password during installation CANNOT be a domain user; it must be a SQL user with SysAdmin rights.

Will you use existing Certificates to establish SSL communication, or will you use Novell Self Signed Certificates?

For disaster recovery and/or failover designs it is recommended that you use enterprise, or otherwise-issued, Certificate Authority (i.e., VeriSign, GeoTrust, Thawte, etc.) SSL certificates for full deployments of ESM. When using your own certificates, the web service certificate and root CA be created on the machine designated as the Policy Distribution Service, then distributed to the appropriate machines. To create an Enterprise Certificate Authority, see the step by step instructions for securely setting up a certificate authority, available at microsoft.com.

For evaluations or small deployments (<100 users) ESM has self-signed certificates that may be used. Novell SSL Certificates will be installed onto the servers when running the typical installation.

How will you deploy your ZENworks Security Clients?

The ZENworks Security Client software may be deployed either individually onto each endpoint, or through an MSI push. Instructions on creating an MSI package may be found on page 55.

Do you want policies to be machine-based or user-based?

Policies can be distributed to a single machine, where every user who logs onto it will receive the same policy, or policies can be set for individual users or groups.

Each installation has several pre-requisites. It is recommended that each check-list of prerequisites be complete BEFORE running the installation for any component. Please review the lists on the following pages:

- “ESM Single-Server Installation” on page 12
- “Policy Distribution Service Installation” on page 15
- “Management Service Installation” on page 26
- “Management Console Installation” on page 39
- “Client Location Assurance Service Installation” on page 51
- “ZENworks Security Client Installation” on page 53

ESM Single-Server Installation

Single Server Installation (SSI) allows both the Policy Distribution Service and the Management Service to co-exist on the same server (not possible without using this installation option). This server must be deployed inside the firewall for security purposes, requiring users to receive policy updates only when they are inside the corporate infrastructure and/or connected via a VPN.

Deployment of the Single Server Installation on a Primary Domain Controller (PDC) is not supported for both security and functionality reasons.

Please make certain the following pre-requisites are in place PRIOR to beginning the installation:

□ ZENworks Security Client (ZSC) to Single Server server name resolution: validate that the target computers (where the ZSC will be installed) can "ping" the SSI server name. If unsuccessful, you will have to resolve this BEFORE continuing with the installation. (Change the SSI server name to FQDN/NETBIOS, change AD to use FQDN/ NETBIOS, change DNS configurations, modifying the local host file on the target computers to include the correct MS information, etc).

□ Enable/Install Microsoft Internet Information Services (IIS), and configure it to accept Secure Socket Layer (SSL) Certificates.

□ If using your own SSL certificates, ensure that the web service certificate and root CA are loaded on the machine and that server name validated in the previous steps (whether NETBIOS or FQDN) matches the "Issued to" value for the certificate configured in IIS.

□ If you are using your own certificates or have already installed the Novell Self Signed Certificate, you can validate SSL as well by trying the following URL from a machine that will have the ZSC installed on it: https:// SSI_SERVER_NAME/AuthenticationServer/ UserService.asmx (Where SSI_SERVER_NAME should be the server name). This should return valid data (an html page) and NOT certificate warnings. ANY certificate warnings MUST be resolved before installation (unless you opt to use Novell Self Signed Certificates instead).

□ Ensure access to a supported RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise). Set database to Mixed mode.

□ Ensure access to a supported directory service (Active Directory, NT Domains*)
*= Only supported when Singer Server Service is installed on a Microsoft Windows 2000 Advanced server (SP4)

It is recommended that the SSI Server be configured (hardened) so as 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, and so cannot be described in advance. Administrators are advised to consult the appropriate section of the Microsoft Technet security webpage. Additional access control recommendations are provided in the ESM Administrator's Manual.

Hardening of IIS: To protect access to only trusted machines, the virtual directory and/or IIS can be set up to have ACLs. Reference the articles below:

Granting and Denying Access to Computers

Restrict Site Access by IP Address or Domain Name

IIS FAQ: 2000 IP address and domain name restrictions

Working With IIS Packet Filtering

For security purposes, it is highly recommended the following default folders be removed from any IIS installation:

- IISHelp
- IISAdmin
- Scripts
- Printers

Novell also recommends using the IIS Lockdown Tool 2.1 available at microsoft.com.

Version 2.1 is driven by supplied templates for the major IIS-dependent Microsoft products. Select the template that most closely matches the role of this server. If in doubt, the Dynamic Web server template is recommended.

Installation Steps

Select Single Server Installation from the master installer menu. This installation combines the installations described previously in this guide for the Policy Distribution Service and the Management Service (see “Policy Distribution Service Installation” and “Management Service Installation” installation steps for further information).

Like their individual installations, the Typical setting will install the Services' defaults and the Novell self-signing SSL certificates. Custom Installation permits the administrator to determine the directory paths and permits the use of an enterprise-owned certificate authority.

Starting the Service

The Combined Distribution and Management Service launches immediately following installation, with no reboot of the server required. The Management Console is used to manage both the Distribution and Management Services using the Configuration feature (see the ESM Administrator’s Manual for full details).

Once this installation is complete, both the Management Console and the Client Location Assurance Service may be likewise installed on this server. If installing the Management Console on a separate machine, copy the ESM Setup Files folder to the designated Management Console machine to complete installation.

Continue to “Management Console Installation” on page 39.

Multi-Server Installation

Multi-Server installation is recommended for large deployments, or when the Policy Distribution Service should be placed outside the corporate firewall to ensure users receive regular policy updates when they are outside the perimeter. Multi-Server installation MUST be done on at least two separate servers, attempts to install both the separate Policy Distribution Service and the Management Service onto the same server will fail (see "ESM Single-Server Installation" on page 12 for a single-server installation option).

Multi-Server installation should begin with the Policy Distribution Service installation on a secured server either outside or inside the corporate firewall.

See "Policy Distribution Service Installation" on page 15.

Once the Policy Distribution Service is installed, the Management Service installation should follow.

See "Management Service Installation" on page 26.

It is recommended the Management Console be installed on this server.

Continue to "Policy Distribution Service Installation" on page 15.

Policy Distribution Service Installation

Which server will host the Policy Distribution Service?

Based on your answers to the first two questions above, select a server that will host the ESM Policy Distribution Service. This server should ALWAYS be reachable by your users, whether within the network, or out in the DMZ. Ensure the required software (see page 7) is installed on the server prior to installation. Once the server is selected, note the server name... both the NETBIOS and Fully Qualified Domain Name (FQDN).

Deployment of the Policy Distribution Service on a Primary Domain Controller (PDC) is not supported for both security and functionality reasons.

Please check off the following pre-requisites PRIOR to beginning the installation:

- □ Ensure Management Service (MS) to Policy Distribution Service (DS) server name resolution: the target computer where the MS will be installed can "ping" the DS server name (NETBIOS if the DS will be configured inside the network firewall, FQDN if installed outside in the DMZ).
- □ If successful, this is the server name to enter during installation step 9. If unsuccessful, you will have to resolve this BEFORE continuing with the installation.
- □ Ensure ZENworks Security Client (ZSC) to DS server name resolution: validate that the endpoint clients (where the ZSC will be installed) can "ping" the same DS server name used above. If unsuccessful, you will have to resolve this BEFORE continuing with the installation.
- □ Enable/Install Microsoft Internet Information Services (IIS), ensure ASP.NET is enabled, and configure it to accept Secure Socket Layer (SSL) Certificates
- □ If using your own SSL certificates, ensure that the "web service" certificate is loaded on the machine and that server name validated in the previous steps (whether NETBIOS or FQDN) matches the "Issued to" value for the certificate configured in IIS.
- □ If using your own SSL certificates, please validate the SSL from the MS server to the DS server: open a web browser on the Management Service and enter the following URL: https://DSNAME (where DSNAME is the server name of the DS). This should return valid data and NOT certificate warnings (valid data may be "Page under Construction"). ANY certificate warnings MUST be resolved before installation (unless you opt to use Novell Self Signed Certificates instead).
- □ Ensure access to a supported RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL Server 2005). Set to DB to Mixed mode. This database should be either hosted on the Management Service server, or a shared server secured behind the enterprise firewall.

It is recommended that the DS Server be configured (hardened) so as 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, and so cannot be described in advance. Administrators are advised to consult the appropriate section of the Microsoft Technet security webpage. Additional access control recommendations are provided in the ESM Administrator's Manual.

Hardening of IIS: To protect access to only trusted machines, the virtual directory and/or IIS can be set up to have ACLs. Reference the articles below:

Granting and Denying Access to Computers

Restrict Site Access by IP Address or Domain Name

IIS FAQ: 2000 IP address and domain name restrictions

Working With IIS Packet Filtering

For security purposes, it is highly recommended the following default folders be removed from any IIS installation:

- IISHelp
- IISAdmin
- Scripts
- Printers

Novell also recommends using the IIS Lockdown Tool 2.1 available at microsoft.com.

Version 2.1 is driven by supplied templates for the major IIS-dependent Microsoft products. Select the template that most closely matches the role of this server. If in doubt, the Dynamic Web server template is recommended.

Installation Steps

Click Policy Distribution Service Installation from the Installation Interface menu. The Policy Distribution Service installation will begin.

At launch, the installer will verify all required software is present on the server. If any are absent, they will be installed automatically before the installation continues to the Welcome Screen (license agreements for the additional software may need to be accepted). If Microsoft Data Access Components (MDAC) 2.8 need to be installed, the server will need to reboot following that installation before ESM installation can continue. If using Windows 2003 Server, ASP.NET 1.1 will be configured to run by the installer.

Once Policy Distribution Service installation begins, perform the following steps

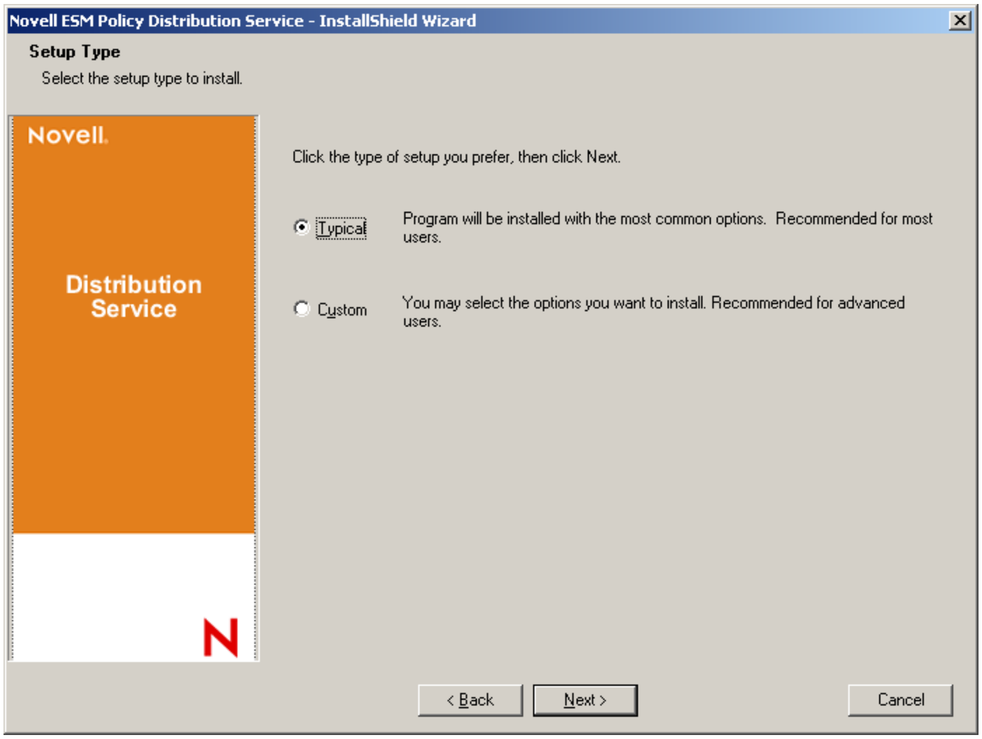
Note:

The following steps outline what you, the user, need to do to complete the installation process. Internal processes will display throughout the installation, and are not documented here unless there is a specific action or information that you will need for installation to be successful.

Step 1: Click NEXT on the Welcome screen to continue

Step 2: Accept the Licensing Agreement and click NEXT

Step 3: Select either a **TYPICAL** or **CUSTOM** installation


Novell ESM Policy Distribution Service - InstallShield Wizard
Novell.
Distribution Service
N
< Back
Next >
Cancel

Setup Type

Select the setup type to install.

Click the type of setup you prefer, then click Next.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Custom — You may select the options you want to install. Recommended for advanced users.

Figure 2: Select Typical or Custom Installation

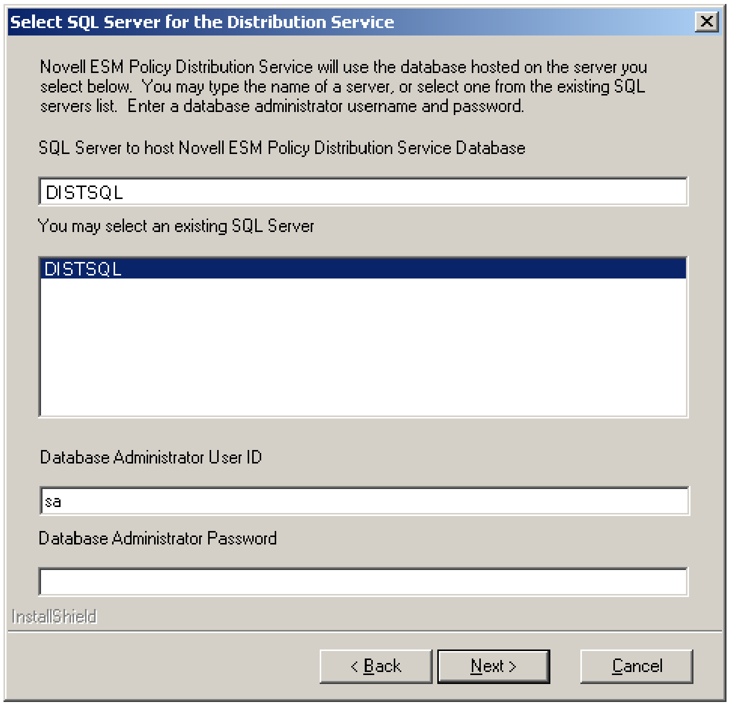
Both installation paths are presented below:

Typical Installation

A typical installation places the Policy Distribution Service software files in the default directory: \Program Files\Novell\ESM Policy Distribution Service. The SQL database name is assigned as STDSDB. The three SQL database files (data, index, and log) are placed in: \Program Files\Microsoft SQL Server\mssql\Data.

Step 1: Novell SSL Certificates are created for the installation. If you wish to use your own SSL certificates, please use Custom Installation. These certificates MUST be distributed to all end users.

Step 2: The installer will detect the available SQL databases on the machine and network. Select a secured SQL database for the Policy Distribution Service and enter the database administrator's name and password (if the password is zero characters, the installer will warn of the potential security issue). The username and password CANNOT be a domain user; it MUST be a SQL user with SysAdmin rights



Select SQL Server for the Distribution Service

Novell ESM Policy Distribution Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Policy Distribution Service Database: DISTSQL

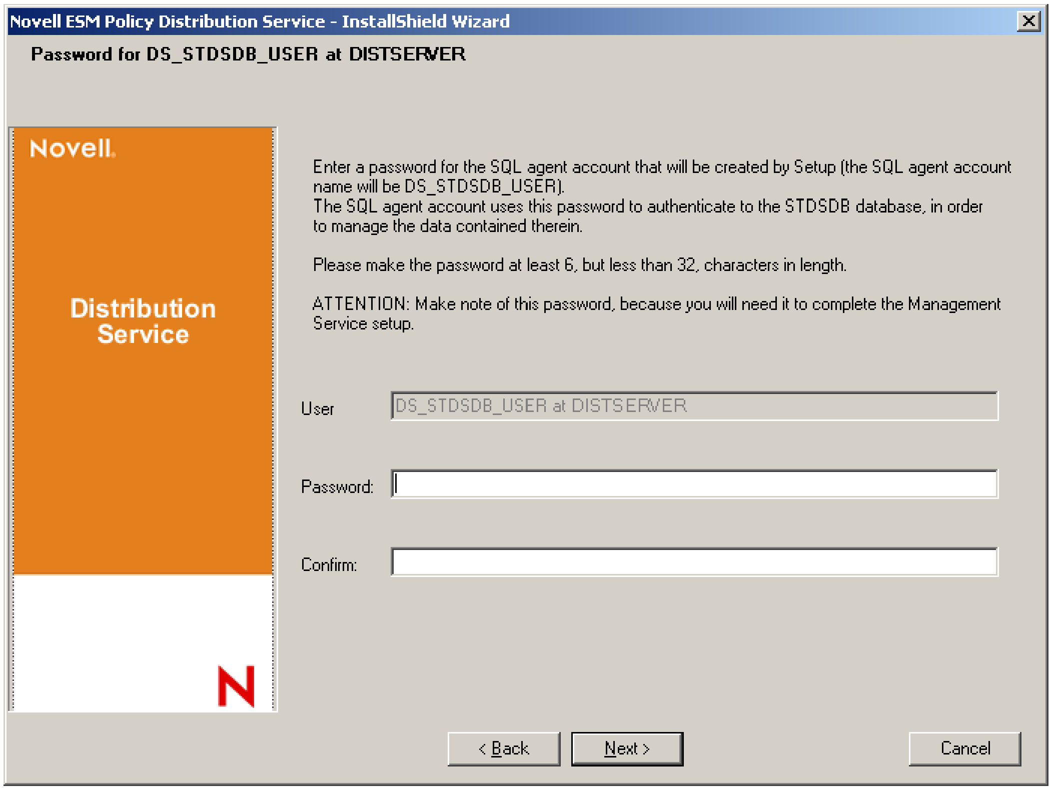
You may select an existing SQL Server: DISTSQL

Database Administrator User ID: sa

Database Administrator Password:

Figure 3: Select SQL Server

Step 3: Enter the password for the Policy Distribution Service agent. This is the username and password the service will use to login to its SQL database.



Novell ESM Policy Distribution Service - InstallShield Wizard

Password for DS_STDSDB_USER at DISTSERVER

Enter a password for the SQL agent account that will be created by Setup (the SQL agent account name will be DS_STDSDB_USER).
The SQL agent account uses this password to authenticate to the STDSDB database, in order to manage the data contained therein.

Please make the password at least 6, but less than 32, characters in length.

ATTENTION: Make note of this password, because you will need it to complete the Management Service setup.

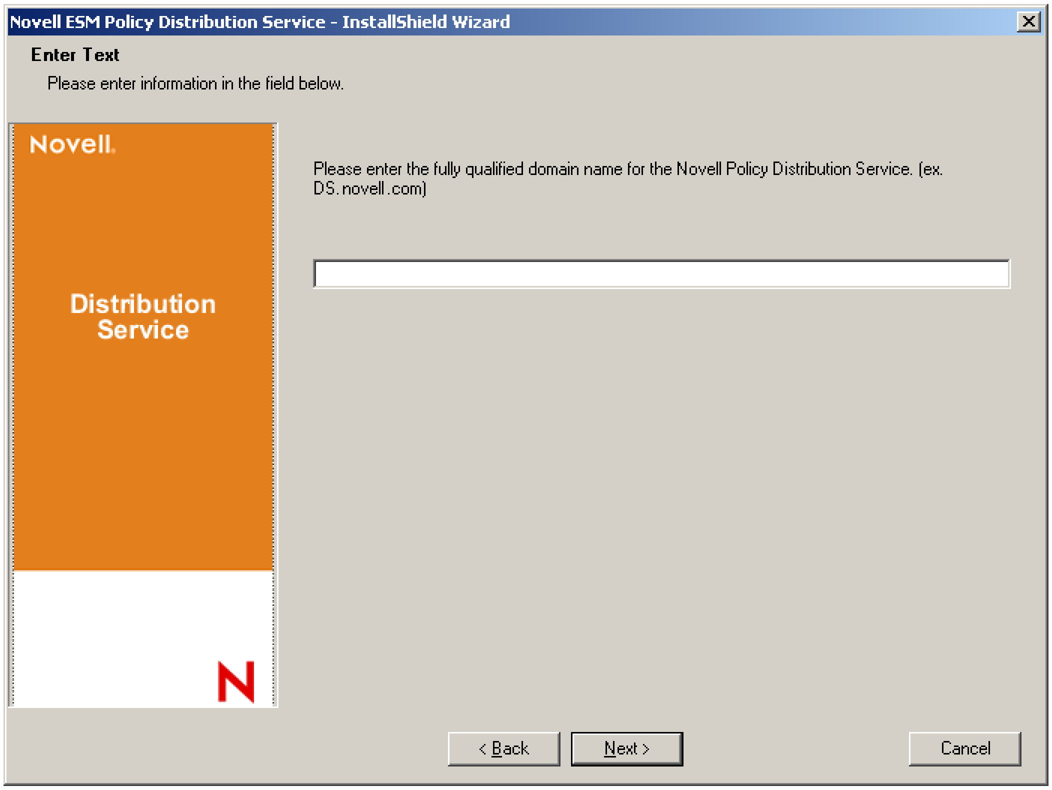
User DS_STDSDB_USER at DISTSERVER

Password:

Confirm:

Figure 4: Distribution Service SQL Password

Step 4: Enter the Policy Distribution Service domain name. This MUST be the fully qualified domain name if the server will reside outside the corporate firewall. Otherwise, only the NETBIOS name for the server is required



Novell ESM Policy Distribution Service - InstallShield Wizard
Enter Text
Please enter information in the field below.
Novell.
Distribution Service
N
< Back
Next >
Cancel

Please enter the fully qualified domain name for the Novell Policy Distribution Service. (ex. DS.novell.com)

Figure 5: Enter Policy Distribution Service Domain Name

Step 5: At the Copy Files screen, click Next. Installation will begin.

Step 6: A ESM Setup Files folder is generated in the installation directory. This contains a Setup ID file and the ESM-DS.cer file (Novell self-signing SSL certificate) required by the Management Service. Copy this file directly onto the machine designated as the host for the Management Service, either via a netshare or by saving the file to a disk or thumb drive and hand-loading it onto the server installation directory

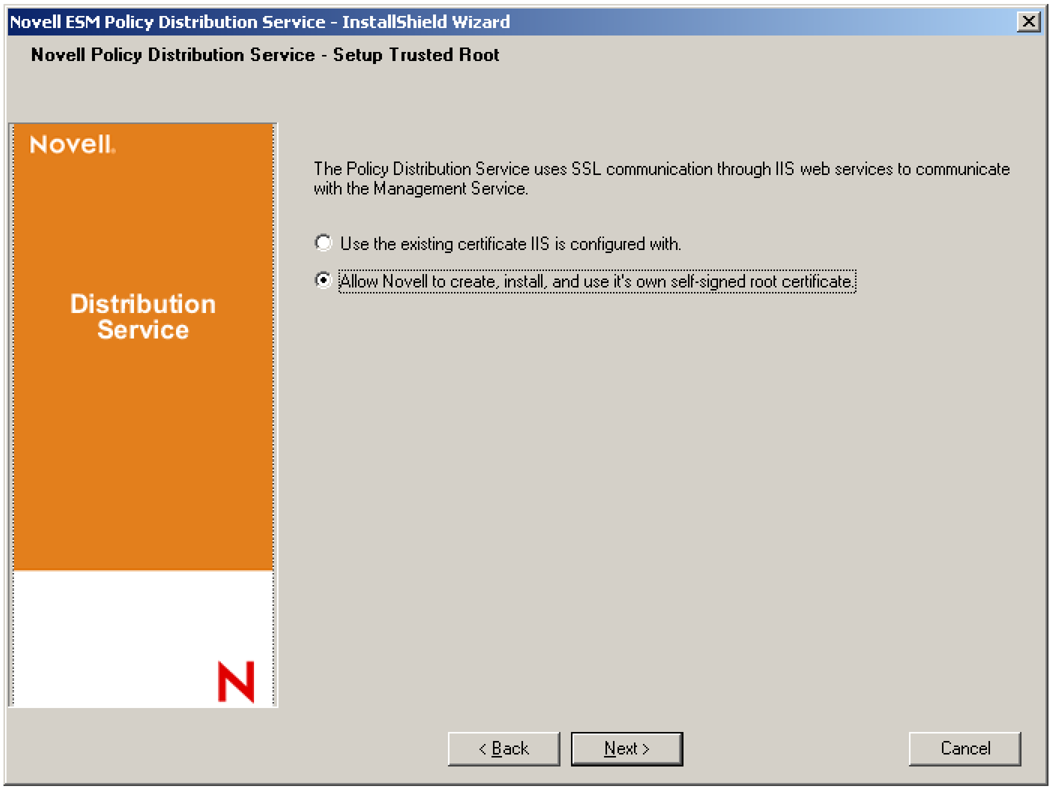
Step 7: The Policy Distribution Service is now installed, click FINISH to close the installation program to launch the performance monitor

Custom Installation

A custom installation will display the defaults used in the typical installation, and will permit the administrator to enter, or browse to, a different directory to place the software files.

The user may select either to install a Novell self-signed SSL certificate, or use one of their own.

Step 1: An SSL Certificate is required for secure communication between the Policy Distribution Service and the Management Service, and between the DS and all Novell Security Clients. If you already have a certificate authority, click: *Use the existing certificate IIS is configured for*.If you need a certificate, click: *Allow Novell to create, install, and use its own self-signed root certificate*. The installer will create the certificates and the signing authority. Regardless of the certificate type, these certificates MUST be distributed to all end users.



Novell ESM Policy Distribution Service - InstallShield Wizard

Novell Policy Distribution Service - Setup Trusted Root

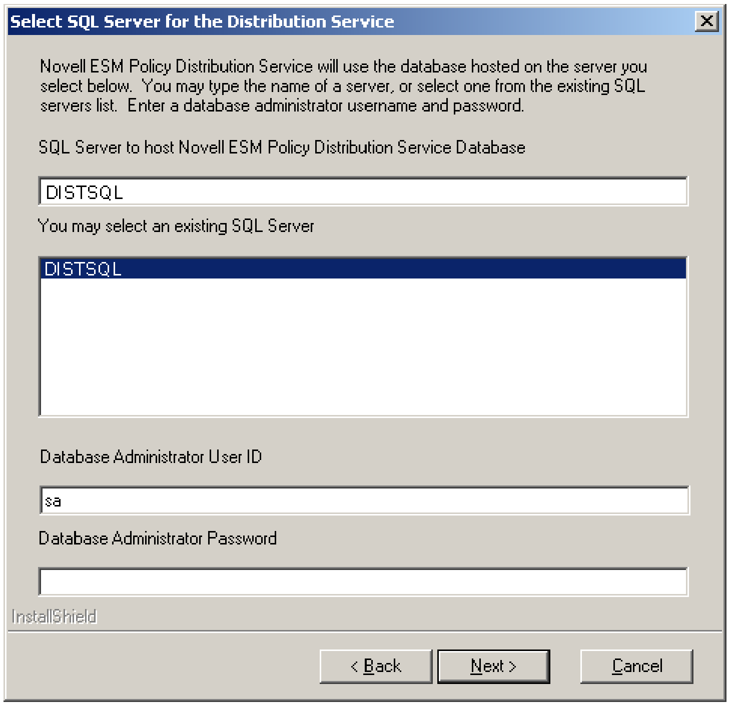
The Policy Distribution Service uses SSL communication through IIS web services to communicate with the Management Service.

○ Use the existing certificate IIS is configured with.

● Allow Novell to create, install, and use it's own self-signed root certificate.

Figure 6: Setup Trusted Root

Step 2: The installer will detect the available SQL databases on the machine and network. Select the secured SQL database for the Policy Distribution Service and enter the database administrator's name and password (if the password is zero characters, the installer will warn of the potential security issue). The username and password CANNOT be a domain user; it MUST be a SQL user with SysAdmin rights



Select SQL Server for the Distribution Service

Novell ESM Policy Distribution Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Policy Distribution Service Database

DISTSQL

You may select an existing SQL Server

DISTSQL

Database Administrator User ID

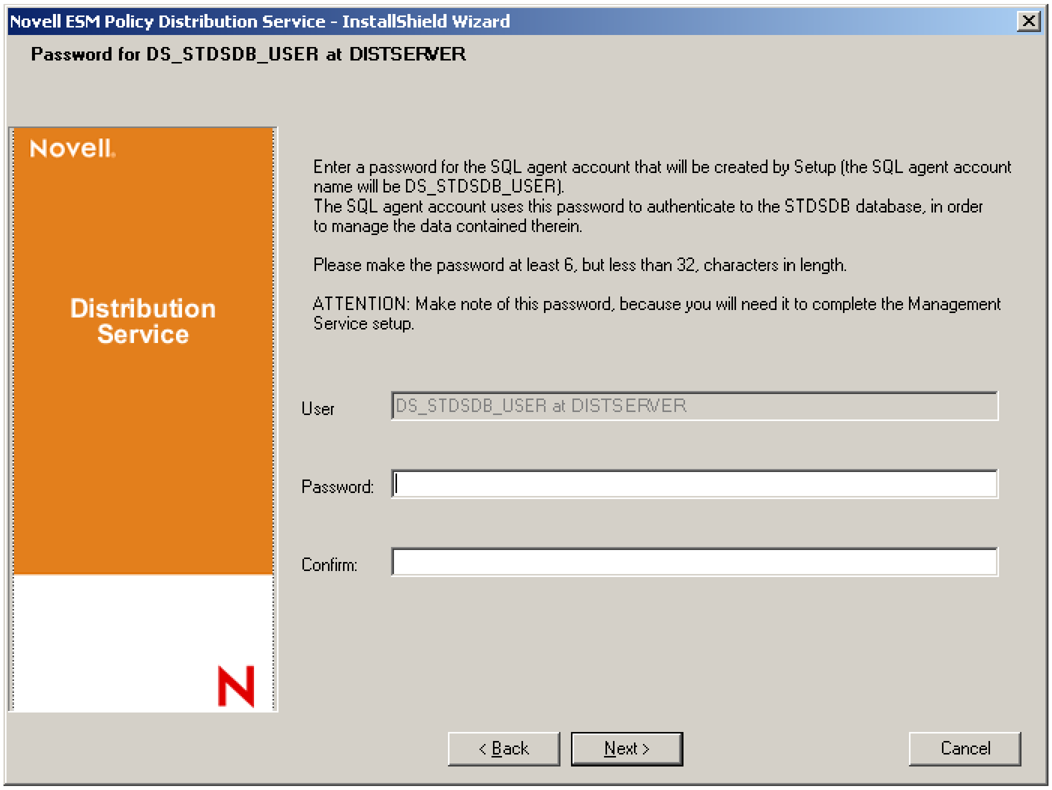
sa

Database Administrator Password

Figure 7: Select SQL Server

Step 3: Set the database name (default is entered as STDSDB).

Step 4: Enter the password for the Policy Distribution Service agent. This is the username and password the service will use to login to its SQL database



Novell ESM Policy Distribution Service - InstallShield Wizard
Novell.
Distribution Service
< Back
Next >
Cancel

Password for DS_STDSDB_USER at DISTSERVER

Enter a password for the SQL agent account that will be created by Setup (the SQL agent account name will be DS_STDSDB_USER).
The SQL agent account uses this password to authenticate to the STDSDB database, in order to manage the data contained therein.

Please make the password at least 6, but less than 32, characters in length.

ATTENTION: Make note of this password, because you will need it to complete the Management Service setup.

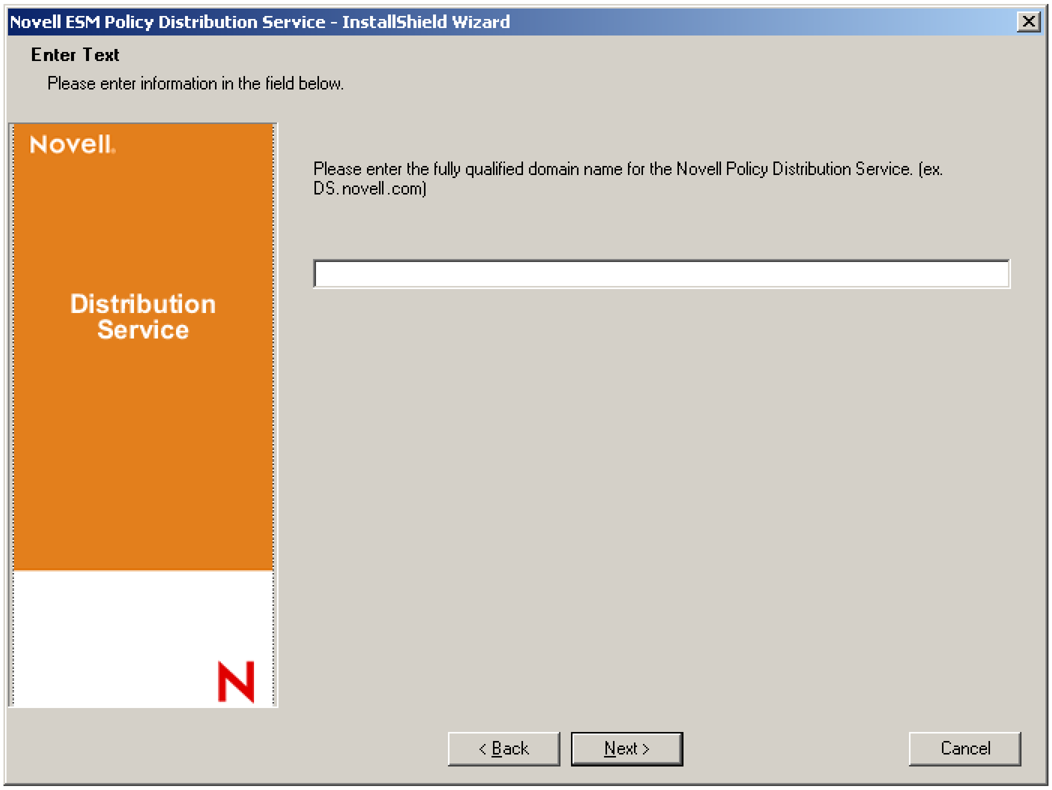
User DS_STDSDB_USER at DISTSERVER

Password:

Confirm:

Figure 8: Distribution Service SQL Password

Step 5: Enter the Policy Distribution Service domain name. This MUST be the fully qualified domain name if the server will reside outside the corporate firewall. Otherwise, only the NETBIOS name for the server is required


Novell ESM Policy Distribution Service - InstallShield Wizard
Enter Text
Please enter information in the field below.
Novell.
Distribution Service
N
< Back
Next >
Cancel

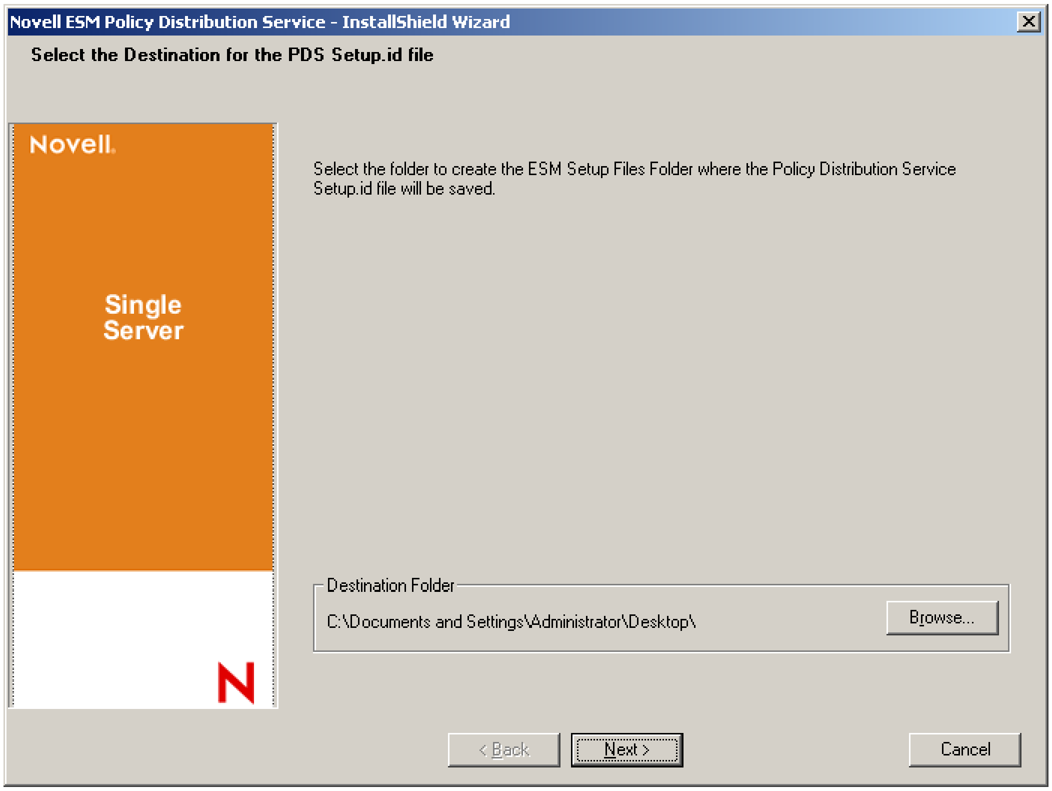
Please enter the fully qualified domain name for the Novell Policy Distribution Service. (ex. DS.novell.com)

Figure 9: Enter Policy Distribution Service Domain Name

Step 6: At the Copy Files screen, click Next. Installation will begin.

Step 7: Select the file paths for the data, index and log files.

Step 8: A ESM Setup files folder is generated in the installation directory. This contains a Setup ID file and the ESM-DS.cer file (Novell self-signing SSL certificate, if selected) required by the Management Service. Use Browse to designate where this file should be saved on the server (default = installation directory).


Novell ESM Policy Distribution Service - InstallShield Wizard

Select the Destination for the PDS Setup.id file

Select the folder to create the ESM Setup Files Folder where the Policy Distribution Service Setup.id file will be saved.

Destination Folder: C:\Documents and Settings\Administrator\Desktop\

Figure 10: Save Setup Files

Step 9: If you chose to use an enterprise SSL certificate, place a copy of this file into the ESM Setup Files folder.

Step 10: Copy the entire ESM Setup Files directly onto the machine designated as the host for the Management Service, either via a netshare or by saving the file to a disk or thumb drive and hand-loading it into the server installation directory

Step 11: The Policy Distribution Service is now installed, click FINISH to close the installation program to launch the performance monitor

Starting the Service

The Policy Distribution Service launches immediately following installation, with no reboot of the server required. The Management Console is used adjust upload times for the Distribution Service using the Configuration tool (See the ESM Adminstrator’s Manual for more details).

Continue to “Management Service Installation” on page 26.

Management Service Installation

Which server will host the Management Service?

The Management Service should be installed on a secure server behind the firewall, and CANNOT share the same server as the Policy Distribution Service (with the exception of a single server installation, see page 12). The Management Service should NOT be installed outside the network firewall, for security reasons. Ensure the required software (see page 7) is installed on the server prior to installation. Once the server is selected, note the server name... both the netbios and Fully Qualified Domain Name (FQDN).

Deployment of the Management Service on a Primary Domain Controller (PDC) is not supported for both security and functionality reasons.

Please make certain the following pre-requisites are in place PRIOR to beginning the installation:

□ Ensure ZENworks Security Client (ZSC) to MS server name resolution: validate that the target computers (where the ZSC will be installed) can "ping" the MS server name. If successful, this is the value entered in the installation shown in step 7. If unsuccessful, you will have to resolve this BEFORE continuing with the installation.

□ Enable/Install Microsoft Internet Information Services (IIS), ensure ASP.NET is enabled, and configure it to accept Secure Socket Layer (SSL) Certificates.

□ If using your own SSL certificates, ensure that the root CA is loaded on the machine and that server name validated in the previous steps (whether NETBIOS or FQDN) matches the "Issued to" value for the certificate configured in IIS.

□ If you are using your own certificates or have already installed the Novell Self Signed Certificate, you can validate SSL as well by trying the following URL from a machine that will have the ZSC installed on it: https://MS_SERVER_NAME/AuthenticationServer/UserService.asmx (Where MS_SERVER_NAME should be the server name). This should return valid data (an html page) and NOT certificate warnings. ANY certificate warnings MUST be resolved before installation (unless you opt to use Novell Self Signed Certificates instead).

□ Ensure access to a supported RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL 2005). Set database to Mixed mode.

□ Ensure access to a supported directory service (Active Directory, NT Domains*).

*= Only supported when Management Service is installed on a Microsoft Windows 2000 Advanced server (SP4)

□ Copy the ESM Setup Files directory which contains the Policy Distribution Service Setup ID and Root SSL Certificate for the Policy Distribution Service, into the installation directory of this server.

It is recommended that the MS Server be configured (hardened) so as 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, and so cannot be described in advance. Administrators are advised to consult the appropriate section of the Microsoft Technet security webpage. Additional access control recommendations are provided in the ESM Administrator's Manual.

Hardening of IIS: To protect access to only trusted machines, the virtual directory and/or IIS can be set up to have ACLs. Reference the articles below:

Granting and Denying Access to Computers

Restrict Site Access by IP Address or Domain Name

IIS FAQ: 2000 IP address and domain name restrictions

Working With IIS Packet Filtering

For security purposes, it is highly recommended the following default folders be removed from any IIS installation:

- IISHelp
- IISAdmin
- Scripts
- Printers

Novell also recommends using the IIS Lockdown Tool 2.1 available at microsoft.com.

Version 2.1 is driven by supplied templates for the major IIS-dependent Microsoft products. Select the template that most closely matches the role of this server. If in doubt, the Dynamic Web server template is recommended.

Installation Steps

Click Management Service Installation from the Installation Interface menu. The Management Service installation will begin.

At launch, the installer will verify all required software is present on the server. If any are absent, they will be installed automatically before the installation continues to the Welcome Screen (license agreements for the additional software may need to be accepted). If Microsoft Data Access Components (MDAC) 2.8 need to be installed, the server will need to reboot following that installation before ESM installation can continue. If using Windows 2003 Server, ASP.NET 1.1 will be configured to run by the installer.

Once Management Service installation begins, perform the following steps:

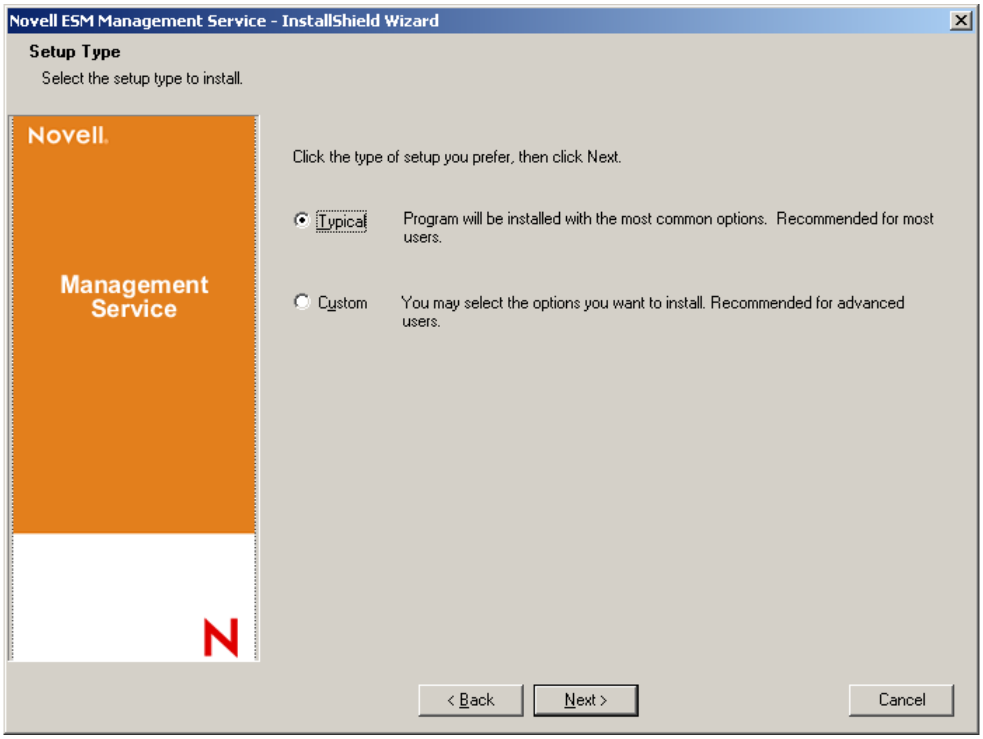
Note:

The following steps outline what you, the user, need to do to complete the installation process. Internal processes will display throughout the installation, and are not documented here unless there is a specific action or information that you will need for installation to be successful.

Step 1: Click NEXT on the Welcome screen to continue

Step 2: Accept the Licensing Agreement and click NEXT

Step 3: Select either a TYPICAL or CUSTOM installation



Novell ESM Management Service - InstallShield Wizard

Setup Type

Select the setup type to install.

Click the type of setup you prefer, then click Next.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Custom — You may select the options you want to install. Recommended for advanced users.

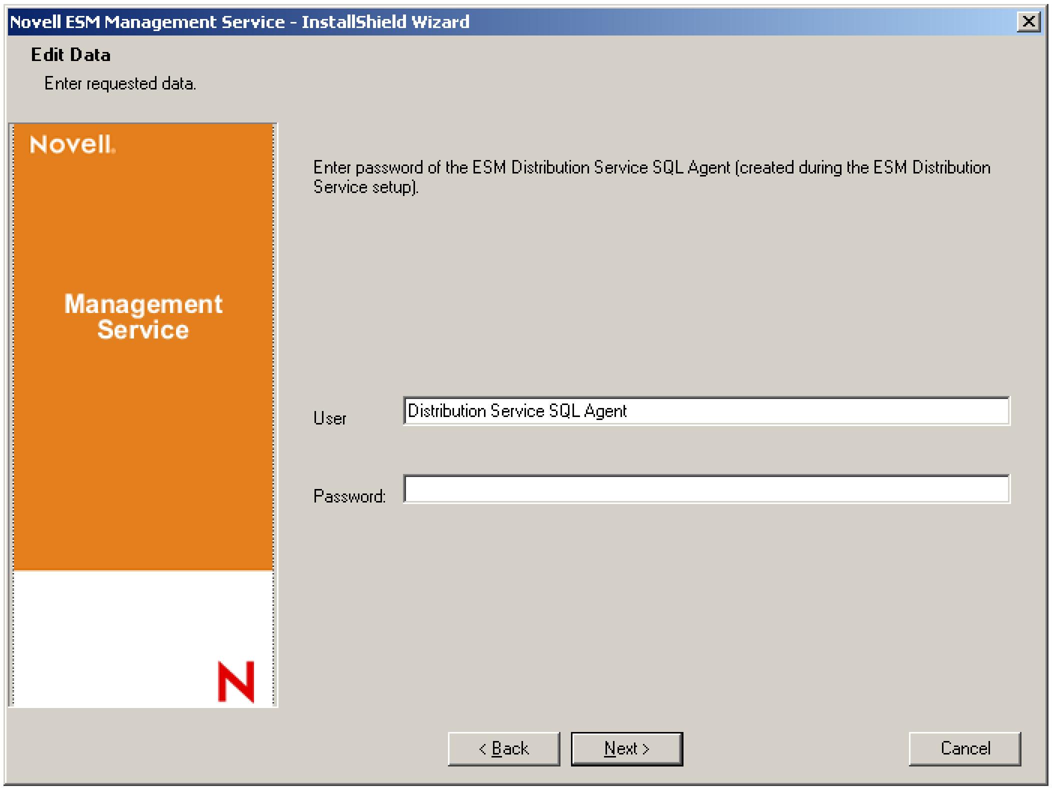
Figure 11: Select Typical or Custom

Both installation paths are presented below:

Typical Installation

A typical installation places the Management Service software files in the default directory: \Program Files\Novell\ESM Management Service. The SQL database name is assigned as STMSDB. The three SQL database files (data, index, and log) are placed in: \Program Files\Microsoft SQL Server\mssql\Data.

Step 1: Enter the Policy Distribution Service's agent password, created in Step 7 of DS installation



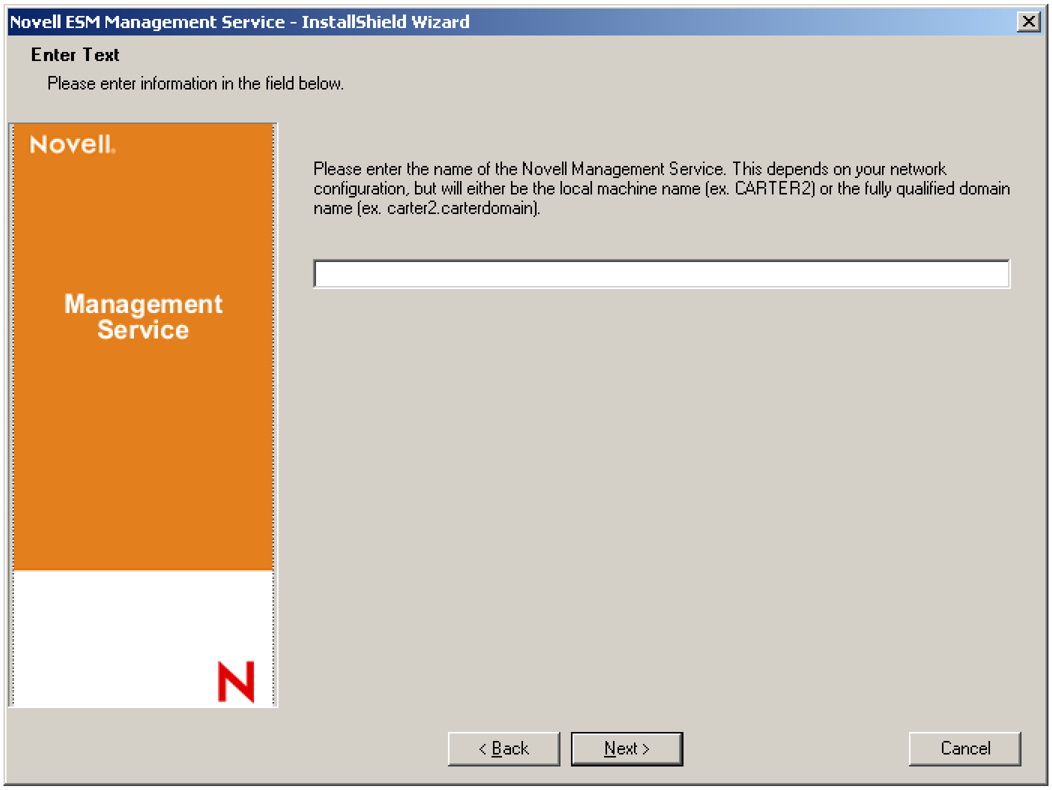
Enter password of the ESM Distribution Service SQL Agent (created during the ESM Distribution Service setup).

User Distribution Service SQL Agent

Password:

Figure 12: Enter SQL password

Step 2: Enter the name of the server that will host the Management Service.



Novell ESM Management Service - InstallShield Wizard

Enter Text

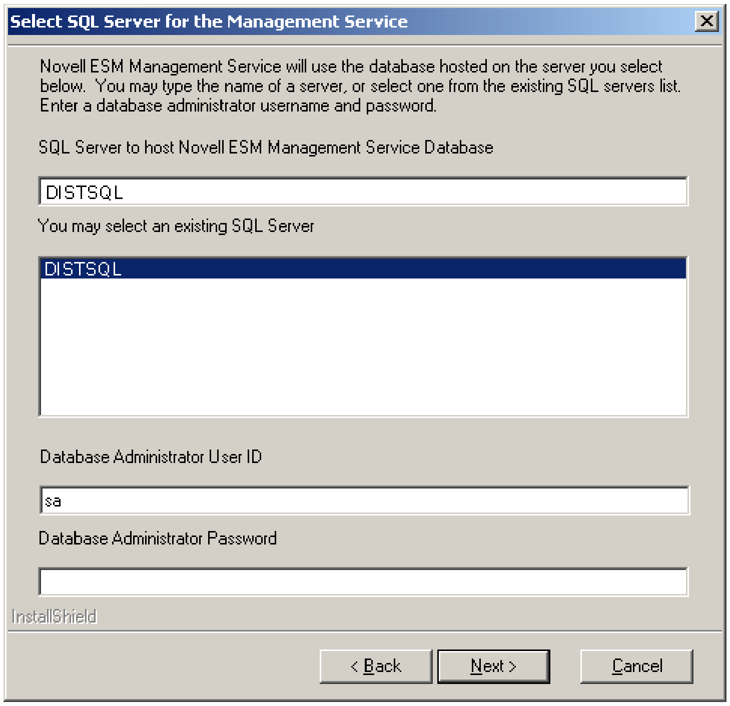
Please enter information in the field below.

Please enter the name of the Novell Management Service. This depends on your network configuration, but will either be the local machine name (ex. CARTER2) or the fully qualified domain name (ex. carter2.carterdomain).

Figure 13: Enter MS Server Name

Step 3: Novell SSL Certificates are created for the installation. If you wish to use your own SSL certificates, please go to Custom Installation. These certificates MUST be distributed to all end users.

Step 4: The installer will detect the available SQL databases on the machine and network. Select the SQL database for the Management Service and enter the database administrator's username and password (if the password is zero characters, the installer will warn of the potential security issue). The username and password CANNOT be a domain user; it must be a SQL user with SysAdmin rights.



Select SQL Server for the Management Service

Novell ESM Management Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Management Service Database

DISTSQL

You may select an existing SQL Server

DISTSQL

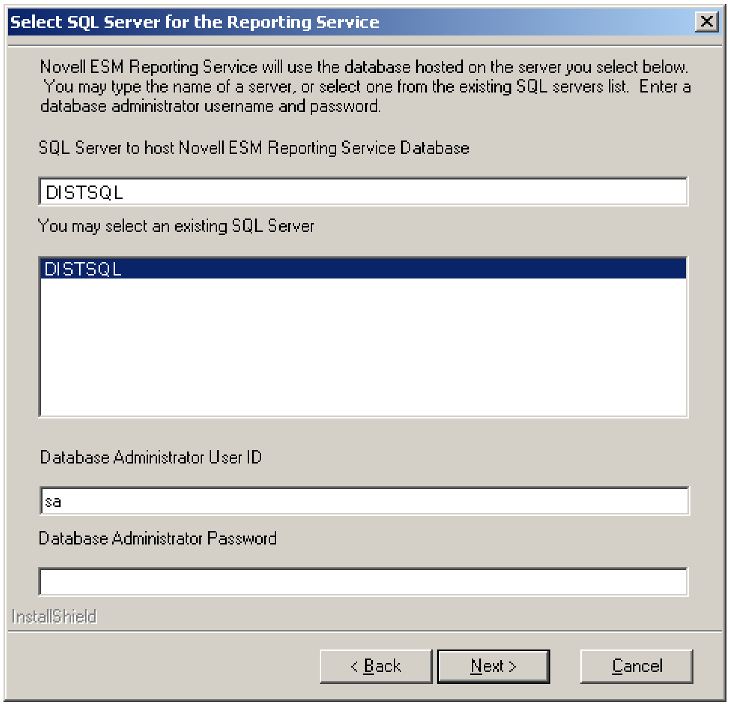
Database Administrator User ID

sa

Database Administrator Password

Figure 14: Select MS SQL Database

Step 5: Select the SQL database for the Reporting Service and enter the database administrator's password for that database. If you plan to capture and store a large number of reports, it is recommended that the Reporting Service database be given its own SQL server.



Select SQL Server for the Reporting Service

Novell ESM Reporting Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Reporting Service Database

DISTSQL

You may select an existing SQL Server

DISTSQL

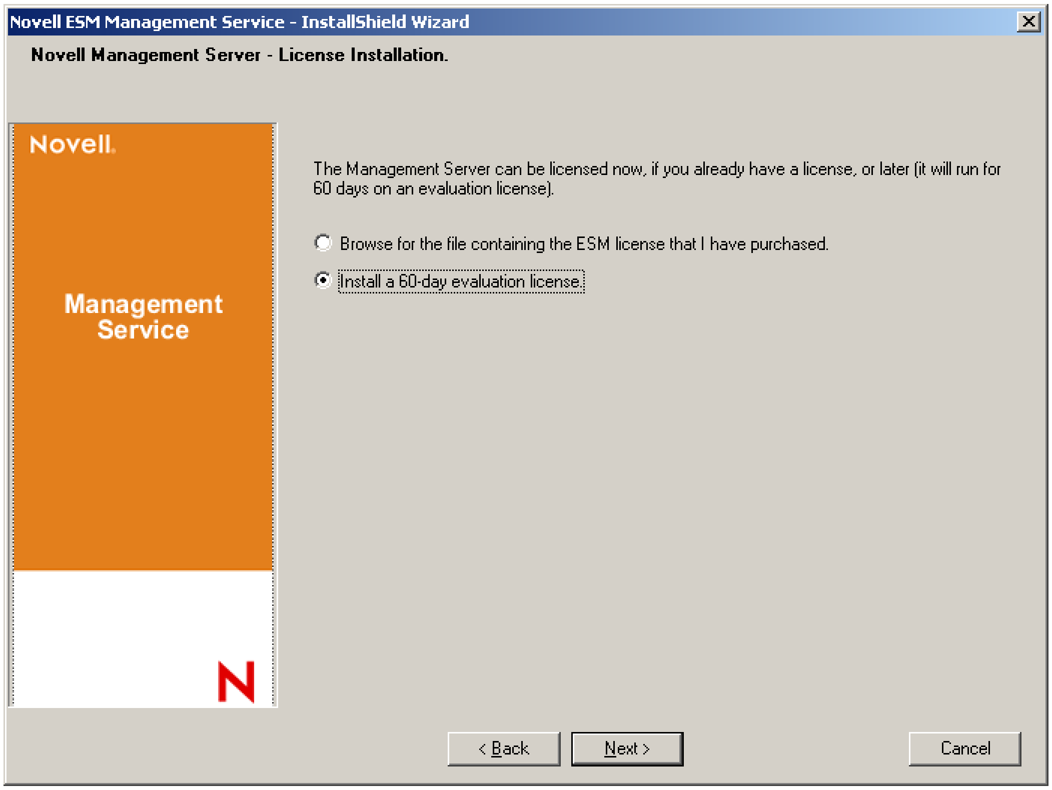
Database Administrator User ID

sa

Database Administrator Password

Figure 15: Select Reporting Service Database

Step 6: If ESM has already been purchased, a separate license file is provided. Copy the license file to this server and browse for it (see the instructions page included with your License file for more details). If you have not yet purchased an ESM license, select 60-Day Evaluation License to continue.



Novell ESM Management Service - InstallShield Wizard

Novell Management Server - License Installation.

The Management Server can be licensed now, if you already have a license, or later (it will run for 60 days on an evaluation license).

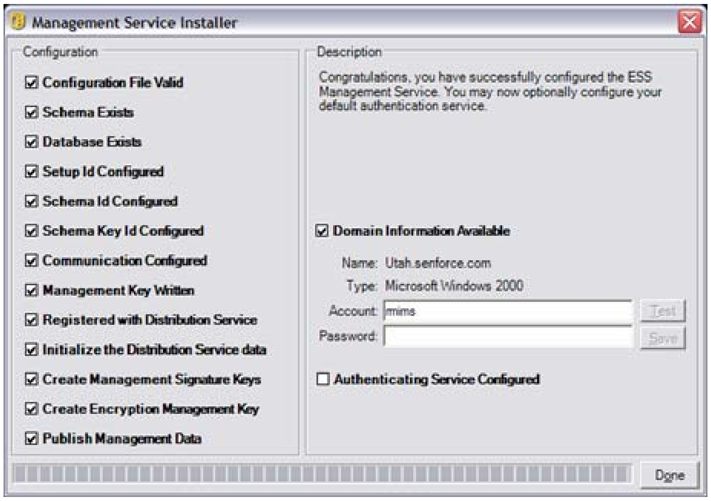
○ Browse for the file containing the ESM license that I have purchased.

● Install a 60-day evaluation license.

Figure 16: Browse for Novell License File

Step 7: At the Copy Files screen, click Next. Installation will begin.

Step 8: The Management Service will run a communication check to both SQL databases and the Policy Distribution Service. If communication cannot be verified, the installer will notify you of the issue. ALL boxes must be checked for installation to succeed.



Management Service Installer

Configuration

☑ Configuration File Valid

☑ Schema Exists

☑ Database Exists

☑ Setup Id Configured

☑ Schema Id Configured

☑ Schema Key Id Configured

☑ Communication Configured

☑ Management Key Written

☑ Registered with Distribution Service

☑ Initialize the Distribution Service data

☑ Create Management Signature Keys

☑ Create Encryption Management Key

☑ Publish Management Data

Description

Congratulations, you have successfully configured the ESS Management Service. You may now optionally configure your default authentication service.

☑ Domain Information Available

Name: Utah.senforce.com

Type: Microsoft Windows 2000

Account: mims

Password:

☐ Authenticating Service Configured

Figure 17: Communication Verification

Step 9: If this installation is occurring on a member server for a domain carrying a directory service, the installer will automatically detect and add the following data into the installation, using a secure, read-only connection:

- Root domain name or machine name
- Domain administrator's name or a resource account with appropriate read permissions

Step 10: Enter the administrator's password in the space provided and click Test to verify connection can be established. If the test is successful, click Save. If the test fails, or the correct domain is not detected it will need to be added manually through the Management Console (see “Adding Directory Services” on page 44)

Note:

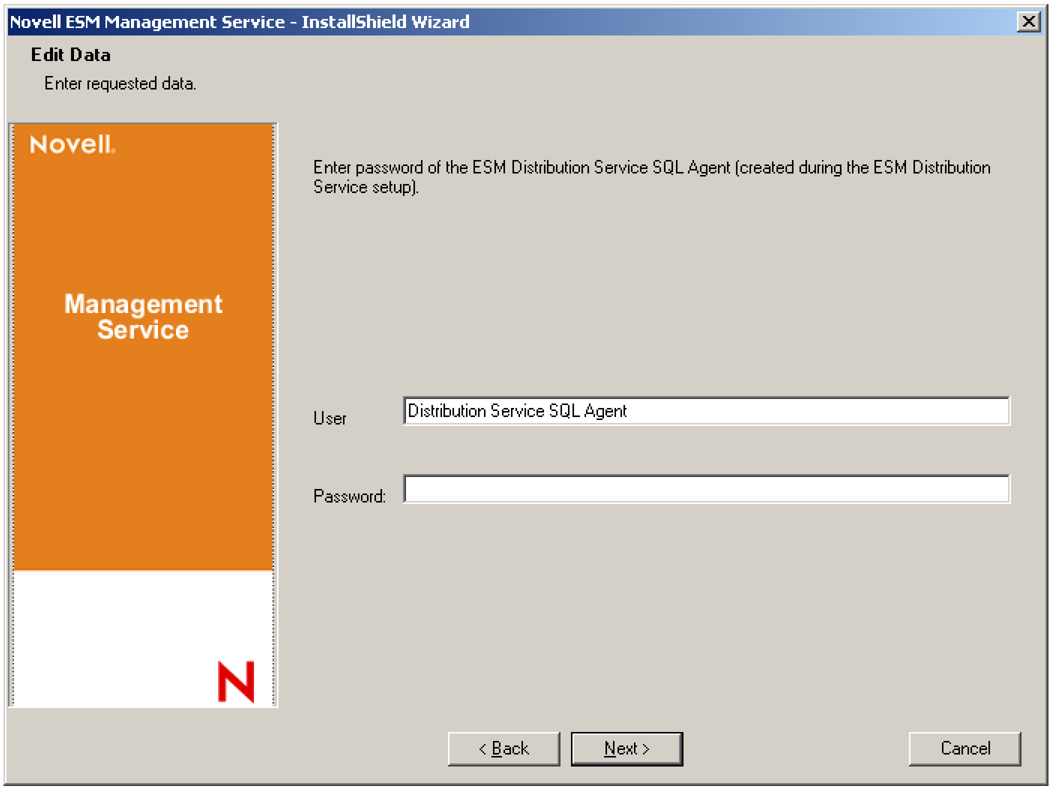
The password entered here should be set to not expire, nor should this account ever be disabled.

Step 11: The Management Service is now installed, click FINISH to close the installation program and launch the performance monitor

Custom Installation

A custom installation will display the defaults used in the typical installation, and will permit the administrator to enter, or browse to, a different location.

Step 1: Enter the Policy Distribution Service's agent password, created in DS installation.



Enter password of the ESM Distribution Service SQL Agent (created during the ESM Distribution Service setup).

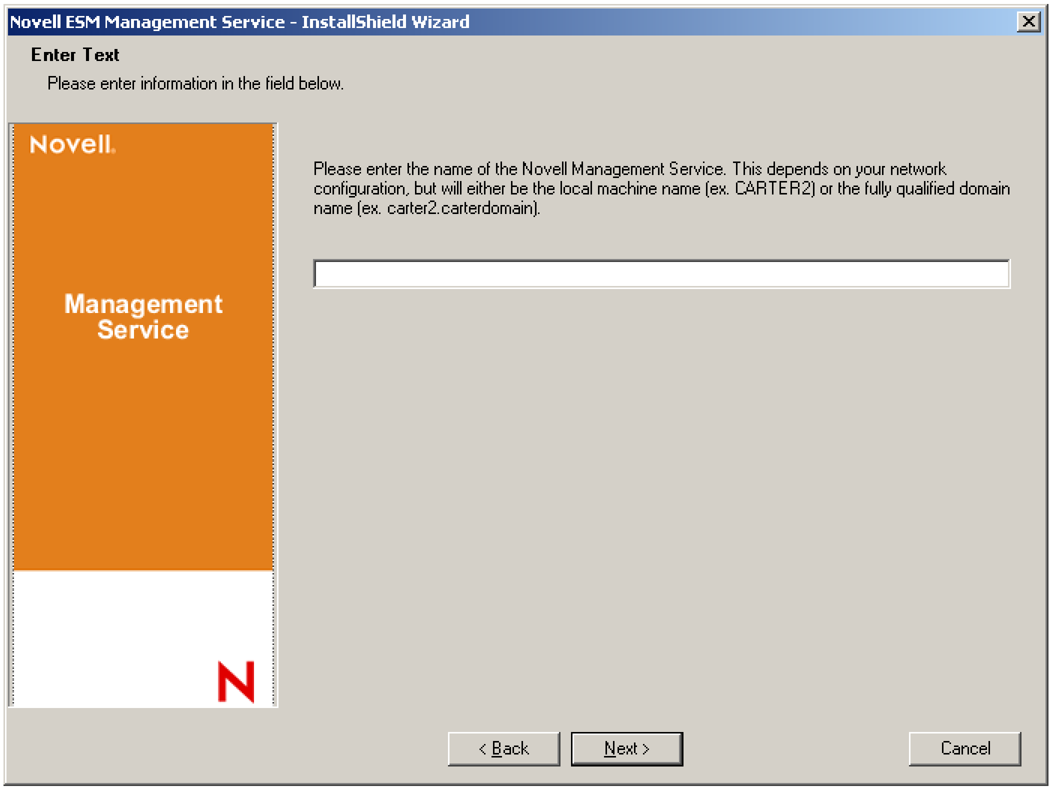
User Distribution Service SQL Agent

Password:

Figure 18: Enter SQL password

Step 2: Select the SSL Certificate type used for the Policy Distribution Service installation. If you used your existing (enterprise) certificate authority, click: *The Novell Distribution Service Used a certificate IIS was already configured with*. If the Distribution Service installer created a Novell certificate, click: *The Novell Distribution Service installed a Novell self signed root certificate*.

Step 3: Enter the name of the server that will host the Management Service


Novell ESM Management Service - InstallShield Wizard

Enter Text

Please enter information in the field below.

Please enter the name of the Novell Management Service. This depends on your network configuration, but will either be the local machine name (ex. CARTER2) or the fully qualified domain name (ex. carter2.carterdomain).

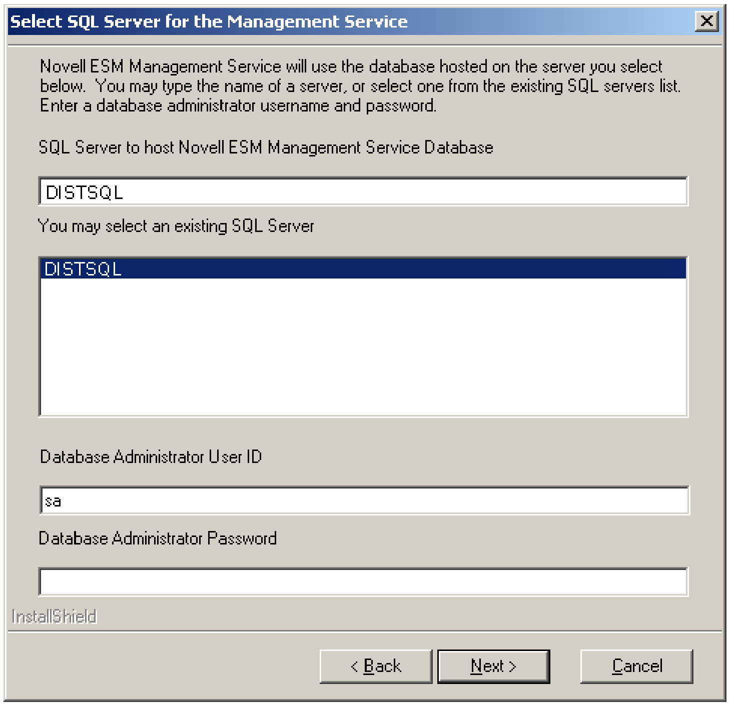
Figure 19: Enter MS Server Name

Step 4: An SSL Certificate is required for secure communication between the Management Service and all ZENworks Security Clients. If you already have a certificate authority, click: *Use the existing certificate IIS is configured for.*If you need a certificate, click: *Allow Novell to create, install, and use its own self-signed root certificate*. The installer will create the certificates and the signing authority. Regardless of the certificate type, these certificates MUST be distributed to all end users.

Step 5: When selecting Novell certificates, select where the certificate can be saved for easy distribution (default = installation directory).

Step 6: The installer will detect the available SQL databases on the machine and network. Select the SQL database for the Management Service and enter the database administrator's username and password (if the password is zero characters, the installer will warn of the potential security issue). The username and password CANNOT be a domain user; it must be a SQL user with SysAdmin rights

.



Select SQL Server for the Management Service

Novell ESM Management Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Management Service Database

DISTSQL

You may select an existing SQL Server

DISTSQL

Database Administrator User ID

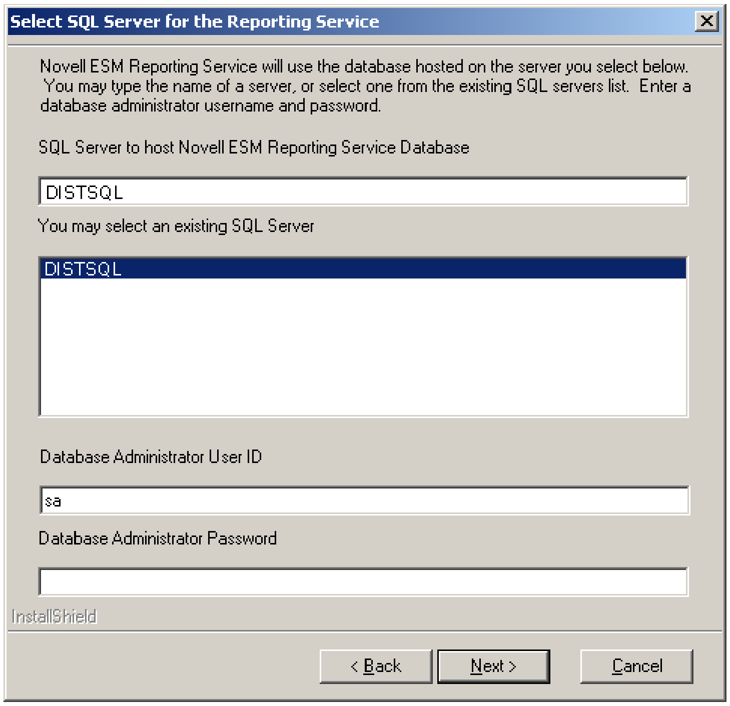
sa

Database Administrator Password

Figure 20: Select MS SQL Database

Step 7: Set the database name (default is entered as STMSDB).

Step 8: Select the SQL database for the Reporting Service and enter the database administrator's password for that database.



Select SQL Server for the Reporting Service

Novell ESM Reporting Service will use the database hosted on the server you select below. You may type the name of a server, or select one from the existing SQL servers list. Enter a database administrator username and password.

SQL Server to host Novell ESM Reporting Service Database

DISTSQL

You may select an existing SQL Server

DISTSQL

Database Administrator User ID

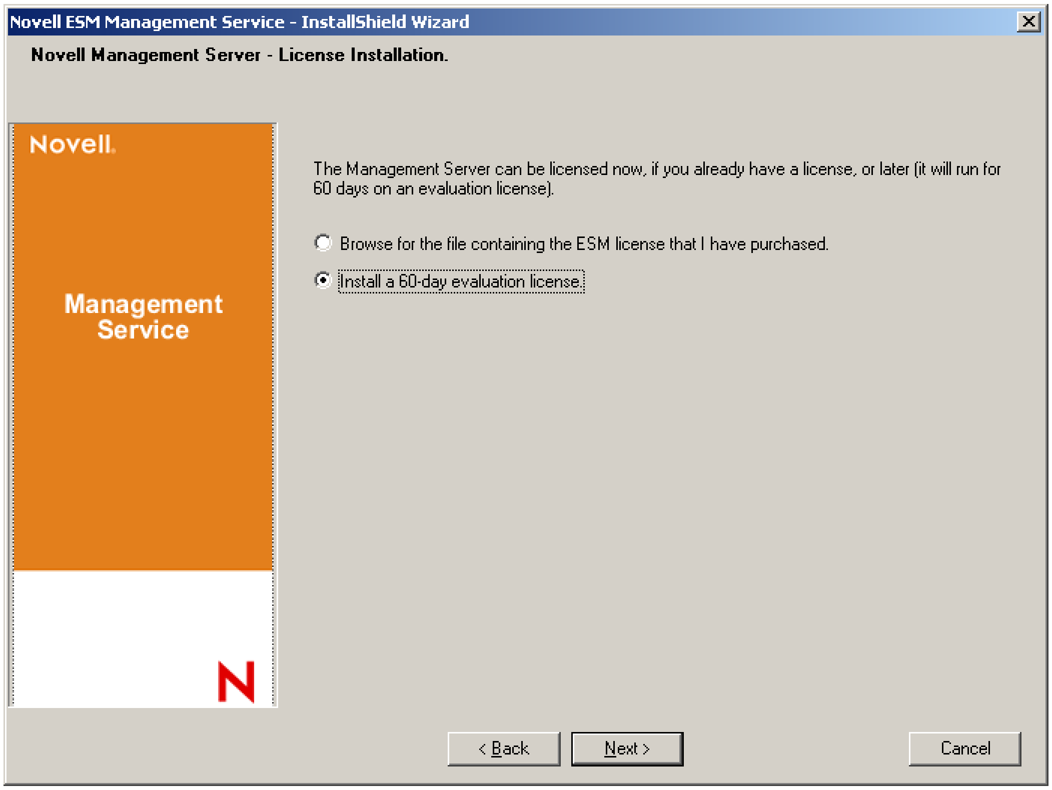
sa

Database Administrator Password

Figure 21: Select Reporting Service Database

Step 9: Set the database name (default is entered as STRSDB)

Step 10: If ESM has already been purchased, a separate license file is provided. Copy the license file to this server and browse for it (see the instructions page included with your License file for more details). If you have not yet purchased an ESM license, select 60-Day Evaluation License to continue.



Novell ESM Management Service - InstallShield Wizard

Novell Management Server - License Installation.

The Management Server can be licensed now, if you already have a license, or later (it will run for 60 days on an evaluation license).

○ Browse for the file containing the ESM license that I have purchased.

● Install a 60-day evaluation license.

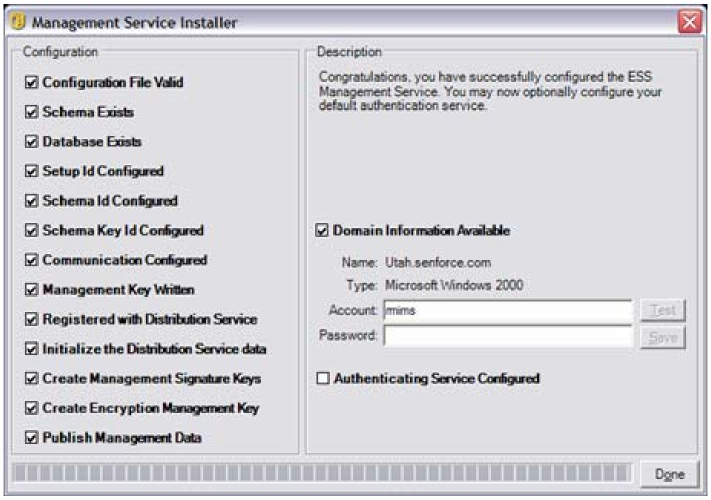
Figure 22: Browse for Novell License File

Step 11: At the Copy Files screen, click Next. Installation will begin.

Step 12: Select the file paths for the Management Service database’s data, index and log files.

Step 13: Select the file paths for the Reporting Service database’s data, index and log files.

Step 14: The Management Service will run a communication check to both SQL databases and the Policy Distribution Service. If communication cannot be verified, the installer will notify you of the issue. ALL boxes must be checked for installation to succeed.



☑ Configuration File Valid
☑ Schema Exists
☑ Database Exists
☑ Setup Id Configured
☑ Schema Id Configured
☑ Schema Key Id Configured
☑ Communication Configured
☑ Management Key Written
☑ Registered with Distribution Service
☑ Initialize the Distribution Service data
☑ Create Management Signature Keys
☑ Create Encryption Management Key
☑ Publish Management Data

Congratulations, you have successfully configured the ESS Management Service. You may now optionally configure your default authentication service.

☑ Domain Information Available

Name: Utah.senforce.com
Type: Microsoft Windows 2000
Account: mims
Password:

☐ Authenticating Service Configured

Figure 23: Communication Verification

Step 15: If this installation is occurring on a member server for a domain carrying a directory service, the installer will automatically detect and add the following data into the installation, using a secure, read-only connection:

- Root domain name or machine name
- Domain administrator's name or a resource account with appropriate read permissions

Note:

The password entered here should be set to not expire, nor should this account ever be disabled.

Step 16: Enter the administrator's password in the space provided and click Test to verify connection can be established. If the test is successful, click Save. If the test fails, or the correct domain is not detected it will need to be added manually through the Management Console (see “Adding Directory Services” on page 44)

Step 17: The Management Service is now installed, click FINISH to close the installation program and launch the performance monitor

Starting the Service

The Management Service launches immediately following installation, with no reboot of the server required. The Management Console is used to manage the data on the Management Service (see the ESM Administrator’s Guide for more details).

Novell recommends installing the Management Console on this server. If installing the Management Console on a separate machine, copy the ESM Setup Files directory, either via a netshare or by saving the file to a disk or thumb drive, to the machine that will host the Management Console.

Continue to “Management Console Installation” on page 39.

Management Console Installation

Where will you host the Management Console?

The Management Console can be installed on the Management Service server, or on a secure PC that has direct communication with the Management Service server. Multiple Management Console can be configured to communicate with a single Management Service, however, it is highly recommended that access to the Management Console be limited to select users.

For security reasons, it is recommended that the Management Console be installed directly on the MS Server.

If installing on a separate workstation, please make certain the following pre-requisites are in place PRIOR to beginning the installation:

- □ The required operating systems when running the Management Console on a PC are: Windows XP SP1, Windows XP SP2, or Windows 2000 SP4. A 1.0 GHz processor is recommended, with a minimum of 256 MB of RAM and 100 MB of disk space available
- □ Copy the ESM Setup files folder which contains the SSL Root Certificates for the Policy Distribution Service and the Management Service, along with the STInstParam.id file, onto the PC
- □ If installing on the Management Service server, verify that the version of Microsoft Internet Explorer is 5.5 or greater.

Installation Steps

Click Management Console Installation from the Installation Interface menu.

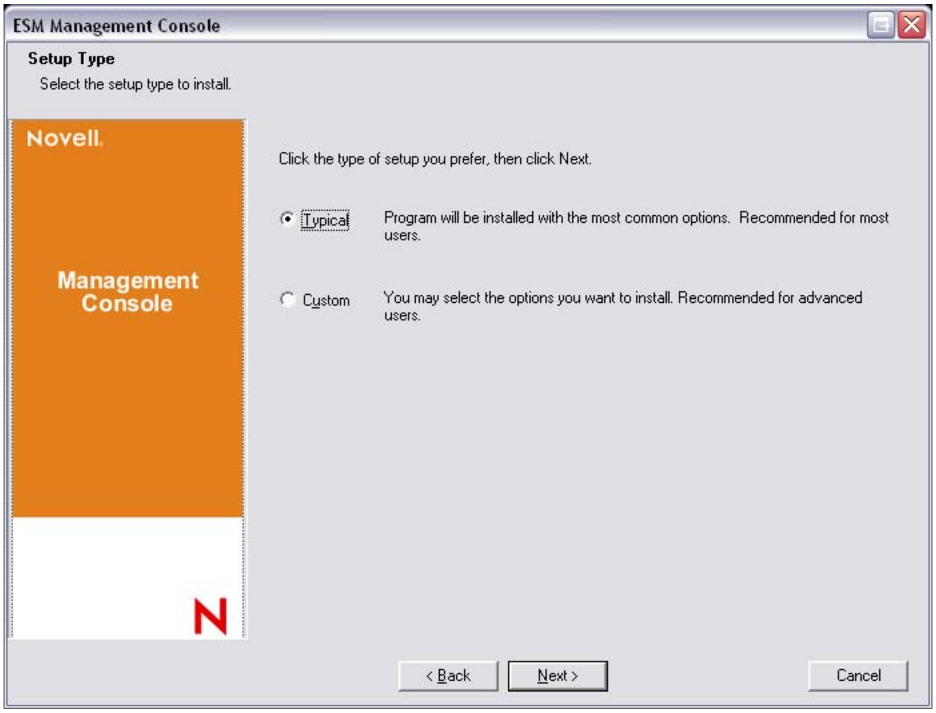
At launch, the installer will verify both the required .NET Framework 1.1 and WSE 2.0 SP2 are present on the machine. If one or both are absent, they will be installed automatically before the installation continues to the Welcome Screen (the license agreement for .NET 1.1 will need to be accepted).

To install the Management Console, perform the following steps:

Step 1: Click NEXT to continue.

Step 2: Accept the Licensing Agreement and click NEXT.

Step 3: Select either a TYPICAL or CUSTOM installation.



Setup Type

Select the setup type to install.

Click the type of setup you prefer, then click Next.

● Typical Program will be installed with the most common options. Recommended for most users.

○ Custom You may select the options you want to install. Recommended for advanced users.

Figure 24: Select Typical or Custom

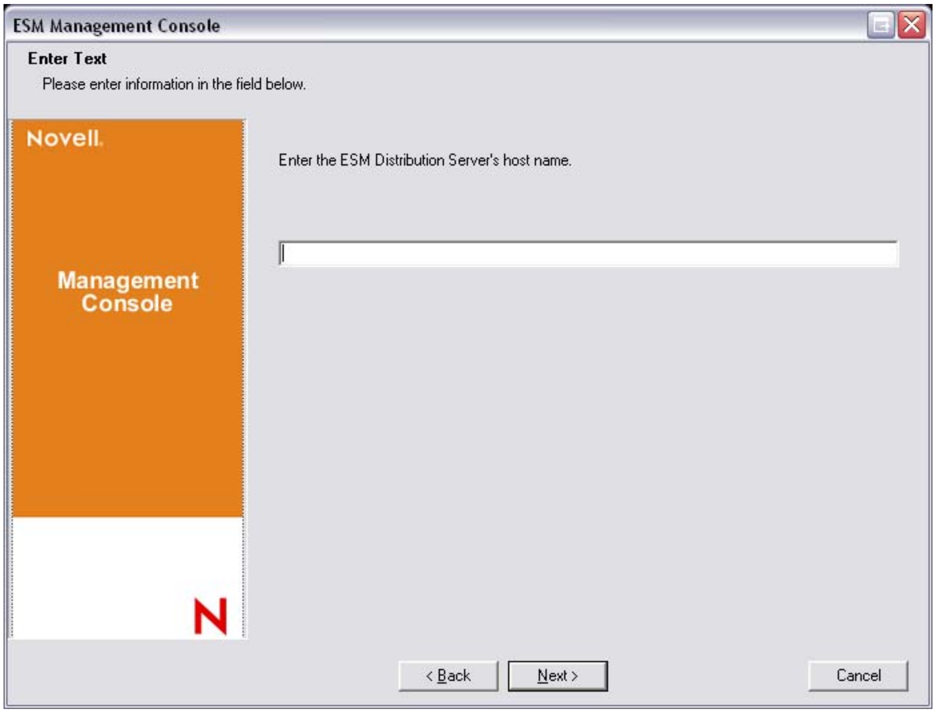
Typical Installation

A typical installation will use all the default server and SSL information contained in the STInstParam.id file and will make the default directory: \Program Files\Novell\ESM Management Console. No additional selections need to be made for Management Console installation, providing the ESM Setup Files directory is on the machine.

Custom Installation

A custom installation will display the STInstParam.id defaults used in the typical installation, and will permit the administrator to change that information.

Step 1: Enter the Policy Distribution Service's hostname (this must be the fully-qualified domain name if the Distribution server is deployed outside the enterprise firewall).



Enter the ESM Distribution Server's host name.

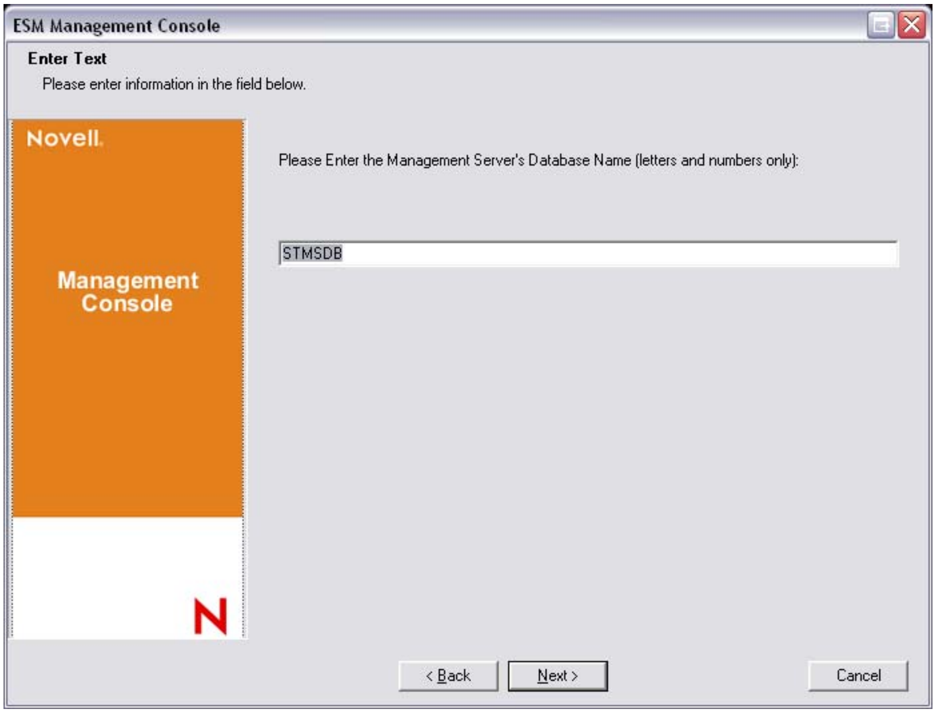
Figure 25: Enter Distribution Service Host Name

Step 2: Enter the Management Service hostname

Step 3: Enter the Management Service SQL database hostname

Step 4: Enter the Management Service SQL database name

.



Please Enter the Management Server's Database Name (letters and numbers only):

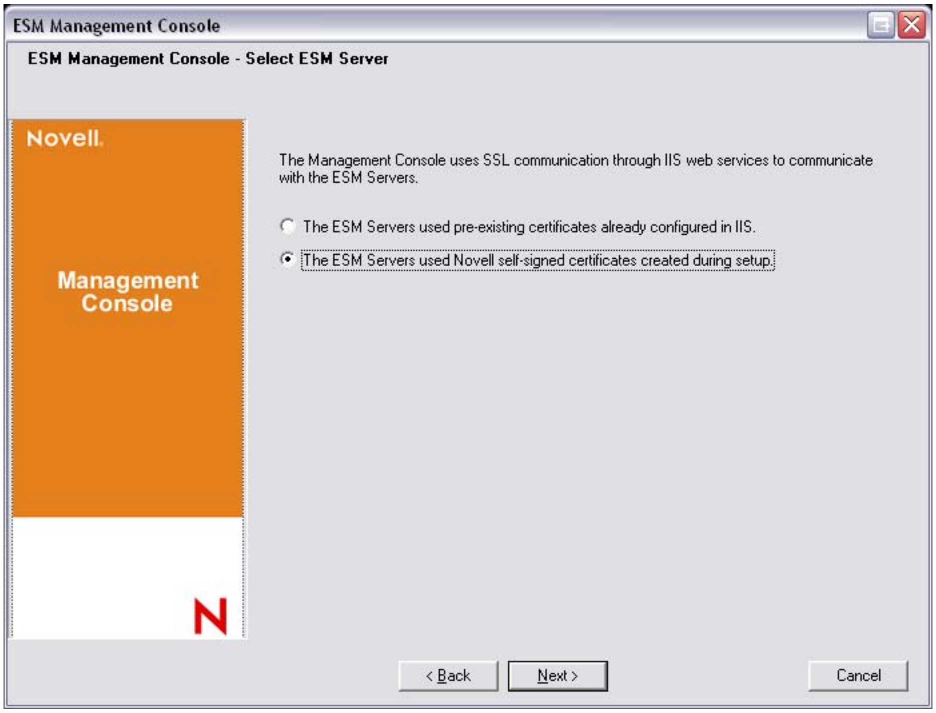
STMSDB

Figure 26: Enter MS SQL database name

Step 5: Enter the SQL SA username and password identified during Management Service installation

Step 6: Select the type of SSL Certificate installed on the Policy Distribution Service and the Management Service

.



ESM Management Console - Select ESM Server

The Management Console uses SSL communication through IIS web services to communicate with the ESM Servers.

○ The ESM Servers used pre-existing certificates already configured in IIS.

● The ESM Servers used Novell self-signed certificates created during setup.

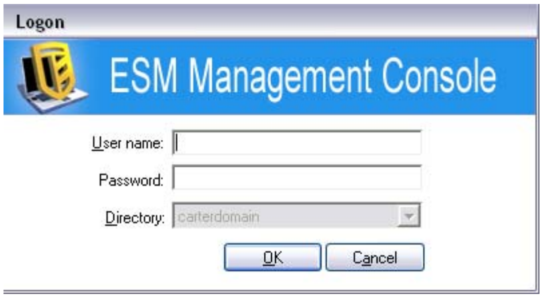
Figure 27: Select Server Certificates

Step 7: Select the directory where the Management Console will be installed (default: \Program Files\Novell\ESM Management Console)

The Management Console is now installed.

Starting the Console

Double-click the Management Console Icon on the desktop to launch the Management Console login window. Log into the Management Console by entering the administrator and password. Before you can enter the username and password, you will need to be connected to the directory service's domain. The username entered MUST be a user on the Management Service domain.



User name:

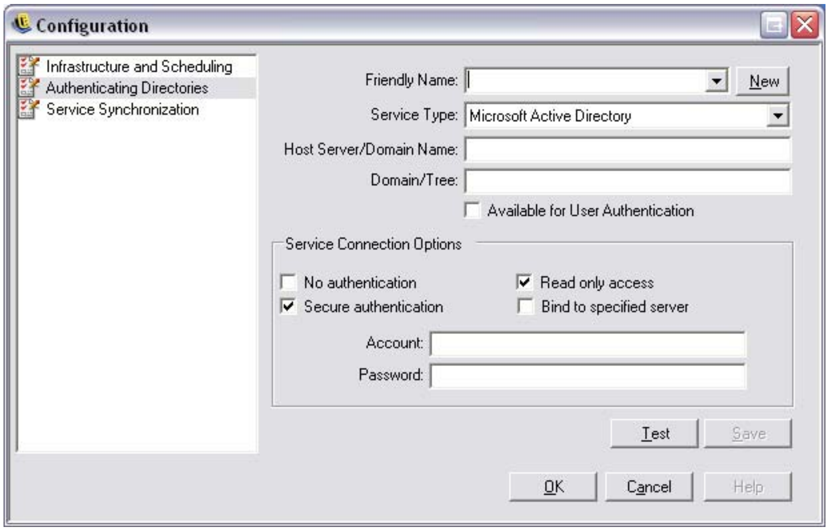
Password:

Directory: carterdomain

Figure 28: Login to ESM Management Console

Adding Directory Services

Step 1: Click the Options button on the login screen, The Configuration window will display.



Friendly Name:

Service Type: Microsoft Active Directory

Host Server/Domain Name:

Domain/Tree:

☐ Available for User Authentication

Service Connection Options

☐ No authentication ☑ Read only access

☑ Secure authentication ☐ Bind to specified server

Account:

Password:

Figure 29: Authenticating Directories

Step 2: Click Authenticating Servers to display the Listening and Validation Service Manager

Step 3: Enter a friendly name for the Directory Service and select its Service Type from the pull-down list

Step 4: In the Host/DN box enter the hostname of a domain controller and leave the Domain/DC box blank (this box will auto populate after a successful test of the user account in Step 8)

Step 5: Check Available for User Authentication if this is the domain a Management Service is installed on to display the domain in the login pull-down menu. If this is a separate domain, leave unchecked

Step 6: Select a Service Connection Option:

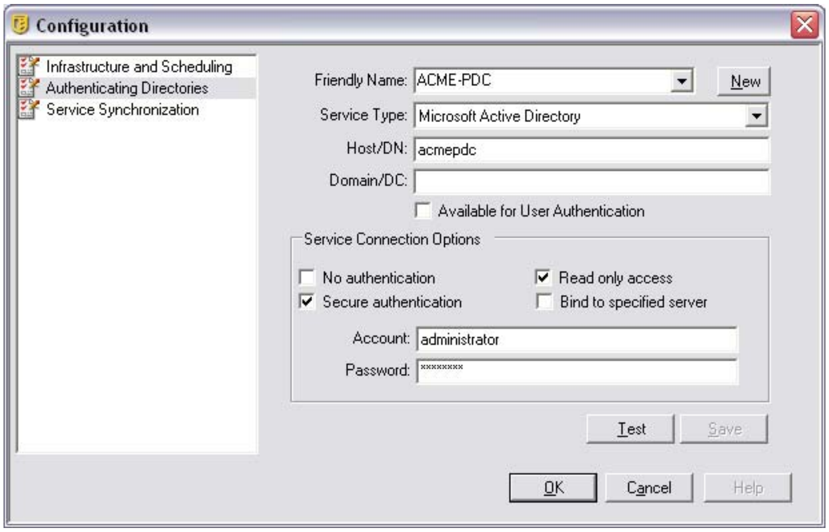
- No authentication - login and password not required for connection to directory service (NOT a recommended configuration)
- Secure authentication - login and password required for connection to directory service
- Read only access - Management Service cannot make updates or changes to the directory service
- Bind to specified server - creates a direct connection to the server hosting the directory service (machine name [netbios] name must be specified in Step 1). This will increase the speed and efficiency of the connection between the services

Step 7: Enter the directory service login name under Account and the login password in the Password field. The login name entered must be a user who has permission to view the ENTIRE directory tree. It is recommended that this user be either the domain administrator or an OU administrator

Note:

The password entered should be set to not expire, nor should this account ever be disabled.

Step 8: Click Test to verify communication to this directory service. If communication cannot be established, the user is notified of the error. Any inaccurate information will be corrected (when possible) by the interface during the test



Friendly Name: ACME-PDC

Service Type: Microsoft Active Directory

Host/DN: acmepdc

Domain/DC:

□ Available for User Authentication

Service Connection Options

□ No authentication ☑ Read only access

☑ Secure authentication □ Bind to specified server

Account: administrator

Password: ********

Figure 30: Completed Directory Screen

Step 9: Click Save to add this directory service to the database. Click New to add another directory service to the database.

Step 10: Click OK or Cancel to exit the Configuration window and return to the login screen.

Management Console Permissions Settings

This control is found in the Tools menu of the Management Console, and is only accessible by the primary administrator for the Management Service and/or any whom have been granted "permissions" access by that administrator. This control is not available when running the "Stand-Alone" Management Console (see “ESM Unmanaged Installation” on page 61, for more details).

The permissions settings define which user or group of users are permitted access to the Management Console, Publish Policies, and/or Change Permission Settings.

During the Management Server installation, an administrator or Resource Account name is entered into the configuration form (see Management Service Installation Steps). Once a successful test has been performed and the user information saved, five permissions are automatically granted to this user (see below).

Once the Management Console is installed, ALL user groups within the domain will be granted full permissions. The resource user should remove permissions from all but the groups/users who should have access. The resource user may set additional permissions for the designated users. The permissions granted have the following results:

- Management Console Access: the user may view policies and components, and edit existing policies. Users granted ONLY this privilege will not be permitted to add or delete polices; the publish and permissions options will be unavailable
- Publish Policy: the user may publish policies ONLY to assigned users/groups
- Change Permission: the user may access and change permissions settings for other users that have already been defined, or grant permissions to new users
- Create Policies: the user may create new policies in the Management Console
- Delete Policies: the user may delete ANY policy in the Management Console

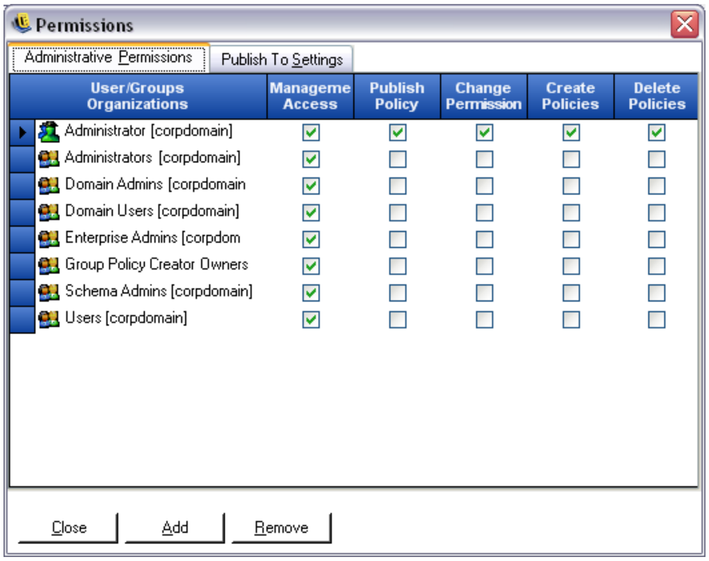
Note:

For security purposes, it is recommended that only the resource user or very FEW administrators be granted the Change Permission and Delete Policies permissions.

Administrative Permissions

To set the Administrative Permissions for individual users, perform the following steps:

Step 1: Open the Tools menu and select *Permissions*. The groups associated with this domain are displayed.



User/Groups Organizations	Manageme Access	Publish Policy	Change Permission	Create Policies	Delete Policies
Administrator [corpdomain]	☑	☑	☑	☑	☑
Administrators [corpdomain]	☑	□	□	□	□
Domain Admins [corpdomain	☑	□	□	□	□
Domain Users [corpdomain]	☑	□	□	□	□
Enterprise Admins [corpdom	☑	□	□	□	□
Group Policy Creator Owners	☑	□	□	□	□
Schema Admins [corpdomain]	☑	□	□	□	□
Users [corpdomain]	☑	□	□	□	□

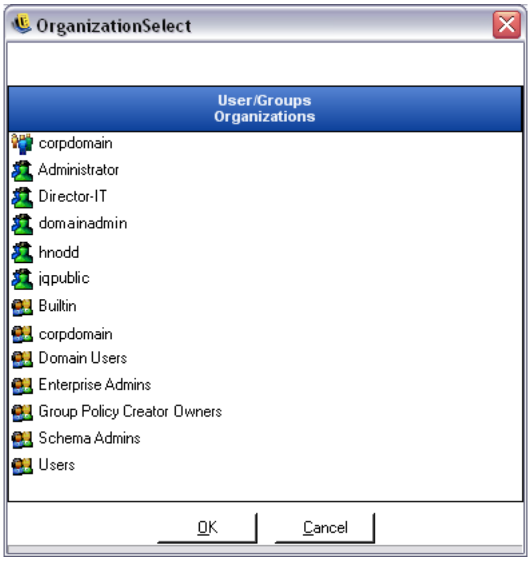
Figure 31: Management Console Permissions Settings Window

Note:

All groups are granted full permissions in the Management Console by default. Administrators should immediately uncheck any and all policy tasks from unauthorized groups. Access to the console can be removed by un-checking that permission.

Step 2: To load users and/or new groups to this list, do the following:

- Click the *Add* button on the bottom of the screen, the Organization Table will display.



User/Groups Organizations
corpdomain
Administrator
Director-IT
domainadmin
hnodd
jqpublic
Builtin
corpdomain
Domain Users
Enterprise Admins
Group Policy Creator Owners
Schema Admins
Users

Figure 32: Permission Settings Organization Table

- Select the appropriate users/groups from the list. To select multiple users, select individually by holding down the CTRL key, or select a series by selecting the top, then holding down the SHIFT key, then selecting the bottom selection.
- When all users/groups have been selected, click the *OK* button. This will add the users/groups to the grid on the Permissions form.

Step 3: Assign any (or all) permissions to the available users/groups.

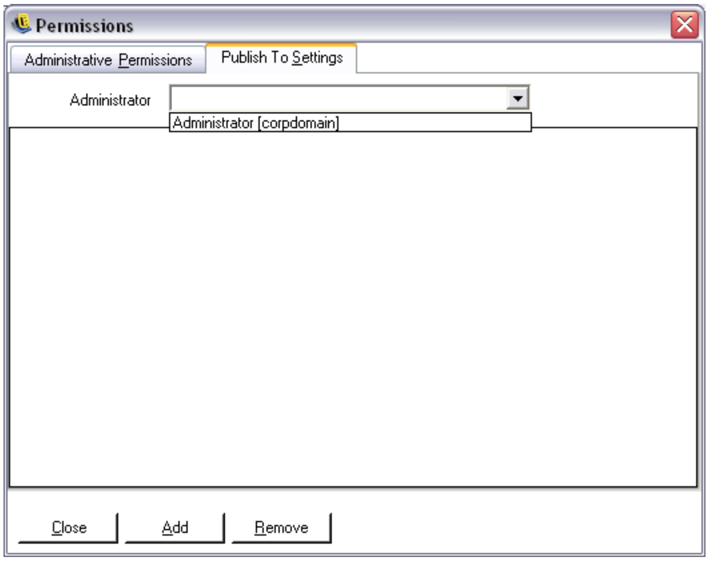
Step 4: To remove a selected user/group, highlight the name and click *Remove*. The selected name will be moved back to Organization Table.

Publish To Settings

Users/Groups who have Publish Policy checked will need to be assigned users and/or groups to publish to. To set the Publish To Settings, perform the following steps:

Step 1: Click the *Publish Settings* tab.

Step 2: Select the users/groups granted the Publish permission from the drop-down list.

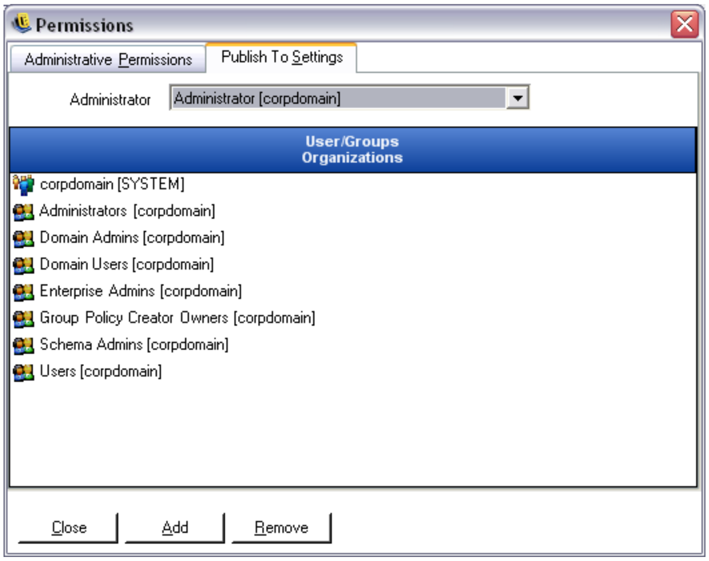


Administrator: Administrator [corpdomain]

Figure 33: Publish To Settings

Assign users/groups to this user/group by:

- Click the *Add* button on the bottom of the screen, the Organization Table will display.
- Select the appropriate users/groups from the list. To select multiple users, select individually by holding down the CTRL key, or select a series by selecting the top, then holding down the SHIFT key, then selecting the bottom selection.
- When all users/groups have been selected, click the *OK* button. This will add the users/groups to the selected name's publish list.



Administrator: Administrator [corpdomain]

User/Groups Organizations
corpdomain [SYSTEM]
Administrators [corpdomain]
Domain Admins [corpdomain]
Domain Users [corpdomain]
Enterprise Admins [corpdomain]
Group Policy Creator Owners [corpdomain]
Schema Admins [corpdomain]
Users [corpdomain]

Figure 34: Publish To List

Step 3: To remove a selected user/group, highlight the name in the list, and click *Remove*. The selected name will be moved back to the Organization Table.

The permission sets are immediately implemented, so the administrator only needs to click *Close*, and accept the changes to return to the editor.

When a new directory service is added, the Resource Account entered is granted full permissions settings, as described above.

Publishing a Policy

To Publish a security policy with the default settings, perform the following steps:

Step 1: Click Create New Policy

Step 2: Enter a name for the policy and click Create

Step 3: Save the policy and click the Publish tab

Step 4: Since ZSC users must check in to display in the tree, select the top of the tree on the left. Double-click to populate the publishing field with all current groups and users

Step 5: Click Publish to send the policy to the Policy Distribution Service

The policy generated in this manner will have the following characteristics:

- A single location (Unknown) is created
- CD/DVD ROM drives are allowed
- Removable storage devices are allowed
- All Communications Ports (incl. Wi-Fi) are permitted
- The Firewall Setting, All Adaptive (all outbound traffic over networking ports is allowed; unsolicited inbound traffic over networking ports is disallowed) is included

For information on creating a more robust security policy, please see the ESM Administrator's Manual for full details on policy components.

Continue to “Client Location Assurance Service Installation” on page 51.

Installing USB Reader

Included in the installation package is Novell's USB Reader, which assists the administrator in creating allowed USB device lists. To install the reader, perform the following steps:

Step 1: Click Setup, the installation begins

Step 2: On the Welcome Screen, click Next to continue

Step 3: Accept the license and click Next

Step 4: On the customer information screen, enter the appropriate username and organization information, and select whether anyone on this computer will be permitted access to this software, or just the user entered above.

Step 5: Click Install

Step 6: Click Finish. The USB Reader is now installed

For more information on using the USB Reader, please read the ESM Administrator's Manual.

Client Location Assurance Service Installation

Which server(s) will host the Client Location Assurance Service (CLAS)?

This server should be accessible ONLY when the user enters a controlled network environment, to help assure they are indeed in the environment the ZSC has identified. Instructions on configurations for failover and redundancies may be found below. CLAS can be deployed on the same server hosting the Single Server Installation or multi-server Management Service installation, if desired.

Install the CLAS onto a server that endpoints will only be able to detect when they are in the network environment which requires cryptographic verification.

Deployment of the CLAS on a Primary Domain Controller (PDC) is not supported for both security and functionality reasons.

Please make certain the following pre-requisites are in place PRIOR to beginning the installation:

- □ ZENworks Security Client (ZSC) to CLAS server name resolution: validate that the target computers (where the ZSC will be installed) can "ping" the CLAS server name. If unsuccessful, you will have to resolve this BEFORE continuing with the installation.
- □ Enable/Install Microsoft Internet Information Services (IIS), and ensure ASP.NET is enabled.

Click Client Location Assurance Service Installation from the Installation Interface menu. The CLAS installation will begin.

At launch, the installer will verify all required software is present on the server. If any are absent, they will be installed automatically before the installation continues to the Welcome Screen (license agreements for the additional software may need to be accepted). If Microsoft Data Access Components 2.8 are not installed, the server will need to reboot following that installation, before ESM installation can continue. If using Windows 2003 Server, ASP.NET 1.1 will be configured to run by the installer.

It is recommended that the CLAS Server be configured (hardened) so as 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, and so cannot be described in advance. Administrators are advised to consult the appropriate section of the Microsoft Technet security webpage. Additional access control recommendations are provided in the ESM Administrator's Manual.

Hardening of IIS: To protect access to only trusted machines, the virtual directory and/or IIS can be set up to have ACLs. Reference the articles below:

Granting and Denying Access to Computers

Restrict Site Access by IP Address or Domain Name

IIS FAQ: 2000 IP address and domain name restrictions

Working With IIS Packet Filtering

For security purposes, it is highly recommended the following default folders be removed from any IIS installation:

- IISHelp
- IISAdmin
- Scripts
- Printers

Novell also recommends using the IIS Lockdown Tool 2.1 available at microsoft.com.

Version 2.1 is driven by supplied templates for the major IIS-dependent Microsoft products. Select the template that most closely matches the role of this server. If in doubt, the Dynamic Web server template is recommended.

Installation Steps

To install the CLAS and generate a license key, perform the following steps:

Step 1: Click NEXT on the Welcome screen to continue

Step 2: Accept the Licensing Agreement and click NEXT

Step 3: The installation will copy files to the default directory: \Program Files\Novell\ESM CLAS

Step 4: The installation of the Client Location Assurance Service generates two keys, the privatekey and the publickey. The publickey file may be stored on the desktop or a different directory. If you wish to store the publickey file in a different directory, click Yes, and browse to the desired folder. Click No to accept the default to store the publickey file with the privatekey file

Step 5: CLAS is now installed, click FINISH to close the installation program.

The public key will need to be accessible to the Management Service.

CLAS Failover Installations

Multiple CLAS iterations may be installed on servers throughout the enterprise, to either cryptographically assure multiple enterprise locations, or to assure that if the primary CLAS server goes down, the location can still be assured.

In the case of the second scenario, the private key is located based on URL, rather than IP address. Therefore, a block of servers can be set up to share a single URL. CLAS may either be installed on a single server, then that server's image can be copied to each additional server, or it may be installed on each server separately, and the private and public keys can be copied over to the other servers. ALL servers in a URL block MUST have the same private and public keys.

Transferring the Public Key to the Management Service

After the installation has completed, the generated public key, which will be transferred via security policy to the ZSC, is located in the \Program Files\Novell\Novell ESM CLAS directory on the server. The public key is identified by the filename publickey. This filename can be changed to any name desired.

The publickey file will need to then be copied and transferred to the Management Service (anywhere on the service), which will allow the Management Console to access and distribute the key to all ZENworks Security Clients through a security policy. OR the publickey file can be loaded onto a PC running an ESM Management Console.

Continue to “ZENworks Security Client Installation” on page 53.

ZENworks Security Client Installation

Click the appropriate ZSC installer from the Installation Interface menu. The ZSC installation will begin. The following pages outline the installation process for both Basic and MSI installation.

- Basic Installation will install the ZSC only on the current machine.
- MSI Installation, will launch the installer in Administrative mode (/a) and will create an MSI Package of the software. This package can then be pushed-down or otherwise made available at a specified network location, with the required user inputs pre-configured. This allows individual users to install the software with the pre-defined server values.

Basic ZSC Installation

This will install the ZSC on the current machine ONLY.

□ Verify all security patches for Microsoft® and anti-virus software are installed and up-to-date

□ Install the Management Service SSL Root Certificates onto the local machine (ESM-MS.cer, or the enterprise certificate)

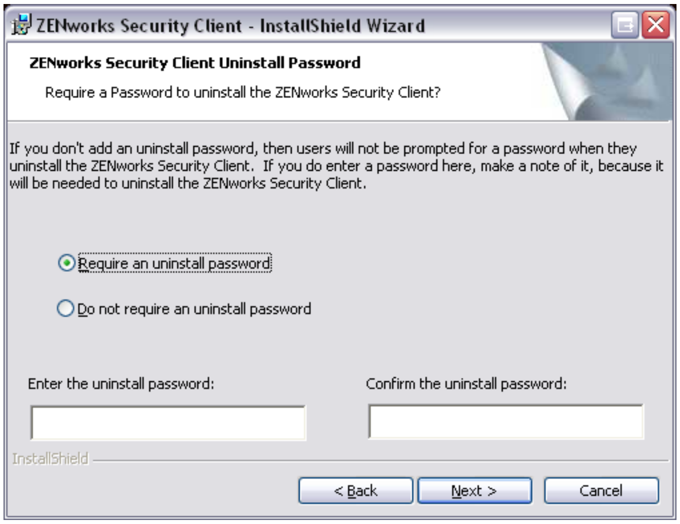
Note:

It is recommended antivirus/spyware software that is interacting with valid registry functions be shut down during the installation of the ZSC

Step 1: Click NEXT on the Welcome screen to continue.

Step 2: Accept the Licensing Agreement and click NEXT.

Step 3: Enter an installation password. This will prevent the user from uninstalling the ZSC through Add/Remove programs (recommended).



ZENworks Security Client - InstallShield Wizard

ZENworks Security Client Uninstall Password

Require a Password to uninstall the ZENworks Security Client?

If you don't add an uninstall password, then users will not be prompted for a password when they uninstall the ZENworks Security Client. If you do enter a password here, make a note of it, because it will be needed to uninstall the ZENworks Security Client.

● Require an uninstall password

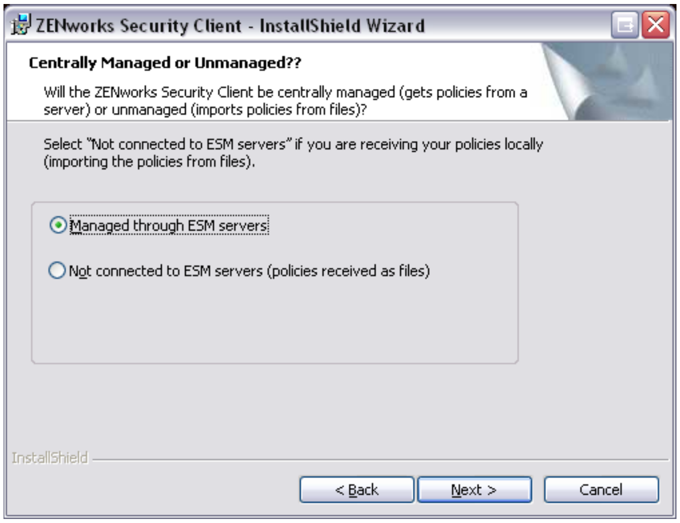
○ Do not require an uninstall password

Enter the uninstall password:

Confirm the uninstall password:

Figure 35: Uninstall Password

Step 4: Select how policies will be received (from Distribution Service for managed clients or retrieved locally for an unmanaged configuration [see page 61 for unmanaged details]).



ZENworks Security Client - InstallShield Wizard

Centrally Managed or Unmanaged??

Will the ZENworks Security Client be centrally managed (gets policies from a server) or unmanaged (imports policies from files)?

Select "Not connected to ESM servers" if you are receiving your policies locally (importing the policies from files).

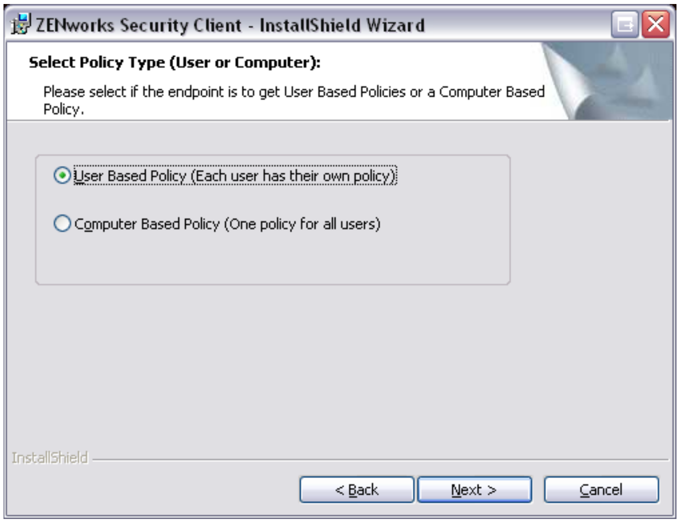
● Managed through ESM servers

○ Not connected to ESM servers (policies received as files)

Figure 36: Management Settings

Step 5: Enter the Management Service information.

Step 6: Select whether policies will be received for users or for the machine (machine-based policies).



ZENworks Security Client - InstallShield Wizard

Select Policy Type (User or Computer):

Please select if the endpoint is to get User Based Policies or a Computer Based Policy.

● User Based Policy (Each user has their own policy)

○ Computer Based Policy (One policy for all users)

Figure 37: User or Machine-based policies

Step 7: Click Install to install the program.

Step 8: Once the software is installed, the user will be prompted to restart their machine.

Note:

You can optionally copy the certificate for the Management Service into a folder co-located with setup.exe, prior to running the installation. This will automatically install the certificate onto the machine (e.g., for all users). This process can also be done with the Novell-issued license.dat file.

MSI Installation

This will create a MSI Package for the ZENworks Security Client. This package is used by a system administrator to publish the installation to a group of users via an Active Directory policy, or through other software distribution methods.

To create the MSI package, perform the following steps:

If using installing from the CD or ISO master installer and if you’re not planning to run any command-line variables (see “Command-line Variables” on page 58):

Step 1: Insert the CD and wait for the master installer to launch.

Step 2: Click **Product Installation.**

Step 3: Click **Security Client.**

Step 4: Click **Create ZSC MSI Package**. The installer will launch.

If using just the setup.exe for installation (the executable can be either downloaded from the Novell installations site, or found on the CD under: D:\ESM32\ZSC), begin with the following:

Step 1: Right click setup.exe.

Step 2: Select **Create Shortcut**.

Step 3: Right-click the shortcut and select **Properties**.

Step 4: At the end of the *Target* field, AFTER the quotes, enter a space click space bar once, then type “/a”

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

Several command-line variables are available for MSI installation. Please see “Command-line Variables” on page 58, for more details.

Step 5: Click **OK**.

Step 6: Double-click the shortcut to lauch the MSI installer.

When installation begins, perform the following steps:

Step 1: Click **NEXT** on the Welcome screen to continue.

Step 2: Accept the Licensing Agreement and click **NEXT**.

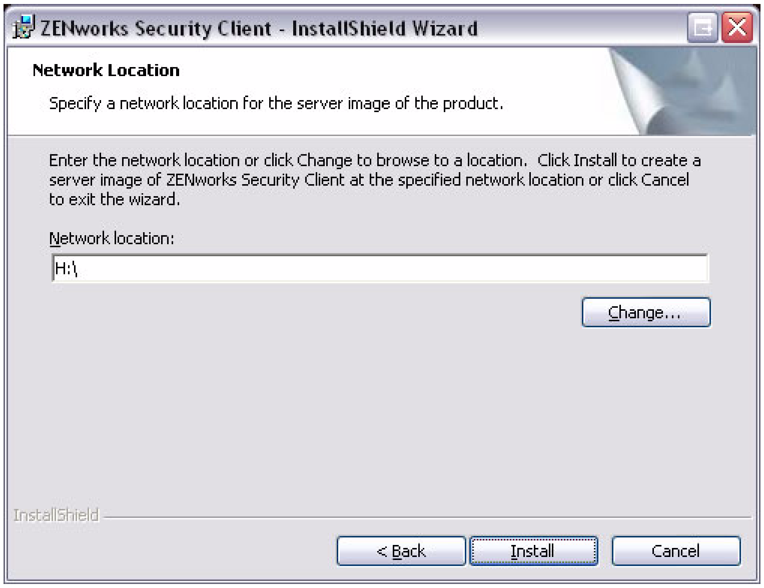
Step 3: Select whether an Uninstall Password is required (recommended) and enter the password.

Step 4: Select how policies will be received (from Distribution Service for managed clients, retrieved locally for an unmanaged configuration). If managed is selected:

- Enter the Management Service information (FQDN or NETBIOS name depending upon how it was entered during Management Service installation).
- Select if they will be user-based or machine-based policies.

Step 5: Enter an email address in the provided field to notify you if installation fails (optional).

Step 6: Enter the network location where the MSI image will be created, or browse to that location by clicking the Change button.



ZENworks Security Client - InstallShield Wizard

Network Location

Specify a network location for the server image of the product.

Enter the network location or click Change to browse to a location. Click Install to create a server image of ZENworks Security Client at the specified network location or click Cancel to exit the wizard.

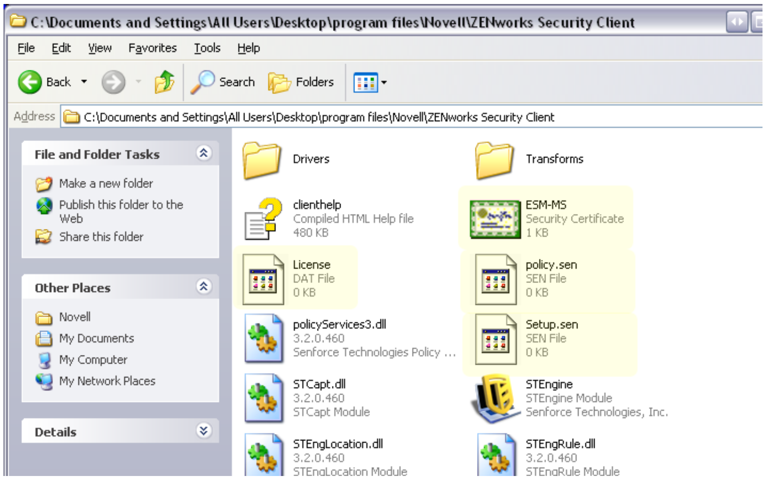
Network location: H:\

Figure 38: Select Network Location for MSI Image

Step 7: Click **Install** to create the MSI image.

Step 8: Browse to the created MSI image and open the "\program files\Novell\ZENworks Security Client\" folder

Step 9: Copy the Management Service SSL certificate (ESM-MS.cer, or the enterprise certificate) and the Novell License Key into this folder, replacing the default 0 KB files currently in the folder. The ESM-MS SSL certificate is available in the ESM Setup Files folder. The license key is emailed separately (if using the 30-day evaluation, no license key is necessary at this time).



C:\Documents and Settings\All Users\Desktop\program files\Novell\ZENworks Security Client

Address: C:\Documents and Settings\All Users\Desktop\program files\Novell\ZENworks Security Client

Figure 39: Replace the Default Files in the MSI Package

To set the MSI package to be pushed down to user groups like a Group Policy, perform the following steps:

Step 1: Open *Administrative Tools - Active Directory Users and Computers*, and open either *Root Domain* or *OU Properties*

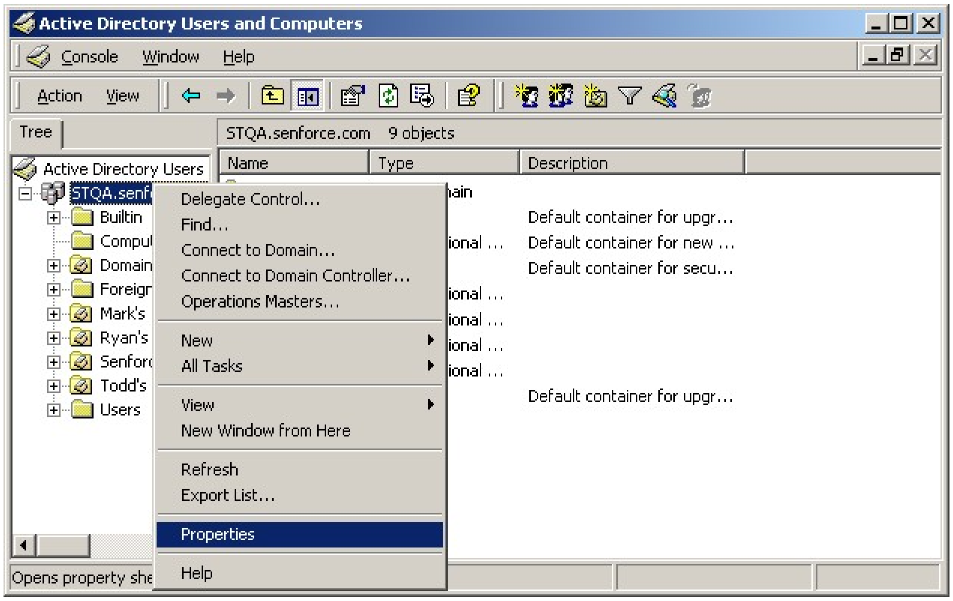
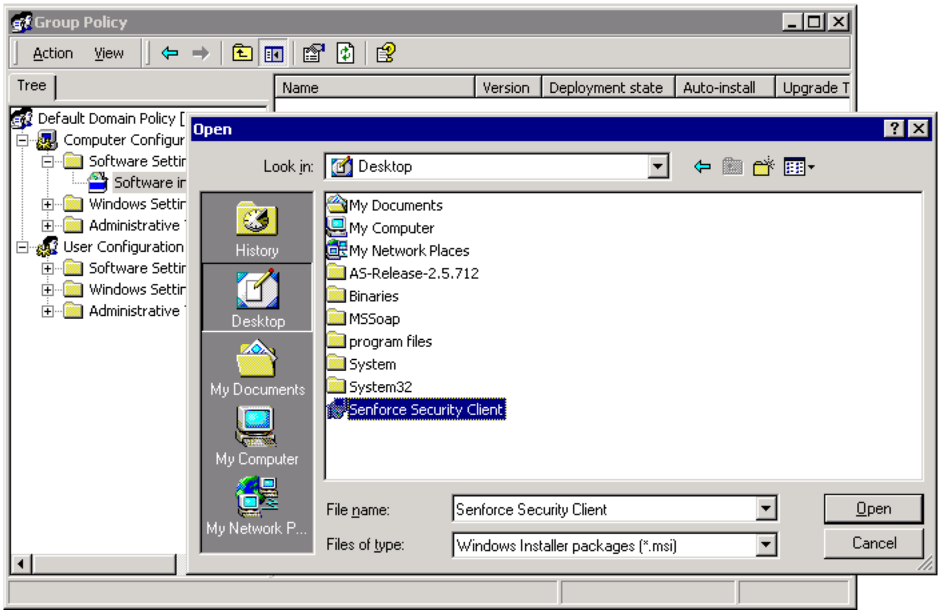


Figure 40: Open Properties in either Root Domain or OU

Step 2: Click the **Group Policy** tab and click **Edit**

Step 3: Add the MSI Package to Computer Configuration



Look in: Desktop

File name: Senforce Security Client

Files of type: Windows Installer packages (*.msi)

Figure 41: Select the MSI package to add

The MSI Package can now be pushed to all users.

Command-line Variables

Command-line variable options are available for MSI installation. These MUST be set in the executable shortcut that is set to run in administrator mode (installations steps above). To use a variable, the following command-line must be entered in the MSI shortcut:

“...\setup.exe” /a /V"*variables*". Enter any of the commands below between the quotation marks. Separate multiple variables with a single space.

Example: setup.exe /a /V"STDRV=stateful STBGL=1" creates an MSI package where the ZENworks Security Client will boot in All Stateful with strict white-listing enforced.

Note:

Booting in stateful MAY cause some interoperability issues (DHCP address delays, Novel network interop issues, etc.).

The following command line variables are available:

Table 4: Command Line Variables

Command Line Variable	Description	Notes
STDRV=stateful	NDIS driver all stateful at boot time.	Changes the default state of the NDIS driver from All Open to All Stateful permitting all network traffic at boot time, until the ZSC has determined its location.
/qn	Quiet install.	Use to suppress the typical MSI Installation process. ZSC will activate at next user reboot.
STRBR=ReallySuppress	No reboot after install completes.	Security enforcement and client self defense are not fully functional until after the first reboot.
STBGL=1	Strict white list enforcement on application control.	A policy MUST be created that identifies the application on the white list, and distributed with this policy.
STUPGRADE=1	Upgrade the ZSC.	Use when upgrading the ZSC.
STUNINSTALL=1	Uninstall the ZSC.	Use when uninstalling the ZSC.
STUIP=”the password”	Uninstall with password	Use when an uninstall password is active.
STNMS=”MS Name”	Change the Management Service name.	Changes the Management Service name for the ZSC.

Table 4: Command Line Variables

Command Line Variable	Description	Notes
POLICYTYPE=1	Change ZSC to machine-based policies.	Use to change MSI-installed ZSCs to accept machine-based, rather than user-based policies.
POLICYTYPE=2	Change ZSC to user-based policies.	Use to change MSI-installed ZSCs to accept user-based, rather than machine-based policies.
STVA=”Adapter name”	Add Virtual Adapter.	Use to activate policy control over a virtual adapter
/L*v c:\log.txt	Turn on logging.	Use to activate logging at installation. If not, this will have to be done through the ZSC Diagnostics tools (see Administrator’s Manual).

Distributing a Policy with the MSI Package

The default policy included at MSI installation can be replaced with an enterprise-configured policy. To push down a specific policy with the MSI image, perform the following steps:

Step 1: Create a policy to be distributed to all users through the Management Console (see the Administrator's Manual for details on Policy Creation)

Step 2: Export the policy, save it as policy.sen

Note:

All policies distributed in this manner (unmanaged) MUST be named policy.sen in order for the ZSC to accept them. Policies not named "policy.sen" will not be implemented by the ZSC.

Step 3: Open the folder the policy was exported into and copy the policy.sen and setup.sen files

Step 4: Browse to the created MSI image and open the "\program files\Novell\ZENworks Security Client\" folder

Step 5: Paste the policy.sen and setup.sen files into the folder. This will replace the default policy.sen and setup.sen files

User Installation of the ZSC from MSI

When the end-user re-authenticates to the domain (through a reboot of their machine), the MSI installation package will run prior to their logging-in. Once completed, the machine will reboot and the user will be permitted to log-in to their machine. The ZSC will be installed and running on the machine.

Running the ZENworks Security Client

The ZSC will run automatically at system startup. For user operation of the ZSC, see the ZENworks Security Client User's Manual.

The User's Manual can be distributed to all users to help them better understand the operation of their new endpoint security software.

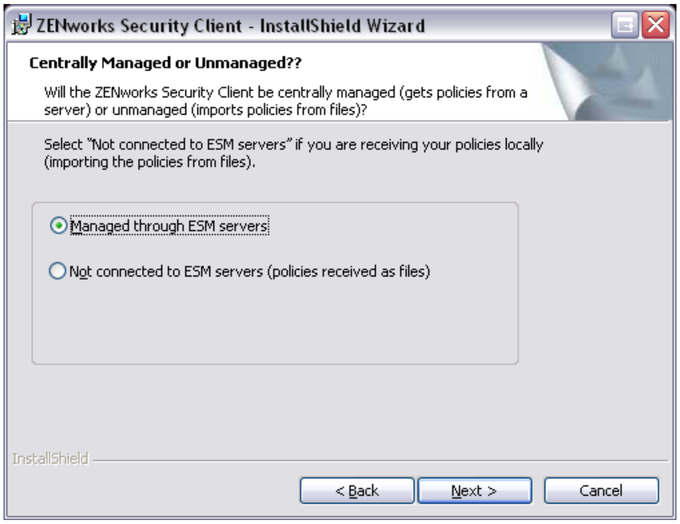
ESM Unmanaged Installation

An enterprise can also run the ESM ZENworks Security Client and Management Console in an Unmanaged mode (without connection to the Policy Distribution Service, or the Management Service). This is available as an installation option, primarily intended for setting up simple evaluations. This option is also ideal for enterprises with little or no server space, or with basic security needs. However, quick policy updates and Compliance Reporting are not available in this configuration.

Unmanaged ZENworks Security Client Installation

To install an unmanaged ZENworks Security Client, follow the instructions on page 53, and select the *Not Connected to ESM Servers (policies received as files)* option. The installation will bypass the questions regarding the names of the servers and will install the ZSC onto this machine (an MSI package may also be created for an Unmanaged ZSC).

.



Centrally Managed or Unmanaged??

Will the ZENworks Security Client be centrally managed (gets policies from a server) or unmanaged (imports policies from files)?

Select "Not connected to ESM servers" if you are receiving your policies locally (importing the policies from files).

● Managed through ESM servers

○ Not connected to ESM servers (policies received as files)

Figure 42: Select "Not Connected to ESM Servers"

Stand-Alone Management Console

This configuration allows an ESM Management Console to be installed and create policies without connecting to an outside Management Service, or distributing policies through the Policy Distribution Service. Select Stand-Alone Management Console Installation from the Master Installer menu, and follow the instructions on page 39 for installation.

At the start of the installation, a SQL database is installed first (if one exists on the machine, the installer will setup the appropriate databases instead). Once the database is installed, the installation will stop. The machine will need to be restarted to activate the SQL database. Following reboot, activate the installation again to continue.

Most policy functionality is available for deployment, with the exception of Reporting. All exported policy files will need to be distributed to an ZSC's *\Program Files\Novell\ZENworks Security Client* directory.

Distributing Unmanaged Policies

To distribute unmanaged polices, perform the following steps:

Step 1: Locate and copy the Management Console's setup.sen file to a separate folder.

The setup.sen file is generated at installation of the Management Console, and placed in *\Program Files\Novell\ESM Management Console*

Step 2: Create a policy in the Management Console (see Adminstrator's Manual)

Step 3: Use the Export command to export the policy to the same folder containing the setup.sen file.
All policies distributed MUST be named policy.sen for the ZSC to accept them.

Step 4: Distribute the policy.sen and setup.sen files. These files MUST be copied to the \Program Files\Novell\ZENworks Security Client\ directory for all unmanaged clients.

The Setup.sen file only needs to be copied to the unmanaged SSCs once, with the first policy. Afterwards, only new policies need to be distributed.

If an Unmanaged ZSC is installed on the same machine as the Stand Alone Management Console, the Setup.sen file will also be copied to the *\Program Files\Novell\ZENworks Security Client* directory. If the Unmanaged ZSC is installed on the machine after the Stand Alone Editor, the file will need to be transferred manually as described above.

Clicking the Publish button will immediately publish the policy to that machine's unmanaged ZENworks Security Client. To provide policies to multiple, unmanaged users use the Export feature as described above.